UNITED STATES
SECURITIES AND EXCHANGE COMMISSION

Washington, D.C. 20549

FORM 10-K

(Mark One)

☒ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the fiscal year ended January 31, 2023

OR

☐ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the transition period from to

Commission file number 001-40531

SENTINELONE, INC.

(Exact name of registrant as specified in its charter)

Delaware	**99-0385461**
(State or other jurisdiction of incorporation or organization)	(I.R.S. Employer Identification No.)

444 Castro Street, Suite 400
Mountain View, California 94041

(Address of Principal Executive Offices)

(855) 868-3733

Registrant's telephone number, including area code)

Securities registered pursuant to Section 12(b) of the Act:

Title of each class	Trading Symbol(s)	Name of each exchange on which registered
Class A common stock, par value $0.0001	**S**	**The New York Stock Exchange**

Securities registered pursuant to section 12(g) of the Act: None.

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes x No ☐

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act. Yes ☐ No x

Indicate by check mark whether the registrant: (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports); and (2) has been subject to such filing requirements for the past 90 days. Yes x No ☐

Indicate by check mark whether the registrant has submitted electronically every Interactive Data File required to be submitted pursuant to Rule 405 of Regulation S-T (§232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit such files). Yes x No ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, a smaller reporting company, or an emerging growth company. See the definitions of “large accelerated filer,” “accelerated filer,” smaller reporting company,” and “emerging growth company” in Rule 12b-2 of the Exchange Act:

Large accelerated filer	☒	Accelerated filer	☐
Non-accelerated filer	☐	Smaller reporting company	☐
		Emerging growth company	☐

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Indicate by check mark whether the registrant has filed a report on and attestation to its management’s assessment of the effectiveness of its internal control over financial reporting under Section 404(b) of the Sarbanes-Oxley Act (15 U.S.C. 7262(b)) by the registered public accounting firm that prepared or issued its audit report. ☒

If securities are registered pursuant to Section 12(b) of the Act, indicate by check mark whether the financial statements of the registrant included in the filing reflect the correction of an error to previously issued financial statements. ☐

Indicate by check mark whether any of those error corrections are restatements that required a recovery analysis of incentive-based compensation received by any of the registrant's executive officers during the relevant recovery period pursuant to §240.10D-1(b). ☐

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes ☐ No ☒

The aggregate market value of voting stock held by non-affiliates of the registrant on July 31, 2022, based on the closing price of $24.85 for shares of the Registrant's Class A common stock as reported by the New York Stock Exchange, was approximately $3.5 billion.

As of March 24, 2023, the registrant had outstanding 235,013,639 shares of Class A common stock and 53,607,352 shares of Class B common stock.

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the registrant's definitive proxy statement relating to its 2023 Annual Meeting of Stockholders (Proxy Statement) are incorporated by reference into Part III of this Annual Report on Form 10-K where indicated. Such Proxy Statement will be filed with the United States Securities and Exchange Commission (SEC) within 120 days after the end of the registrant's fiscal year ended January 31, 2023 to which this Annual Report on Form 10-K relates.

TABLE OF CONTENTS

Special Note About Forward-Looking Statements

This Annual Report on Form 10-K contains forward-looking statements within the meaning of Section 17A of the Securities Act of 1933, as amended (the Securities Act), and Section 21E of the Securities Exchange Act of 1934, as amended (the Exchange Act), about us and our industry that involve substantial risks and uncertainties. All statements contained in this Annual Report on Form 10-K, other than statements of historical fact, including statements regarding our future operating results and financial condition, our business strategy and plans, market growth, and our objectives for future operations, are forward-looking statements. The words "believe," "may," "will," "potentially," "estimate," "continue," "anticipate," "intend," "could," "would," "project," "target," "plan," "expect," and similar expressions are intended to identify forward-looking statements.

Forward-looking statements include, but are not limited to, statements about:

- our future financial performance, including our expectations regarding our total revenue, cost of revenue, gross profit or gross margin, operating expenses, including changes in operating expenses and our ability to achieve and maintain future profitability;
- the political, economic, and macroeconomic climate, whether in the cybersecurity industry in general, or among specific types of customers or within particular geographies, including but not limited to, the impacts related to labor shortages, supply chain disruptions, a potential recession, inflation, and rising interest rates;
- our business plan and our ability to effectively manage our growth;
- our total market opportunity;
- anticipated trends, growth rates, and challenges in our business and in the markets in which we operate;
- our ability to maintain the security and availability of our platform;
- market acceptance of our platform and our ability to increase adoption of our platform;
- beliefs and objectives for future operations;
- our ability to further penetrate our existing customer base and attract, retain, and expand our customer base;
- our ability to timely and effectively scale and adapt our platform;
- our ability to develop new products and services and bring them to market in a timely manner and make enhancements to our platform;
- our expectations concerning relationships with third parties;
- our ability to maintain, protect, and enhance our intellectual property;
- our ability to continue to expand internationally;
- the effects of increased competition in our markets and our ability to compete effectively;
- future acquisitions or investments in complementary companies, products, services, or technologies and our ability to integrate such acquisitions or investments;
- our ability to stay in compliance with laws and regulations that currently apply or become applicable to our business both in the United States and internationally;
- economic and industry trends, projected growth, or trend analysis;

- the impact of the continuing COVID-19 pandemic on our operations, financial results, and liquidity and capital resources, including on our and our customers, sales, expenses, and employees;
- the impact of natural or man-made global events on our business, including wars and other armed conflict, such as Russia's invasion of Ukraine;
- expenses associated with being a public company; and
- other statements regarding our future operations, financial condition, and prospects and business strategies.

We caution you that the foregoing list may not contain all of the forward-looking statements made in this Annual Report on Form 10-K.

These forward-looking statements are subject to a number of risks, uncertainties, and assumptions, including those described in the section titled "Risk Factors" and elsewhere in this Annual Report on Form 10-K. Moreover, we operate in a very competitive and rapidly changing environment, and new risks emerge from time to time. It is not possible for our management to predict all risks, nor can we assess the impact of all factors on our business or the extent to which any factor, or combination of factors, may cause actual results to differ materially from those contained in any forward-looking statements we may make. In light of these risks, uncertainties, and assumptions, the forward-looking events and circumstances discussed in this Annual Report on Form 10-K may not occur, and actual results could differ materially and adversely from those anticipated or implied in the forward-looking statements.

You should not rely upon forward-looking statements as predictions of future events. The events and circumstances reflected in the forward-looking statements may not be achieved or occur. We undertake no obligation to update publicly any of these forward-looking statements for any reason after the date of this Annual Report or to conform these statements to actual results or to changes in our expectations, except as required by law. Our forward-looking statements do not reflect the potential impact of any future acquisitions, partnerships, mergers, dispositions, joint ventures, or investments we may make.

You should read this Annual Report on Form 10-K and the documents that we reference in this Annual Report on Form 10-K and have filed with the SEC as exhibits to this report with the understanding that our actual future results, performance, and events and circumstances may be materially different from what we expect.

PART I

ITEM 1. BUSINESS

Overview

Cybersecurity is indispensable to our digital way of life, with millions of cyberattacks occurring every year resulting in trillions of dollars in damages. We are in the midst of a generational shift in cybersecurity, ushered in by the ongoing digital transformation of the enterprise. Attacks can inflict damages that span operational disruption, leadership change, loss of customer trust, and intellectual property theft, among others. The rise and persistence of cyberattacks clearly shows that there is a long way to go from here. Enterprises must deploy solutions that enable them to stay one step ahead of attackers and address intrusion attempts in real-time at machine speed - empowering human operators with the speed, scale, and precision of technology.

We envisioned a revolutionary data and artificial intelligence (AI) paradigm where technology alone could autonomously prevent, detect, and respond to cyberattacks. It is time to fight machine with machine. We pioneered the world's first purpose-built AI-powered Extended Detection and Response (XDR) platform to make cybersecurity defense truly autonomous, from the endpoint and beyond. Our Singularity Platform instantly defends against cyberattacks - performing at a faster speed, greater scale, and higher accuracy than otherwise possible from any single human or even a crowd.

Our Singularity Platform ingests, correlates, and queries petabytes of structured and unstructured data from a myriad of ever-expanding disparate external and internal sources in real-time. We build rich context and deliver greater visibility by constructing a dynamic representation of data across an organization. As a result, our AI models are highly accurate, actionable, and autonomous. Our distributed AI models run both locally on every endpoint and every cloud workload, as well as on our cloud platform. Our Static and vector-agnostic Behavioral AI models, which run on the endpoints themselves, provide our customers with protection even when their devices are not connected to the cloud. In the cloud, our Streaming AI detects anomalies that surface when multiple data feeds are correlated.

Furthermore, our platform provides visibility across an organization's digital assets through one console, making it easy and very fast for analysts to search through petabytes of data to investigate incidents and hunt threats. Our Singularity Platform offers multi-tenancy and can be deployed on a diverse range of environments that our customers choose, including public, private, or hybrid clouds.

On each endpoint and cloud workload, we run highly optimized AI models in a single lightweight software agent. Our Static AI model predicts file-based attacks of all types, even previously unknown threats, often referred to as "zero-day attacks," with extreme precision in milliseconds. Our Behavioral AI model maps, monitors, and links all behaviors on the endpoint to create rich, contextual narratives that we call Storylines. These high-fidelity Storylines are continuously evaluated by our Behavioral AI model. When activity is deemed a threat, our software autonomously takes action to kill the attack. Because Storylines contain a complete record of unauthorized changes made during an attack, we are ready to remediate or roll back these changes.

The power to turn back time on a device is unique in the market. It is the ultimate safety net and exemplifies autonomous cybersecurity. Therefore, our software eliminates manual, expensive, and time-consuming incident cleanup. In the cloud, our platform aggregates Storylines. Our Streaming AI detects anomalies that surface when multiple data feeds are correlated with additional external and internal data. By providing full visibility into the Storyline of every secured device across the organization through one console, our platform makes it very fast for analysts to easily search through petabytes of data to investigate incidents and proactively hunt threats.

We have extended protection and visibility beyond the traditional endpoint to cloud workloads, identity credentials, unmanaged devices, and IoT devices. This empowers security analysts of all skill levels to hunt, investigate, and remediate even the most sophisticated threats across the network leveraging automated context provided by our Storylines. Our proprietary data stack - DataSet - and cloud architecture enable us to retain this rich, contextual data on behalf of our customers for extended periods of time in a highly cost-efficient manner. All of this threat intelligence is fed back into our AI model and further strengthens our algorithms, creating a strong flywheel effect and deepening our competitive moat.

Our Singularity Platform can be flexibly deployed on the environments that our customers choose, including public, private, or hybrid clouds. Our feature parity across Windows, macOS, Linux, and Kubernetes offers best-of-breed protection, visibility, and control across today's heterogeneous information technology (IT) environments. Together, these capabilities make our platform the logical choice for organizations of all sizes, industry verticals, and compliance requirements. Our platform offers true multi-tenancy, which enables the world's largest organizations and our managed security providers and incident response partners with an excellent management experience. Our customers realize improved cybersecurity outcomes with fewer people.

Our Singularity Platform is used globally by organizations of all sizes across a broad range of industries. Our AI and automation driven approach to cybersecurity has been adopted by some of the world's largest organizations. As a result, we have grown rapidly since our inception. As of January 31, 2023, we had over 10,000 customers, increasing from over 6,700 as of January 31, 2022. Our revenue for fiscal 2023 and 2022 was $422.2 million and $204.8 million, respectively, representing year-over-year growth of 106%. During this period, we continued to invest in growing our business to capitalize on our market opportunity. As a result, our net loss for fiscal 2023 was $378.7 million compared with net loss of $271.1 million in fiscal 2022.

Industry Background

Cybersecurity is fundamentally a data problem. Advances in AI, specifically machine learning, where algorithms use data to make decisions with minimal human intervention, are already revolutionizing fields such as healthcare, advertising, and securities trading. We believe that AI is ripe for revolutionizing cybersecurity. First, organizations need to ingest, normalize, and correlate petabytes of structured and unstructured data from a myriad of external and internal data in a cost efficient manner. Second, organizations need to apply powerful AI models on this high-fidelity contextual data to automatically detect known and unknown threats, then autonomously remediate and neutralize the threats. It is critical that we harness the power of data and AI to protect our digital way of life.

Stakes are high for organizations and cybercriminals. The exponential growth of sensitive customer and business data has simultaneously made many organizations and governments the target of highly sophisticated cybercriminals. Powered by very large networks of individual attackers distributed worldwide, cybercrime is practically infinite in scale and transcends geographical boundaries. To gain access to an organization's data, cybercriminals target endpoints, applications, user credentials, and deploy a variety of sophisticated methods in the form of attack frameworks, machine learning, weaponized exploits, fileless techniques, and social engineering. As a result, solutions that help strengthen and scale their cyber defenses cost effectively is a top-level priority for organizations today.

Tectonic shifts in IT require a "Zero Trust" operating procedure. With millions of remote devices accessing thousands of applications running in public, private and hybrid clouds, traditional perimeter-based security controls are bypassed and organizations have to operate in a "Zero Trust" IT environment. The attack surface has expanded considerably, and the notion of a corporate perimeter protected by firewalls is a relic of the past, making the endpoint the epicenter, and endpoint protection software the first, and last, line of defense. Several tectonic shifts in IT have increasingly left companies vulnerable including:

- ***Rapid adoption of cloud computing.*** Cloud computing has become a strategic imperative for organizations to accelerate their digital transformation. Security and compliance is a shared responsibility model between the cloud infrastructure provider and their customer, organizations are looking for technology solutions that protect their growing cloud workloads while enabling flexible deployment options across public, private and hybrid clouds.

- ***The operating system landscape is more complex than ever before.*** The diversification of IT and bring your-own-device policies brought Macs and other devices into today's organizations. Organizations are looking for cybersecurity solutions that deliver comprehensive defense capabilities and feature parity across a large variety of operating systems, including Windows, macOS, and Linux, without burdening their IT teams.

- ***Proliferation of connected devices*.** Billions of connected devices are online today and the numbers are only expected to increase. Many of these devices will have little to no built-in security capabilities. Cybercriminals are increasingly exploiting inherent vulnerabilities in these devices to breach organizations. Unmanaged devices are especially vulnerable. As a result, the attack surface has exploded. Visibility across connected devices and continuous assessment of their risk profile has become a top priority for organizations.

- ***Remote work is here to stay.*** The COVID-19 pandemic changed the way most organizations operate, accelerating technology's role in supporting remote work. The pandemic has accelerated the structural shift towards a more distributed workforce. The growth of remote work has increased the risk of cyberattacks. As a result of the accelerated structural shift towards a distributed workforce, organizations are increasingly looking for cybersecurity solutions that safeguard their remote workforce and employee credentials.

Sophisticated cyberattacks circumvent existing security controls. Cyberattacks have evolved from malware to highly sophisticated, organized and large-scale attacks by malicious insiders, criminal syndicates, and nation-states seeking to circumvent existing security controls and undermine critical societal functions through a variety of attacks that are fast acting that take only seconds to breach organizations, exfiltrate data, demand ransoms, and disrupt operations. Alternatively, some attacks, such as advanced persistent attacks (APT), and targeted attacks, are designed to breach the organization and stealthily infiltrate across assets to steal data, facilitate future attacks, or cause other harm over a long period of time, all while operating undetected.

Cybersecurity teams are unable to scale. While the number of connected devices, applications and cyber threats have increased exponentially, organizations are facing an acute shortage of skilled cybersecurity talent. The large number of security solutions that companies have deployed over time generate large volumes of alerts that overwhelm security teams as they have to sift through and analyze. Out of necessity, organizations are demanding solutions that do not require human intervention to prevent, detect, and remediate cyber threats.

Limitations of Existing Solutions

Organizations must deploy solutions that enable them to stay one step ahead of attackers and address intrusion attempts in real-time. As attackers up the ante, developing new skills and deploying new tactics and techniques, existing tools are often unable to prevent and respond effectively to breaches. The result is a rising number of successful high-profile attacks.

Key limitations of existing tools are that they:

- ***Cover a limited spectrum of cyber threats*.** Existing tools, such as signature-based approaches, human-powered monitoring, application whitelisting and sandboxing, are each effective under limited circumstances, but lack the ability to detect the full spectrum of threats organizations are dealing with. For example, signature-based approaches can detect attacks that have been seen previously, but are incapable of preventing a wide range of attacks, such as unknown malware, ransomware, modified versions of previously known attacks and the exploitation of zero day vulnerabilities. In addition, they lack the ability to detect and prevent an increasing number of fileless attacks, that deposit no malware, but instead exploit operating system vulnerabilities and use trusted tools within IT environments. In general, enterprises need to take a more holistic view of security protection across endpoints, cloud environments, and identity credentials. A unified platform approach is needed to deliver comprehensive protection, visibility, and user experience. As a result, despite deploying a myriad of point solutions, organizations have continued to suffer huge losses from cyberattacks.

- ***Utilize AI approaches that rely on humans to power protection mechanisms*.** First generation AI tools cannot handle the volume, variety, and velocity of data that must be ingested and analyzed, in real-time, to be effective in preventing breaches. These tools often rely on ineffective pattern-matching algorithms in the cloud that generate so much "noise" that human intervention is required to extract useful "signals." Without curated, contextual data, these tools only generate more alerts that need to be analyzed by humans. They cannot take action at machine speed and are thus unable to detect and prevent or stop many fast-acting

attacks. Additionally, due to communication latency with the cloud, these tools cannot generate actionable insights in real-time, which is required to stop many current threats.

- ***Lack long-term data visibility to proactively investigate advanced threats.*** Existing endpoint detection and response (EDR) tools lack the capability to store large sets of historical data cost efficiently, and consequently often only offer limited data retention capabilities. This results in only partial datasets being available for threat hunting and time bound retrospective forensic analysis. Limited historical EDR data makes full incident investigation challenging for security personnel, as they are unable to go back in time and see how the attack breached the organization and progressed.

- ***Struggle to protect complex modern IT environments.*** Existing tools were not designed to protect today's multi-cloud, multi-device, multi-OS IT environments. Vendors have extended their existing solutions by bolting on functionalities, which has led to a wide disparity of capabilities across endpoints and operating systems. Existing tools further lack the ability to identify unmanaged IoT devices which often have very limited, if any, built-in security capabilities and can be used by attackers to access the networks of target organizations. This lack of unified visibility and control over endpoints, cloud workloads, and IoT devices results in gaps in security coverage for organizations.

- ***Lack deployment flexibility for organizations.*** Organizations struggle with the limited deployment methods mandated by existing tools. On-premise tools impose complexity and maintenance burdens on organizations. These tools typically lack the ability to quickly adapt to organizations' rapidly evolving IT environments, which requires significant upfront investments and configuration and integration efforts. On the other hand, cloud-only cybersecurity vendors are unsuitable for many large and complex enterprises and governments that need private or hybrid cloud solutions to meet their security, regulatory, and compliance requirements.

- ***Inhibit technology workflow automation.*** Many existing tools lack out-of-the box APIs and rely heavily on professional services, which makes the integration and implementation process long, expensive and often unattainable. The lack of flexible workflow integrations limits organizations' ability to reduce overhead by automating processes, and to improve their security by ensuring that process steps are done quickly, consistently, and according to their predefined requirements.

A new paradigm for cybersecurity is needed to autonomously protect organizations and their heterogeneous IT footprints from highly sophisticated, machine-based attacks in a holistic, seamless, and automated manner.

Our Revolutionary Autonomous Approach to Cybersecurity

Our AI-powered Singularity Platform defines and delivers XDR. Our platform ingests, correlates, and queries petabytes of structured and unstructured data from a myriad of disparate external and internal sources in real-time. We build rich context by constructing a dynamic representation of data across an organization. As a result, our AI models are highly accurate, actionable, and autonomous. Our distributed AI models run both locally on every endpoint and every cloud workload, as well as on our cloud platform. Our Static and vector-agnostic Behavioral AI models, which run on the endpoints themselves, provide our customers with protection even when their devices are not connected to the cloud. In the cloud, our Streaming AI detects anomalies that surface when multiple data feeds are correlated. Furthermore, our platform provides visibility across an organization's digital assets through one console, making it easy and very fast for analysts to search through petabytes of data to investigate incidents and hunt threats. Our Singularity Platform offers multi-tenancy and can be deployed on a diverse range of environments that our customers choose, including public, private, or hybrid clouds.

Singularity Platform Capabilities and Our Competitive Strengths

- ***Protects against present and future cyber threats.*** A combination of our powerful Static AI and Behavioral AI on the device with Streaming AI models in the cloud addresses the spectrum of attacks in an evolving threat landscape, including ransomware, known and unknown malware, trojans, hacking tools, memory exploits, script misuse, bad macros and "living off the land," or file-less, attacks. As our on-device machine

learning models assess how an endpoint behaves, they are completely independent of the attack vector itself or any further updates and configurations.

- ***Platform approach enables protection and visibility across all digital assets.*** Our Singularity Platform provides organizations with our full suite of real-time threat prevention, detection, and remediation capabilities across all of their endpoints, cloud workloads, servers, operating systems, and user credentials. Our platform further leverages our agents, combined with passive and active network discovery methods, to provide our customers with organization-wide visibility into all of their network assets, managed and unmanaged. Our platform approach helps enterprise consolidate security tools while enhancing enterprise-wide coverage.

- ***Provides autonomous protection and remediation.*** Powered by our AI and Storyline technology, our agents defend and heal endpoints autonomously and in real-time by stopping malicious processes, quarantining, remediating, and even rolling back events to surgically keep endpoints clean. Rollbacks are performed autonomously and in real-time, eliminating the need for manual, expensive, and time-consuming incident cleanup.

- ***Enables facilitated, as well as fully-automated, incident investigation and proactive threat hunting.*** Our platform gives security teams the ability to search their IT assets for behavioral indicators via a single-click interface. Our deep visibility and contextual data empowers security analysts of all skill levels to run queries at very fast speeds, and quickly understand the root causes behind the most complex threats. Our watchlists further lighten the load on security teams by giving them the ability to schedule customized and fully automated threat hunting searches according to their own criteria.

- ***Provides full forensic recall for complete remediation.*** We offer our customers the ability to retain rich, contextual data for up to three years in a highly cost efficient manner. This forensic data helps our customers to investigate breaches that have stealthily infiltrated their organization and operated undetected for many months. It gives them the ability to ensure that any incident has been fully remediated without the need to reimage or replace elements of their IT infrastructure.

- ***Provides a superior customer experience.*** We put the user at the center of our product development and engineering processes. The combination of our intuitive and clean user interface, our ability to provide context with one click, and our high degree of automation empowers our customers to use our platform independent of their expertise level.

- ***Proprietary data stack.*** Our modern, innovative, and extensible data stack - DataSet - enables us to ingest, process and analyze massive amounts and a wide variety of data types efficiently. Our independent, component-driven architecture allows us to evolve rapidly leveraging continued innovations of public cloud infrastructure, while controlling every aspect of our innovation roadmap and customer experience. As more data improves our AI algorithms and cross-organizational visibility, our data stack allows us to offer superior threat protection for our customers.

- ***Deeply embedded within our customers' IT stacks.*** Our API-first approach and Singularity Marketplace allow our customers to easily integrate intelligence, analytics, automation, and other third-party business applications with our platform.

- ***Flexible deployment model that delivers rapid time to value.*** Our Singularity Platform can be quickly and easily deployed on a diverse range of environments of our customers, and without extensive configuration or maintenance - including the public, private or hybrid cloud, making it relevant for organizations of all sizes with varying compliance and regulatory requirements.

- ***Rich partner ecosystem.*** We have deep partnerships with many of the leading Independent Software Vendors (ISVs), alliance partners whom we engage with on joint technology and/or go-to-market strategies; and channel partners, such as distributors, resellers, Managed Service Providers (MSPs), Managed Security Service Providers (MSSPs), Managed Detection and Response Providers (MDRs), Original Equipment Manufacturers (OEMs), and Incident Response (IR) firms. Our partner relationships provide us with significantly broader market reach. In particular, we do not currently have a services offering that competes with our IR partners. Therefore, they seek to bring us into remediation situations where their customers often become our customers. As a result, many of our partners act as force multipliers and broaden our market reach. By empowering MSPs, MSSPs, MDRs, and IR firms with our technology and through our deep partnerships with them, we benefit from the market penetration of those entities.

- ***Quality and access of cybersecurity and AI talent.*** Our thought leadership in security and AI, combined with our award-winning culture, allows us to attract and retain some of the best talent at a global scale. It allows us to develop state-of-the-art solutions, to innovate faster, and to solve many of the industry's most complex problems.

We believe our leading security and platform breadth position us well to consolidate and unify spend across multiple categories. Over time, we believe this unification and re-architecture of the prevention, detection and response paradigm will create new opportunities for additional products and features for us.

Growth Strategy

Key elements of our growth strategy include:

- ***Continue to innovate and enhance our cybersecurity and data platform.*** We will continue to expand our platform and XDR capabilities by developing new modules to include greater functionality and address additional use cases. As a pioneer in autonomous and AI-based endpoint security, we have established a track record for expanding our platform capabilities with new modules. Through convergence of cybersecurity and data, we intend to bring our customers and prospects a variety of differentiated cybersecurity-first and enhanced data analytics offerings. Having access to some of the world's top cybersecurity and AI talent through our distributed workforce model and our research and development centers across North America, Europe, Middle East, and Asia allows us to continue hiring top technical talent and innovate to maintain our leading position.

- ***Drive new customer acquisition.*** As of January 31, 2023, we had over 10,000 customers, ranging from large enterprises, such as Fortune 500 companies, to small and medium-sized businesses around the world. We intend to continue to add new customers through a product-first approach. This approach enables us to build trusted relationships with a large and rapidly growing group of highly influential managed service and incident response providers, as opposed to creating a dynamic of competition that creates friction between product vendors and service providers. We derive significant customer acquisition benefits from our cloud-delivered platform, which makes it easy to onboard new customers. We are currently certified under the Federal Risk and Authorization Management Program (FedRAMP), and we intend to further grow our footprint within the U.S. federal government. We intend to continue to build our relationships with our channel partners, including MSPs, MSSPs, MDRs, OEMs, and IR firms, as well as our alliance partners to expand our market reach.

- ***Increase adoption within our customer base.*** We have been successful in our ability to grow revenue from our customer base as they deploy additional endpoints and expand the use of our platform. As we enhance our platform functionality and value proposition, we expect many of our customers to adopt additional platform functionalities and Singularity modules to address all of their cybersecurity use cases through the same platform and agent. Our customers can seamlessly activate additional modules to expand platform capabilities through the already deployed agent. Module driven growth has been broad-based with notable strength from our cloud and data modules. This enables us to show in-product promotions and trials and to

drive the expansion of our Singularity Modules. The success of our land-and-expand strategy is evidenced by our greater than 130% dollar-based net retention rate as of January 31, 2023.

- ***Expand our global footprint.*** Revenue generated outside of the United States was 35% for fiscal 2023, compared to 32% for fiscal 2022. We intend to continue to grow our international customer base by increasing our investments in international operations. We are continuing to invest and hire talent to expand our business in Asia-Pacific and Europe, the Middle East and Africa, and Latin America.

- ***Expand our total addressable market through acquisitions.*** We evaluate acquisition prospects that align with our platform, customers, and strategic market opportunities. We intend to use these opportunities to extend the reach of our Singularity Platform into adjacencies that complement our core offerings. For example, in May 2022, we acquired Attivo Networks, Inc. (Attivo), a leading identity security and lateral movement protection company, which allowed us to deliver comprehensive identity security as part of our Singularity platform. In addition, through S Ventures, a $100 million fund that we announced in 2022 to invest in next generation category-defining security and data companies, we are able to further enhance our platform capabilities in areas that may be of future interest to us. We are committed to innovation, automation, and securing data wherever it resides with a front-row seat into cutting-edge cybersecurity technologies.

Our Singularity Platform

Our Singularity Platform delivers AI-powered autonomous threat prevention, detection, and response capabilities across an organization's endpoints and cloud workloads, enabling seamless and automatic protection against a full spectrum of cyber threats. We built our platform to be deployed as a cloud service or in private and hybrid clouds.

Our platform capabilities are connected through three key patented technologies:

- ***Data Analytics.*** Our data analytics technology can ingest, correlate, and query petabytes of structured and unstructured data from disparate external and internal sources at machine speed.

- ***AI.*** Our Static, Behavioral, and Streaming AI technologies that run in a distributed manner on our data cloud as well as on every endpoint and every cloud workload we protect.

- ***Storyline.*** Our Storyline technology builds a model of real-time running processes and their behaviors, to create rich, contextual data narratives which become the input to our Behavioral AI model. Storyline powers our unified Endpoint Protection Platform (EPP), EDR, or XDR functionalities. Storyline is the foundation of our EPP while providing unprecedented levels of visibility with contextual information for benign and malicious processes. We extend our fundamental protection, visibility and response capabilities well beyond the endpoint to cloud, and third-party solutions in our Singularity Platform. We designed our platform based on our "design to delight" principle and developed a powerful yet simple and intuitive user experience.

Proprietary Security Data Lake

Dataset is our fully integrated security data lake that seamlessly fuses together the data, access, control, and integration planes of EPP, EDR, Cloud Workload Protection (CWP), Identity Protection, and IoT security into a centralized platform. With our Singularity Platform, enterprises gain access to their security data from multiple sources through a single pane of glass. It was designed with the goal of optimizing scale, cost and performance - what we call the Golden Ratio of Big Data. This is achieved by the use of innovative data structures, storage systems, and algorithms:

- ***Ingest.*** Our platform is able to ingest structured and unstructured data from any source, with little to no manual configuration and at unprecedented speed and scale.

- ***Normalize***. Aligns every data point to extract the shared elements regardless of origin and to produce true insights.

- ***Correlate.*** We correlate events from multiple sources into Storylines which contains event data, both benign and malicious, in a context-rich format for easy understanding.

- ***Analyze.*** Our Singularity Platform enriches and visualizes every Storyline with information from Threat Intelligence sources, both homegrown and through integrations with third-party intelligence information services.

Endpoint Protection

Our next-generation cybersecurity technology provides autonomous real-time protection across all operating systems, including Windows, Linux, macOS, and cloud-native and containerized workloads. Our endpoint protection is powered by distributed AI which resides both on devices as well as in the cloud for always-on, machine-speed protection. It is capable of autonomous decision making on the device and stopping threats in milliseconds rather than minutes, hours or even days. We are able to provide superior performance compared to traditional signature-based antivirus tools and earlier next-gen antivirus products with the following three key capabilities:

- ***Static AI.*** Our on-device AI model can detect file-based attacks, even those that are previously unknown zero-day exploits, with extreme precision in milliseconds. Our Static AI model is the output of a supervised machine learning cycle that is trained on a continuously evolving data set from billions of files coupled with the data from multiple threat intelligence sources, including our proprietary Embedded Threat Intelligence.

- ***Behavioral AI.*** Our on-device AI model continuously scores Storylines from the device to precisely classify individual or group behaviors as benign or malicious. The accuracy of our Behavioral AI is powered by the rich contextual information that is encoded in each Storyline that is being scored. As a result, it is attack vector agnostic because it is not limited to any particular pathway used by attackers to penetrate a system, such as zero-day vulnerability exploits and living off the land attacks.

- ***Embedded Threat Intelligence.*** Our cloud threat intelligence system combines threat information from our data analytics and research teams, Vigilance MDR and IR services, and other commercial and proprietary threat feeds.

Endpoint Detection and Response

Unlike first-generation EDR products that are reactive and mainly focused on collecting data, our ActiveEDR solutions leverage Storylines to reduce analysis time and to automate response actions by significantly minimizing the time between detection and response through technology automation. It enables on-device behavioral analysis, auto-remediation, and response in a fully autonomous fashion. ActiveEDR reduces analysis time and requirements for specialized skills by providing technology-generated context which would otherwise need to be produced by highly skilled people manually in a time-intensive and error prone fashion. ActiveEDR excels at visualizing context, pinpointing anomalies, and providing a variety of granular responses. The main capabilities of ActiveEDR are:

- ***Deep Visibility Threat Hunting.*** Deep Visibility Threat Hunting provides an easy-to-use search interface on top of our Deep Visibility dataset. The Storylines shown within Deep Visibility hunts enable one-click responses, which are far easier and faster to execute than manually scripting responses. As a result, both entry level analysts and highly skilled analysts can analyze results faster, review more alerts, and be more productive with the power of technology.

- ***Response Capabilities*.** Our Singularity Platform offers one of the broadest sets of response actions in the EDR market. Leveraging Storylines, we automate responses or make them optionally initiated by operators. Our response capabilities enable security analyst to *Kill*, *Quarantine*, *Remediate*, *Remote Shell, and Rollback.*

Multi-tenancy Architecture

We offer complete multi-tenancy with four tiers— Global, Account, Site, and Group. Policies set at the higher tier of the hierarchy are automatically inherited by the lower levels, but administrators may override them to create local policies at any tier. We also support fully customizable Role Based Access Control (RBAC), that allows organizations to create specific rules controlling console permissions at a granular level. This enables large, distributed teams to work independently while at the same time providing a global view for the CISO and other stakeholders. It further enables our platform adoption by the world's largest organizations, MSPs, MSSPs, MDRs, OEMs, and IR firms.

XDR Integrations

Singularity XDR unifies and extends detection, investigation, and response capability across the entire enterprise, providing security teams with centralized end-to-end enterprise visibility, powerful analytics, and automated responses across the technology stack. This empowers security teams to see data collected by disparate security solutions from all platforms, including endpoints, cloud workloads, network devices, email, identity, and more, within a single dashboard. It enables customers to seamlessly extend the power of the Singularity Platform across the entire IT stack—regardless of vendor—to automate response actions. Our XDR integrations give customers the flexibility to operate our platform as a platform-as-a-service in their own customized graphical user interface and workflows simply by leveraging our robust, well-documented and easy-to-use APIs.

IT and Security Operations

Our Singularity Platform enables security and IT teams to identify vulnerabilities, fix insecure configurations, and manage endpoints. Vulnerable and mis-configured applications make it easier for attackers to gain entry and evade detection. Addressing these vulnerabilities and mis-configured settings strengthens the security risk profile of our customers. Our platform has the following capabilities:

- ***Application Inventory*.** Maintains a software application inventory across an entire organization, by capturing the list of installed applications and their attributes such as their version numbers, install date, and publisher. Our software collects this information in real-time, enabling our customers to easily search and sort through these attributes in a global application inventory view within the console. Customers can quickly perform software frequency analysis and compliance checks.

- ***Scanless Vulnerability Assessment*.** Using our real-time organization-wide Application Inventory database, our solution is able to provide highly accurate and dynamic Vulnerability Management information without the need to deploy another solution. We do so by matching version information from our Application Inventory database to the known vulnerabilities published as Common Vulnerability Enumeration records.

- ***Device Control.*** Allows maximum granularity and flexibility when defining Device Control policies to prevent data exfiltration and malware entry. Our Device Control module supports two main media types: USB and Bluetooth devices. Our Bluetooth Device Control capability augments our IoT capability, limiting pairing with unsanctioned hardware and other wearable devices. We believe the ability to provide granular control for Bluetooth devices in conjunction with other forms of USB media is a competitive differentiator.

- ***Native OS Host Firewall Control*.** Leverages native operating system infrastructure to provide an application-aware and location-aware endpoint firewall orchestrator for remote devices. Firewall control provides visibility, malware prevention, and network segmentation by utilizing the native firewall capabilities on Windows, macOS, and Linux devices. With our Singularity Platform, we enable our users to keep their workforce protected, segment their networks, and block traffic from malicious IPs/C2 servers using the same console that they use to monitor threats.

- ***File Integrity Monitoring.*** The data collected by our Deep Visibility EDR can be used to replace traditional file integrity monitoring solutions. Coupled with Storyline Active Response (STAR), our File Integrity solution (FIM) is able to automatically alert or remediate unauthorized changes to these files. Organizations use this to be compliant with PCI DSS and other regulatory requirements while eliminating other agents, products, and spend.

Singularity Platform Tiers

Our Singularity Platform offers a highly flexible deployment model. It is primarily hosted in Amazon Web Services (AWS) in multiple regions - North America, European Union, Asia Pacific, and AWS GovCloud. We also support deploying our platform in Google Cloud as well as customers' on-premise data centers, private, and hybrid cloud environments for organizations with specialized hosting and data sovereignty needs.

Our Singularity Platform provides feature parity across Windows, macOS, and Linux. It provides customers with full flexibility through a multi-tier offering priced on a per agent basis, which generally corresponds with an endpoint, server, virtual machine, or host. The tiers of our Singularity Platform include:

- ***Singularity Core.*** Our entry level security solution for organizations that want to replace antivirus tools with our EPP which we believe is more effective and easier to manage than legacy antivirus and next-gen antivirus products. Singularity Core includes our Static and Behavioral AI models and autonomous threat response and rollback features.
- ***Singularity Control.*** Made for organizations seeking best-of-breed security with the addition of our "security suite" features for endpoint management. It provides additional features for control network connectivity, USB and Bluetooth peripherals, and to uncover rogue devices.
- ***Singularity Complete.*** Our flagship offering that includes a comprehensive suite of product capabilities.

Singularity Platform Modules

We further offer customers a broad set of capabilities through our Singularity Modules. We price our modules as a subscription on a per agent basis. Our most notable modules include:

Cloud Security

Our Cloud Workload Protection (CWP) solution extends distributed, autonomous endpoint protection, detection, and response to compute workloads running in public clouds, private clouds, and on-prem data centers. Our runtime protection delivers prevention, detection, response and hunting functionalities purpose-built for these environments. We offer full-fledged EPP and EDR for servers, virtual machines, and containerized workloads. Our Cloud Application Control locks down the running image of servers and containers to prevent configuration drift and protect against unauthorized changes, in line with best practices for cloud workload security.

Identity Protection

Our identity security portfolio acts as a force multipliers for security teams, allowing them to assume a more robust security posture and extend the capabilities of the Singularity Platform to protect user credentials. Our Singularity Identity solution detects and responds to identity-based attacks and finds attackers early, before they can exploit identities. Our identity solution also reduces the potential attack surface and proactively increases security by identifying misconfigurations and credential exposures that create attack paths for attackers to move laterally. Our identity security portfolio includes:

- ***Singularity Identity*** detects real-time identity attacks across the enterprise that target Active Directory and Active Directory (Azure AD). It delivers holistic identity threat detection and response including credential theft, privilege escalation, lateral movement, data cloaking, identity exposure, and more for zero trust cybersecurity.

- ***Singularity Ranger Active Directory*** uncovers vulnerabilities in Active Directory and Azure AD with a cloud-delivered, continuous identity assessment solution. It provides instant Active Directory visibility of misconfigurations, suspicious password changes, credential harvesting, unauthorized access, and more.

- ***Singularity Hologram*** lures network and insider threat actors into revealing themselves. Through misdirection of the attack with tactics including breadcrumbs and decoy accounts, files and IPs, organizations gain the advantage of time to detect, analyze, and stop an attacker without impacting enterprise assets.

Attack Surface Management

Our Ranger module enables control of the enterprise network attack surface in real time by discovering, identifying, and containing any device-based threat. Ranger leverages the presence of our software in an organization's network to track assets, create an Enterprise Asset Map, perform network segmentation, deploy our agents to unprotected devices, and provide risk scores. Ranger provides organization-wide inventory and control of IoT devices by discovering connected devices, including virtual machines, containers, and IoT devices such as printers, smart TVs, and thermostats. Ranger has four key component features:

- ***Rogue Discovery*****.** Enables administrators to identify unprotected or "rogue assets" and verifies our agent is installed on all corporate assets.

- ***Ranger Insight*****.** Provides a clear picture of the inventory and risk in the IoT environment, including open ports, header and application versions, and vulnerability information,

- ***Rogue Control*****.** Creates network segments to restrict access to a corporate network. Rogue Control prevents unsanctioned devices, such as guest machines, from connecting to authorized networks.

- ***Ranger Auto-Deploy*****.** Rapidly deploys our agents using service credentials to unprotected endpoints with no additional IT infrastructure or software. Auto-Deploy provides security teams with complete, instant asset coverage.

Mobile Endpoint Security

Our Singularity Mobile module enables customers to manage mobile devices through behavioral AI-driven protection, detection, and response directly for iOS, Android, and ChromeOS devices. It delivers mobile threat defense that is local, adaptive, and real-time, to thwart mobile malware and phishing attacks at the device, with or without a cloud connection. It is the industry's leading on-device behavioral AI product that dynamically detects never before seen malware, phishing, exploits, and man-in-the-middle attacks. Singularity Mobile provides security and data privacy to support zero trust.

XDR Power Tools

Our Singularity XDR Power Tools modules complement and extend Singularity EDR & XDR capabilities for organizations seeking advanced investigative workflows and a long, retrospective look back to support comprehensive incident response. These modules include:

- ***Binary Vault*****.** Enables customers to store and download copies of any file that has been executed in their environment for forensic review and reverse engineering. Binary Vault can store a copy of every known binary, both benign and malicious, that executes across an enterprise. This enables advanced security analysts to download a copy of any file that has been executed in their environment for forensic review and reverse engineering, and provides them with access to a broader dataset and more complete lookback capabilities than any of our competitors.

- ***Remote Script Orchestration (RSO)*****.** Enables enterprises and incident responders to investigate and respond to threats on multiple endpoints across the organization remotely, enabling them to easily manage their entire fleet. In incident response situations, rapid artifact extraction and endpoint state querying across the entire enterprise is critical. Our remote script orchestration module allows concurrent execution of

custom and preset scripts across an enterprise, instead of having to triage with a device by device approach. By converging our protection, detection, and response capabilities with remote script orchestration, our platform is the only solution that is needed to respond to a breach.

- ***Storyline Active Response (STAR).*** STAR gives users the capability to set custom Indicators of Compromise (IOC) based rules for real-time analysis, alerting, and automatic response workflows. Our STAR module is also capable of ingesting threat intelligence feeds to enhance and correlate analyses. The STAR module uses Streaming AI technology to match billions of events to tens of millions of IOCs at the time of ingestion. STAR is a threat hunting and workflow orchestration force multiplier. Without STAR, it is difficult for security analysts to keep pace with the number and complexity of emerging threats from an EDR perspective.

- ***Data Retention.*** Offers data retention from one month to three years and beyond. Modern attacks can take days and weeks to initiate after infiltration. Therefore, it is critical for an EDR solution to provide visibility for extended periods of time. This enhances both retrospective analysis and proactive hunting measures. Our platform has been designed and built to support extended data retention to time periods that far exceed what others are able to offer, and we do so on a cost-efficient basis due to our data retention architecture. We offer data retention for up to three years to provide maximum value from our Deep Visibility Threat Hunting module.

- ***Cloud Funnel.*** Allows organizations to export their XDR data in real-time to their private data lakes, whether locally-hosted or in the cloud. It securely streams a copy of all endpoint EDR telemetry to a customer's local data lake for further correlation with other security tools, while allowing offline data storage for audit and compliance.

WatchTower

WatchTower delivers threat hunting and insights to help customers understand the nature of threats, targeted attacks, threat actors, and risk reduction. It provides intelligence-driven, cross-platform threat hunting to help customers adapt to the modern threat landscape through visibility and actionability to novel attacker techniques, global APT, campaigns, and emerging cybercrimes. As we track threat actors globally, WatchTower parses, consolidates, and contextualizes threat intelligence sources and hunts for threats in our customers' environments. WatchTower distills intelligence down to its most valuable insights, such as a summary bulletin of the threat, its impact on our customers' organizations, and how the threat can be addressed.

Vigilance MDR

Vigilance MDR leverages the expertise of our in-house security analysts to review, act upon, and document every threat that our Singularity Platform autonomously identifies. It adds a human lens to cybersecurity understanding and augments our customers' in-house security teams. Due to the autonomous nature of our Singularity Platform, Vigilance MDR provides rapid response times to threats. Our technology-powered digital forensics analysis and incident response offering takes Vigilance MDR two steps further and provides customers with a full-service solution and enables customers to benefit from world-class SOC operations with customized threat annotation and response. Vigilance MDR helps customers of all sizes augment their cybersecurity staff with a 24/7/365 globally-distributed operation which operates under the industry's only publicly available Service Level Agreements.

DataSet Platform

Building upon the acquisition of Scalyr, Inc., we launched DataSet, a revolutionary live enterprise data platform for data queries, analytics, insights, and retention. DataSet expands our capabilities beyond cybersecurity use cases, such as data analytics. DataSet takes a security-first perspective to data analytics. It is a cloud-native flexible enterprise data platform built for all types of data live or historical, at petabyte scale. By eliminating data schema requirements from the ingestion process and index limitations from querying, DataSet can process massive amounts of live data in real time, delivering log management, data analytics, and alerting with unparalleled speed, performance, and efficiency built on a security and privacy-first foundation.

As a software as a service (SaaS) platform, it can be deployed in minutes and is easy to operate without any maintenance requirement. DataSet is built for the cloud and offered as a cloud service freeing up engineering resources from managing data refineries. DataSet is built with the security and controls that enterprises require for their most precious asset: data.

Our Customers

As of January 31, 2023, we had over 10,000 customers using our Singularity Platform in approximately 80 countries. We are protecting the digital infrastructures of thousands of customers around the world, including large global enterprises, small and medium sized businesses, and government organizations. Our business does not depend on any single end customer. For a definition of customer, see the section titled "Management's Discussion and Analysis of Financial Condition and Results of Operations—Key Business Metrics—Customers with ARR of $100,000 or More."

Seasonality

We experience seasonal fluctuations in our financial results due to the annual budget approval process of many of our customers. We typically receive a higher percentage of our annual orders from new customers, as well as renewal orders from existing customers, in our fourth fiscal quarter as compared to other quarters due to the annual budget approval process of many of our customers.

Human Capital Resources

Our Team

As of January 31, 2023, we had over 2,100 full-time employees worldwide. We also engage temporary employees and consultants as needed to support our operations.

Our U.S.-based employees include team members in all key functions, including go-to-market, customer success, technology, product, and support. Each of our U.S. offices has a different functional focus but share a driven, customer-centric culture. Our headquarters in Mountain View, California is where the majority of our executive team, marketing, finance, legal, people and talent, and sales operations is located, which supports cross functional collaboration. Our office in Eugene, Oregon hosts our North American customer success and support team, as well as our sales development and inside sales teams. Having these teams together supports a highly collaborative and customer-focused site.

Our office in Tel Aviv, Israel benefits from Israel's concentration of cybersecurity experts. This team draws from a deep pool of Israeli military cybersecurity and intelligence experts, product mavens, and general technical talent. Our office in Prague, Czech Republic houses research and product development functions to augment current teams across the globe and the expansion of our global engineering organization.

Our European head office is in Amsterdam, Netherlands, which we chose for its talent pool, language versatility, diversity, labor and tax laws, and central location in relation to our offices in the United States and Israel.

Our Dubai office is primarily focused on go-to-market activities in the Middle East and Africa and supports our new business efforts in connecting with both customers and partners across these regions.

Our Bangalore, India office houses engineering talent as well as supportive functions across general, administrative and go-to-market. The economic climate in India continues to expand with endless potential. We are excited to continue our investment across this beautiful country.

None of our employees are represented by a labor union or are a party to a collective bargaining arrangement. We have not experienced any work stoppages and we believe that our employee relations are strong.

Our Culture

Our mission is to Secure Tomorrow™ and our purpose is to be a Force for Good. Our core values are at the foundation of our equitable culture and guide our approach on how we build and grow our business with all stakeholders:

- *Trust*. Be dependable. Conduct yourself with the highest integrity at all times.
- *Accountability*. Be reliable in all your actions and words. Put customers first. Be the owner.
- *OneSentinel*. Be passionate about driving team success and collaboration across our company.
- *Relentlessness*. Act with unwavering purpose and determination in everything you do.
- *Ingenuity*. Encourage innovative approaches to problem-solving and market leadership. Embrace diverse perspectives. Hustle.
- *Community*. Be kind to one another. Think about how your actions will affect others. Together.

Our Employee Value Proposition was designed using feedback from employees around the globe. It is our promise to all Sentinels and candidates on what to expect while working at SentinelOne. *Here you will drive innovation*, pushing the boundaries of cybersecurity to determine what's next. *Here you will build your future*, with amazing benefits and tools to grow. *Here you will enjoy your work*, in a culture that is built on equity, integrity and autonomous action.

We value transparent and respectful communication as key components of our continuous feedback culture, something that we view as a key driver of our business success. We benefit from the varied perspectives that come from our global workforce. We believe in the strengths of diversity and are committed to building out a diverse talent base. We plan to continue investing in hiring employees both in and outside of the United States.

We received multiple workplace accolades in 2022.

- Fortune recognized the company as a Best Workplace in Technology, Best Medium Workplace, Best Workplace for Millennials, and Best Workplace in the Bay Area.
- Dun's 100 list acknowledged SentinelOne as one of the Best High Tech Companies to Work for and one of the Top 10 High Tech Companies to Work for Parents in 2022.
- SentinelOne also achieved Great Place to Work certification for the USA, UK, France, India, and Netherlands in 2022.
- Comparably awarded SentinelOne with 14 distinctions in 2022, including Best Company for Diversity, Best Company for Women, Best CEO, Best Company Perks & Benefits, Best Company Compensation, Happiest Employees, Best Career Growth, Best CEOs for Diversity, Best CEOs for Women, Best Sales Team, Best Engineering Team, Best Places to Work in the Bay Area, Best Global Culture, and Best Company Outlook.

Our presence and engagement across all social media platforms continues to grow rapidly, a reflection of the market's perception of us and our leadership as innovators in the cybersecurity space. We pride ourselves on offering employees an award-winning culture centered around trust and integrity, as together, we work to defeat every cyberattack with autonomous technology.

Retention and Talent Development

We believe that motivating and retaining talent at all levels is vital to our success. Our compensation and benefits program is intended to anticipate and meet the needs of our employees. In addition to base salary, these programs, which vary by country and region, include bi-annual bonuses, equity awards, an employee stock purchase plan, a 401(k) plan, including a 401(k) match in the United States, healthcare and insurance benefits, health savings

and flexible spending accounts, unlimited vacation, wellness reimbursement, 16 weeks of gender-neutral parental leave and more. We have increased our investment in training and development and have rolled out several key programs as well as enabling our employees to access over 1,000 on demand webinars in technical and soft skills areas.

Since the COVID-19 pandemic, we continue to globally align our benefits to focus on business continuity and employee well-being. We have been very intentional with our efforts to support employees while working from home and in their return to the office. Further, we have enhanced and promoted programs to support employees' physical and mental health and well-being. We have built a company that we believe thrives whether our employees are in offices or remote.

Diversity, Equity and Inclusion

We aim to cultivate and foster an inclusive workplace that is diverse, equitable, and inclusive, where Sentinels can fulfill their potential. We have developed a SentinelOne Diversity, Equity and Inclusion (DEI) framework that includes a commitment statement and a three-year roadmap focused on moving towards our long term DEI goals. We also have five key pillars to support our DEI initiatives.

- Diversifying our talent pipeline including targeting hiring diverse slates across key functional areas and targeting underrepresented groups through our University Recruiting program.
- Amplifying the power of communities through our Inclusion Networks including Women's Inclusion Network, WIN@sentinelone; Black Inclusion Network, BLK@sentinelone; Pride Inclusion Network, Out@sentinelone; Latino Inclusion Network, Latinos@sentinelone and Veteran's Inclusion Network, Served@sentinelone.
- Holding ourselves accountable through data and insights and publishing a DEI dashboard.
- Creating an equitable culture for all through strategic partnerships including Women in Cybersecurity (WiCys). Through the S Foundation, we offer grants and scholarships to organizations within our communities. And we have established partnerships that support and advocate for underrepresented groups in the workforce.
- Hearing all voices through our internal celebrations including Black History Month, Women's History Month, Pride, and Hispanic Heritage Month. In addition, MentorOne program provides Sentinels the opportunity to mentor and be mentored to develop professionally.

Research and Development

Our research and development organization is responsible for the design, development, testing, and delivery of new technologies, features and integrations of our platform, as well as the continued improvement and iteration of our existing products. It is also responsible for operating and scaling our platform including its underlying infrastructure. Our most significant investments are in research and development to drive core technology innovation and bring new products to market. Research and development employees are located primarily in our Israel, India, and the Czech Republic offices, and remotely.

We have a proven team that constantly works to expand our market, customer and user reach and impact with new, innovative products. We intend to continue to invest in our research and development capabilities to extend our platform and products.

Our Go-To-Market Strategy

Our sales and marketing organizations partner to create brand awareness, drive demand, and develop customer relationships to deliver strong sales pipeline coverage and revenue growth.

Sales

We sell subscriptions to our Singularity Platform through our direct sales team, which is composed of field sales and inside sales professionals. Our sales team leverages our global network of channel and alliance partners for prospect access and fulfillment. For specific market segments, our channel partners independently manage the complete sales cycle resulting in a highly scaled and leveraged sales experience. Our sales team also identifies existing customers who may be interested in free trials of additional platform modules, which serves as a powerful driver of our "land and expand" growth model. Through segmenting our sales teams by customer size, we can deploy an efficient and scalable sales model which enables rapid prospect engagement, thorough technology evaluations, and yields lasting customer relationships.

Marketing

Our marketing organization is focused on building our brand reputation, increasing the awareness of our platform, and driving prospect and customer demand. To support these efforts, we deliver broad based brand campaigns to build awareness of our solutions and our company. We also deliver targeted and situational content to demonstrate thought leadership in the security industry, including speaking engagements with the security industry's foremost organizations to provide expert advice, educating the public about the cyber threats, and identifying threat research discoveries that illustrate the business outcomes and differentiation of our solution. We engage in paid media, web marketing, out of home media advertising, industry and trade conferences, analyst engagements, producing whitepapers, demand generation via digital and web, telemarketing, and targeted displacement campaigns. We employ a wide range of digital programs, including search engine marketing, online and social media initiatives, and content syndication to increase traffic to our website and encourage new customers to free trials of our Singularity Platform. Additionally, we engage in joint marketing activities with our channel and alliance partners. Over the past several years, we have experienced significant increases in our brand relevance as demonstrated by coverage in leading global press, analyst publications, website traffic, web demo requests, and channel partner engagement.

Partnership Ecosystem

We work with a number of partners to create "better together" technology solutions for mutual customers, many of which we then leverage in joint go-to-market strategies. These partnerships include many of the leading ISVs, alliance partners, MSPs, MSSPs, MDRs, OEMs, and IR firms. We provide our partners with our differentiated technology and platform to enable them to provide the best security service to their own customers.

Our Singularity Platform offers our partners complete multi-tenancy and a superior level of management capability and flexibility with tiering, policy inheritance, and customizable role-based access control from the same console. Our data model and open architecture enable our partners to rapidly build and innovate across a wide range of use cases and deliver their products on top of our technology. As such, our partners are not our competitors but instead, act as force multipliers for our go-to-market investments.

Our partner integrations deliver more secure solutions and an improved end user experience to their customers. Our ISV and alliance partnerships focus on security analytics, network and infrastructure security, threat platforms and orchestration, automation, and other mainstream technology integrations.

Singularity Marketplace

Singularity Marketplace is an open application ecosystem that enables customers to seamlessly integrate dozens of applications. Organizations can gain visibility over data across historically disparate security solutions without the need for custom business logic, coding or complex configuration. Organizations can integrate any security applications and tools regard-less of vendor into a single platform without coding or scripting required. Singularity Marketplace extends the power of our platform across the entire security and IT stack to build an effective threat defense posture with layered security, collaborative processes, and integrated products.

Singularity Marketplace enables security teams to converge on a single pane-of-glass for extended detection and response workflows to minimize context switching and distractions during triage and incident response. It helps

them gain insights from shared security events without requiring a massive time investment in custom business logic, code, and complex configuration. It allows security teams to drive a unified, orchestrated response among security tools in different domains.

Competition

The market for our solutions is competitive and characterized by an evolving IT environment, customer requirements, industry standards and by frequent new product and service offerings and improvements. We compete with an array of established and emerging security solution vendors.

Our competitors include the following:

- endpoint security providers, such as CrowdStrike Holdings, Inc. (CrowdStrike) and VMware, Inc. (VMware);
- legacy antivirus providers such as Trellix (formerly McAfee Corp.), Symantec (a subsidiary of Broadcom, Inc.) (Symantec), and Microsoft Corporation (Microsoft); and
- providers of general network security products and services who offer a broad portfolio of solutions, such as Palo Alto Networks, Inc. (Palo Alto Networks)

We compete on the basis of a number of factors, including but not limited to our:

- ability of our technology to detect, prevent, and block threats;
- breadth of our functionality;
- ability to automate threat prevention and remediation with limited human intervention;
- performance of our platform;
- speed of our threat hunting capabilities;
- support for cloud, hybrid, and on-premise deployments;
- support for various operating systems;
- platform data retention capabilities;
- ability to integrate with other participants in the security ecosystem;
- ease of use to deploy, manage, and maintain our platform;
- quality of our MDR service;
- strength of sales, marketing, and channel partner relationships; and
- customer support.

Although certain of our competitors enjoy greater brand awareness and recognition, deep customer relationships, and larger existing customer bases, we believe that we compete favorably with respect to our autonomous and AI-powered threat prevention, detection, response, and hunting capabilities.

Intellectual Property

The protection of our technology and intellectual property is an important aspect of our business. We rely upon a combination of trademarks, trade secrets, know-how, copyrights, patents, confidentiality procedures, contractual commitments, domain names, and other legal rights to establish and protect our intellectual property. We generally enter into confidentiality agreements and invention or work product assignment agreements with our officers,

employees, agents, contractors, and business partners to control access to, and clarify ownership of, our proprietary information.

As of January 31, 2023, we had 48 issued patents and 29 pending patent applications in the United States and abroad. These patents and patent applications seek to protect our proprietary inventions relevant to our business. These issued patents are scheduled to expire on or around the years between 2033 and 2041 and cover various aspects of our platform and technology.

As of January 31, 2023, we had 7 trademark registrations in the United States, including registrations for "SentinelOne" and our logo. We also had 74 trademark registrations and applications in certain foreign jurisdictions. Additionally, we are the registered holder of a number of domain names, including sentinelone.com and dataset.com.

Government Regulation

We are subject to many varying laws and regulations in the United States, the United Kingdom, the European Union and throughout the world, including those related to privacy, data protection, intellectual property, consumer protection, marketing, advertising, employment and labor, competition, customs and international trade, taxation, and more. As we grow and expand our geographical reach, we may become subject to additional regulations in the United States and internationally.

These laws often require companies to implement specific information security controls to protect certain types of information, such as personal data. These laws and regulations are constantly evolving and may be interpreted, applied, created, or amended in a manner that could harm our current or future business. Our compliance with these laws and regulations may be onerous and could, individually or in the aggregate, increase our cost of doing business, impact our competitive position relative to our peers, and/or otherwise adversely affect our business, reputation, operating results and financial condition. However we believe we are currently in material compliance with such laws and regulations to which we are subject and do not currently expect continued compliance to have a material impact on our capital expenditures, earnings, or competitive position. See the section titled "Risk Factors" for additional information about the laws and regulations we are subject to and the risks of our business associated with such laws and regulations.

Corporate Information

We were incorporated in the State of Delaware as Sentinel Labs, Inc. in January 2013. We changed our name to SentinelOne, Inc. in March 2021. Our principal executive offices are located at 444 Castro Street, Suite 400, Mountain View, California 94041. Our telephone number is (855) 868-3733. We completed our initial public offering (IPO) of shares of our Class A common stock in July 2021.

SentinelOne, the SentinelOne logo, and other registered or common law trade names, trademarks, or service marks of SentinelOne appearing in this prospectus are the property of SentinelOne. This prospectus contains additional trade names, trademarks, and service marks of ours and of other companies. We do not intend our use or display of other companies' trade names, trademarks, or service marks to imply a relationship with these other companies, or endorsement or sponsorship of us by these other companies. Other trademarks appearing in this prospectus are the property of their respective holders. Solely for convenience, our trademarks and trade names referred to in this prospectus appear without the ® and ™ symbols, but those references are not intended to indicate, in any way, that we will not assert, to the fullest extent under applicable law, our rights, or the right of the applicable licensor, to these trademarks and trade names.

Available Information

We file electronically with the SEC our Annual Report on Form 10-K, Definitive Proxy Statements on Schedule 14A, Quarterly Reports on Form 10-Q, Current Reports on Form 8-K, and amendments to reports filed or furnished pursuant to Section 13(a) or 15(d) of the Exchange Act. The SEC maintains a website at www.sec.gov that contains reports, proxy and information statements and other information that we file with the SEC electronically. We will

make available on our website at www.sentinelone.com, free of charge, copies of these reports and other information as soon as reasonably practicable after we electronically file such material with, or furnish it to, the SEC.

We use our investor relations page on our website (www.sentinelone.com), press releases, public conference calls, public webcasts, our Twitter account (@SentinelOne), our Facebook page, and our LinkedIn page as means of disclosing material non-public information and for complying with our disclosure obligations under Regulation FD. The information disclosed by the foregoing channels could be deemed to be material information. As such, we encourage investors, the media, and others to follow the channels listed above and to review the information disclosed through such channels. Any updates to the list of disclosure channels through which we will announce information will be posted on the investor relations page on our website.

The contents of the websites referred to above are not incorporated into this filing. Further, our references to the URLs for these websites are intended to be inactive textual references only.

ITEM 1A. RISK FACTORS

Investing in our Class A common stock involves a high degree of risk. You should carefully consider the risks and uncertainties described below, together with all of the other information in this Annual Report on Form 10-K, including the section titled "Management's Discussion and Analysis of Financial Condition and Results of Operations," and our consolidated financial statements and the accompanying notes included before making a decision to invest in our Class A common stock. Our business, financial condition, operating results, or prospects could also be adversely affected by risks and uncertainties that are not presently known to us or that we currently believe are not material. If any of the risks actually occur, our business, financial condition, operating results, and prospects could be adversely affected. In that event, the market price of our Class A common stock could decline, and you could lose all or part of your investment.

Summary Risk Factors

Our business is subject to numerous risks and uncertainties, including those risks more fully described below. These risks include, among others, the following, which we consider our most material risks:

Risks Related to Our Business and Industry

- We have a limited operating history, which makes it difficult to evaluate our current business and future prospects and increases the risks associated with your investment.
- We have a history of losses, anticipate increases in our operating expenses in the future, and may not achieve or sustain profitability. If we cannot achieve and sustain profitability, our business, operating results, and financial condition will be adversely affected.
- We face intense competition and could lose market share to our competitors, which would adversely affect our business, operating results, and financial condition.
- Our operating results may fluctuate significantly, which could make our future results difficult to predict and could cause our operating results to fall below expectations.
- Adverse economic conditions or reduced information technology spending could adversely affect our business, operating results and financial condition.
- A network or data security incident against us, whether actual, alleged, or perceived, would harm our reputation, create liability, and regulatory exposure, and adversely affect our business, operating results, and financial condition.
- Defects, errors, or vulnerabilities in our platform, the failure of our platform to block malware or prevent a security breach, misuse of our platform, or risks of product liability claims would harm our reputation and adversely affect our business, operating results, and financial condition.

- Existing and future acquisitions, strategic investments, partnerships or alliances could be difficult to identify and integrate, divert the attention of key management personnel, disrupt our business, dilute stockholder value and adversely affect our business, operating results, and financial condition.
- If we are unable to retain our customers, renew and expand our relationships with them, and add new customers, we may not be able to sustain revenue growth, and we may not achieve or maintain profitability in the future.

- If our platform is not effectively interoperated within our customers' IT infrastructure, deployments could be delayed or canceled, which would adversely affect our business, operating results, and financial condition.
- Disruptions or other business interruptions that affect the availability of our platform could adversely affect our customer relationships and overall business.
- We may not be able to timely and cost-effectively scale and adapt our existing technology to meet our customers' performance and other requirements.
- If we are unable to maintain successful relationships with our channel partners and alliance partners, or if our channel partners or alliance partners fail to perform, our ability to market, sell and distribute our platform will be limited, and our business, operating results, and financial condition will be harmed.

Risks Related to Regulatory Matters

- If we fail to adequately protect personal information or other information we collect, process, share, or maintain under applicable laws, our business, operating results, and financial condition could be adversely affected.

Risks Related to Our People

- We rely on our management team and other key employees and will need additional personnel to grow our business, and the loss of one or more key employees or our inability to hire, integrate, train, manage, retain, and motivate qualified personnel, including members of our board of directors, could harm our business.

Risks Related to our Intellectual Property

- Our proprietary rights may be difficult to enforce, which could enable others to copy or use aspects of our platform without compensating us.
- Third parties have claimed and may claim in the future that our platform infringes their intellectual property rights and this may create liability for us or otherwise adversely affect our business, operating results and financial condition.

Risks Related to Ownership of Our Class A Common Stock

- The market price of our Class A common stock may be volatile, and you could lose all or part of your investment.
- The dual class structure of our common stock has the effect of concentrating voting control with certain stockholders who held our capital stock prior to the completion of our IPO, including our directors, executive officers, and other beneficial owners who hold in the aggregate approximately 85% of the voting power of our capital stock, which will limit or preclude your ability to influence corporate matters, including the election of directors and the approval of any change of control transaction.

General Risk Factors

- Adverse economic conditions or reduced information technology spending could adversely affect our business, operating results, and financial condition.

Risks Related to Our Business and Industry

We have a limited operating history, which makes it difficult to evaluate our current business and future prospects and increases the risks associated with your investment.

We were founded in January 2013 and released our first endpoint security solution in February 2015. Our limited operating history and financial data may make it difficult to evaluate our current business, future prospects and other trends. We have encountered, and will continue to encounter, risks and uncertainties frequently experienced by growing companies in rapidly changing industries and sectors, such as the risks and uncertainties described herein. Any predictions about our future revenue and expenses may not be as accurate as they would be if we had a longer operating history or operated in a more predictable or established market. If our assumptions regarding these risks and uncertainties are incorrect or change due to fluctuations in our markets or otherwise, or if we do not address these risks successfully, our operating and financial results could differ materially from our expectations and our business and operating results would be adversely affected. We cannot assure you that we will be successful in addressing these and other challenges we may face in the future.

We have a history of losses, anticipate increases in our operating expenses in the future, and may not achieve or sustain profitability. If we cannot achieve and sustain profitability, our business, operating results, and financial condition will be adversely affected.

We have incurred net losses in all periods since our inception, and we may not achieve or maintain profitability in the future. We experienced a net loss of $378.7 million and $271.1 million for the fiscal years ended January 31, 2023 and 2022, respectively. As of January 31, 2023, we had an accumulated deficit of $1,000.4 million. While we have experienced significant growth in revenue in recent periods, we cannot predict when or whether we will reach or maintain profitability. We also expect our operating expenses to increase in the future as we continue to invest for our future growth, including expanding our research and development function to drive further development of our platform, expanding our sales and marketing activities, developing the functionality to expand into adjacent markets, and reaching customers in new geographic locations, which will negatively affect our operating results if our total revenue does not increase. In addition to the anticipated costs to grow our business, we have incurred and expect to continue to incur significant additional legal, accounting, and other expenses as a public company. Our revenue growth is expected to slow or decline and our revenue may decline for a number of other reasons, including reduced demand for our platform, increased competition, a decrease in the growth or reduction in size of our overall market, or if we cannot capitalize on growth opportunities, including acquisitions, new products, services, and feature releases. If we fail to increase our revenue to offset increases in our operating expenses, or manage our costs as we invest in our business, we may not achieve or sustain profitability.

We face intense competition and could lose market share to our competitors, which would adversely affect our business, operating results, and financial condition.

The market for cybersecurity products and services is intensely competitive, fragmented and is rapidly evolving, characterized by changes in technology, customer requirements, industry standards, increasingly sophisticated attackers and by frequent introductions of new or improved products and services. We expect to continue to face intense competition from current competitors, as well as from new entrants into the market. If we are unable to anticipate or react to these challenges, our competitive position could weaken, and we would experience a decline in revenue or reduced revenue growth, and loss of market share that would adversely affect our business, operating results, and financial condition.

Our competitors and potential competitors include the following:

- endpoint security providers, such as CrowdStrike and VMware;
- legacy anti-virus providers such as Trellix, Symantec, and Microsoft; and
- providers of general network security products and services who offer a broad portfolio of solutions, such as Palo Alto Networks.

Our ability to compete effectively depends upon numerous factors, many of which are beyond our control, including, but not limited to:

- our ability to attract and retain new customers, expand our platform or sell additional products and services to our existing customers;
- our ability to attract, train, retain, and motivate talented employees;
- the budgeting cycles, seasonal buying patterns, and purchasing practices of our customers, including any slowdown in technology spending due to U.S. and global macro-economic issues, including global banking and finance related issues, rising interest rates, overall market downturns, inflation, supply chain disruptions, the COVID-19 pandemic or otherwise;
- changes in customer, distributor or reseller requirements or market needs;
- price competition;
- the timing and success of new product and service introductions by us or our competitors or any other change in the competitive landscape of our industry, including consolidation among our competitors or customers and strategic partnerships entered into by and between our competitors;
- changes in our mix of products, subscriptions and services sold, including changes in the average contract length for subscriptions and support;
- our ability to successfully and continuously expand our business domestically and internationally;
- changes in the growth rate of endpoint security, cloud security and overall cybersecurity product platform and services sectors;
- deferral of orders from customers in anticipation of new or enhanced products and services announced by us or our competitors;
- significant security breaches of, technical difficulties with or interruptions to, the use of our platform;
- the timing and costs related to the development or acquisition of technologies or businesses or strategic partnerships;
- our ability to execute, complete or integrate efficiently any acquisitions that we may undertake;
- increased expenses, unforeseen liabilities, or write-downs and any impact on our operating results from any acquisitions we consummate;
- our ability to increase the size and productivity of our distribution channels;
- decisions by potential customers to purchase security solutions from larger, more established security vendors or from their primary network equipment vendors;
- timing of revenue recognition and revenue deferrals;
- insolvency or credit difficulties confronting our customers, which could increase due to U.S. and global macro-economic issues, including global banking and finance related issues, inflation, rising interest rates, market downturns and the effects of the COVID-19 pandemic, which would adversely affect their ability to purchase or pay for our platform, products, and services in a timely manner or at all;
- the cost and potential outcomes of litigation or other proceedings, which could have a material adverse effect on our business;
- future accounting pronouncements or changes in our accounting policies;

- increases or decreases in our expenses caused by fluctuations in foreign currency exchange rates; and
- general macroeconomic conditions, both domestically and in our foreign markets that could impact some or all regions where we operate, including global economic slowdowns, global banking and finance related issues, increased risk of inflation, rising interest rates, labor shortages and potential global recession.

Many of our competitors have greater financial, technical, marketing, sales, and other resources, greater name recognition, longer operating histories, and a larger base of customers than we do. Our competitors may be able to devote greater resources to the development, promotion and sale of their products and services than we can, and they may offer lower pricing than we do or bundle certain competing products and services at lower prices. Our competitors may also have greater resources for research and development of new technologies, customer support and to pursue acquisitions, or they may have other financial, technical, or other resource advantages. Our larger competitors have substantially broader and more diverse product and service offerings and more mature distribution and go-to-market strategies, which allows them to leverage their existing customer and distributor relationships to gain business in a manner that discourages potential customers from purchasing our platform.

Conditions in our market could change rapidly and significantly as a result of technological advancements, including but not limited to increased advancements and proliferation in the use of open artificial intelligence applications, partnering or acquisitions by our competitors or continuing market consolidation. Some of our competitors have recently made or could make acquisitions of businesses or have established cooperative relationships that may allow them to offer more directly competitive and comprehensive products and services than were previously offered and adapt more quickly to new technologies and customer needs. These competitive pressures in our market or our failure to compete effectively may result in price reductions, fewer orders, reduced revenue and gross margin, increased net losses and loss of market share. Even if there is significant demand for endpoint and cloud security solutions like ours, if our competitors include functionality that is, or is perceived to be, equivalent to or better than ours in legacy products that are already generally accepted as necessary components of an organization's IT security architecture, we will have difficulty increasing the market penetration of our platform. Furthermore, even if the functionality offered by other cybersecurity providers is different and more limited than the functionality of our platform, organizations may elect to accept such limited functionality in lieu of purchasing products and services from additional vendors like us. If we are unable to compete successfully, or if competing successfully requires us to take aggressive action with respect to pricing or other actions, our business, financial condition and operating results would be adversely affected.

Our operating results may fluctuate significantly, which could make our future results difficult to predict and could cause our operating results to fall below expectations.

Our operating results have varied significantly from period to period in the past, and we expect that our operating results will continue to vary significantly in the future such that period-to-period comparisons of our operating results may not be meaningful. This could adversely affect our business, operating results, and financial condition. Accordingly, our financial results in any one quarter should not be relied upon as indicative of future performance. Fluctuations in quarterly results may negatively impact the trading price of our Class A common stock. Our quarterly financial results may fluctuate as a result of a number of factors, many of which are outside of our control and may be difficult to predict, including, without limitation:

- general economic, macroeconomic and political conditions, both domestic and in our foreign markets, that could impact some or all regions where we operate, including any global economic slowdown, global banking and finance related issues, increased risk of inflation, rising interest rates, labor shortages and potential global recession, war, terrorism or armed conflict, including Russia's invasion of Ukraine, or instability in the global system;
- our ability to attract new and retain existing customers or sell additional features to existing customers;
- the budgeting cycles, seasonal buying patterns, and purchasing practices of customers;
- the timing and length of our sales cycles;

- changes in customer or channel partner requirements or market needs;
- changes in the growth rate of the cybersecurity market generally and market for endpoint security;
- the timing and success of new product and service introductions by us or our competitors or any other competitive developments, including consolidation among our customers or competitors;
- the level of awareness of cybersecurity threats, particularly advanced cyberattacks, and the market adoption of our platform;
- our ability to successfully expand our business domestically and internationally;
- decisions by organizations to purchase security solutions from larger, more established security vendors or from their primary IT equipment vendors;
- changes in our pricing policies or those of our competitors;
- any disruption in our relationship with ISVs, channel partners, MSPs, MSSPs, MDRs, OEMs and IR firms;
- insolvency or credit difficulties confronting our customers, affecting their ability to purchase or pay for our solution;
- significant security breaches of, technical difficulties with or interruptions to, the use of our platform;
- extraordinary expenses such as litigation or other dispute-related settlement payments or outcomes, taxes, regulatory fines or penalties;
- the impact of the COVID-19 pandemic on our operations, financial results, and liquidity and capital resources, including on customers, sales, expenses, and employees;
- future accounting pronouncements or changes in our accounting policies or practices;
- negative media coverage or publicity;
- the amount and timing of operating costs and capital expenditures related to the expansion of our business; and
- increases or decreases in our expenses caused by fluctuations in foreign currency exchange rates.

In addition, we experience seasonal fluctuations in our financial results as we typically receive a higher percentage of our annual orders from new customers, as well as renewal orders from existing customers, in our fourth fiscal quarter as compared to other quarters due to the annual budget approval process of many of our customers.

Any of the above factors, individually or in the aggregate, may result in significant fluctuations in our financial and other operating results from period to period. As a result of this variability, our historical operating results should not be relied upon as an indication of future performance. Moreover, this variability and unpredictability could result in our failure to meet our operating plan or the expectations of investors or analysts for any period. If we fail to meet such expectations for the reasons described above or other reasons, our stock price could fall substantially, and we could face costly lawsuits, including securities class action suits.

Our platform represents a new approach to endpoint protection and, therefore, it is difficult to predict adoption and demand for our platform.

Our cloud-native, artificial intelligence-enabled endpoint security platform represents a new approach to endpoint protection. Accordingly, it is difficult to predict customer adoption and demand for our platform, the size and growth rate of this market, the entry of competitive products and services or the success of existing competitive products and services.

Any expansion in our market depends on a number of factors, including the cost, performance and perceived value associated with, and customer adoption of, our platform. If the market for our platform does not achieve widespread adoption or there is a reduction in demand for our software or our services caused by a lack of customer acceptance, implementation challenges for deployment, technological challenges, competing technologies and services, decreases in corporate spending, weakening economic conditions, or otherwise, it could result in reduced customer orders and decreased revenue, which would adversely affect our business operations and financial condition.

Our platform interoperates with, but does not necessarily replace, other security products. Businesses that use other cybersecurity products and services may be hesitant to purchase our platform if they believe their existing products and services provide a level of security that is sufficient to meet their needs. If we do not succeed in convincing customers that our platform should be an integral part of their overall approach to security, our sales will not grow as quickly as anticipated, or at all, which would have an adverse impact on our business, operating results, and financial condition.

If businesses do not continue to adopt our platform for any of the reasons discussed above or for other reasons not contemplated, our sales would not grow as quickly as anticipated, or at all, and our business, operating results, and financial condition would be adversely affected.

A network or data security incident against us, whether actual, alleged, or perceived, would harm our reputation, create liability and regulatory exposure, and adversely impact our business, operating results, and financial condition.

Companies are subject to an increasing number and wide variety of attacks on their networks on an ongoing basis. Traditional computer “hackers,” malicious code (such as viruses and worms), phishing attempts, ransomware, account takeover, business email compromise, employee fraud, theft or misuse, denial of service attacks, and sophisticated nation-state and nation-state supported actors engage in intrusions and attacks that create risks for our internal networks and cloud deployed products and the information they store and process. Cybersecurity companies face particularly intense attack efforts, and we have faced, and will continue to face, cyber threats and attacks from a variety of sources. The research that we conduct and report may make us, or our customers, a further target for attacks of all kinds. State-supported and geopolitical-related cyberattacks may increase in connection with Russia’s invasion of Ukraine and any related political or economic responses and counter-responses. The war in Ukraine and associated activities in Ukraine and Russia has increased the risk of cyberattacks on various types of infrastructure and operations, and the United States government has warned companies to be prepared for a significant increase in Russian cyberattacks in response to the sanctions on Russia.

Although we have implemented security measures to prevent such attacks, our networks and systems may be breached due to the actions of outside parties, employee error, malfeasance, a combination of these, or otherwise, and as a result, an unauthorized party may obtain access to our and/or our customers’ systems, networks, or data. We may face difficulties or delays in identifying or otherwise responding to any attacks or actual or potential security breaches or threats. A breach in our data security or an attack against our platform could impact our networks or the networks and data of our customers that are secured by our platform, creating system disruptions or slowdowns and providing access to malicious parties to information stored on our networks or the networks of our customers, resulting in data being publicly disclosed, misused, altered, lost, or stolen, which could subject us to liability and adversely affect our financial condition. The COVID-19 pandemic may have generally increased the attack surface available to criminals, as companies and individuals work online and remotely, which has increased the risk of a successful cyber security attack. We have accordingly increased our investments in protective measures and risk mitigation strategies, but we cannot guarantee that our efforts, or the efforts of those upon whom we rely and partner with, will be successful in preventing any such information security incidents. Protecting our own assets has become more expensive from a dollar investment and time perspective.

Any actual, alleged or perceived security breach in our systems or networks, or any other actual, alleged or perceived data security incident we suffer, could result in damage to our reputation, negative publicity, loss of customers and sales, loss of competitive advantages over our competitors, increased costs to remedy any problems and otherwise respond to any incident, regulatory investigations and enforcement actions, costly litigation, and other liability. We would also be exposed to a risk of loss or litigation and potential liability under laws, regulations and

contracts that protect the privacy and security of personal information. For example, the California Consumer Privacy Act of 2018 (CCPA), imposes a private right of action for security breaches that could lead to some form of remedy including regulatory scrutiny, fines, private right of action settlements, and other consequences. Where a security incident involves a breach of security leading to the accidental or unlawful destruction, loss, alternation, unauthorized disclosure of, or access to, personal data in respect of which we are a controller or processor under the GDPR and U.K. GDPR (as defined below), this could result in fines of up to €20 million or 4% of annual global turnover under the GDPR or £17 million and 4% of total annual revenue in the case of the U.K. GDPR. We may also be required to notify such breaches to regulators and/or individuals which may result in us incurring additional costs.

In addition, we may incur significant financial and operational costs to investigate, remediate, eliminate and put in place additional tools and devices designed to prevent actual or perceived security breaches and other security incidents, as well as costs to comply with any notification obligations resulting from any security incidents. Any of these negative outcomes could adversely affect the market perception of our platform and customer and investor confidence in our company, and would adversely affect our business, operating results, and financial condition.

Defects, errors, or vulnerabilities in our platform, the failure of our platform to block malware or prevent a security breach, misuse of our platform, or risks of product liability claims would harm our reputation and adversely impact our business, operating results, and financial condition.

Our platform and product features are multi-faceted and may be deployed with material defects, software “bugs” or errors that are not detected until after their commercial release and deployment to our customers. From time to time, certain of our customers have reported defects in our platform related to performance, scalability, and compatibility. Our platform and product features also provide our customers with the ability to customize a multitude of settings, and it is possible that a customer could misconfigure our platform or otherwise fail to configure our products in an optimal manner. Such defects and misconfigurations of our platform could cause our platform to operate at suboptimal efficacy, cause it to fail to secure customers’ computing environments and detect and block threats, or temporarily interrupt the functionality of our customers’ endpoints. We also make frequent updates to our platform, which may fail, resulting in temporary vulnerability that increases the likelihood of a material defect.

In addition, because the techniques used by computer hackers to access or sabotage target computing environments change frequently and generally are not recognized until launched against a target, there is a risk that an advanced attack could emerge that our platform is unable to detect or prevent. Furthermore, as a well-known provider of security solutions, our networks, platform, products, including cloud-based technology, and customers could be targeted by attacks specifically designed to disrupt our business and harm our reputation. In addition, due to the Russian invasion there could be a significant increase in Russian cyberattacks against our customers, resulting in an increased risk of a security breach of our customers’ systems. In addition, defects or errors in our platform could result in a failure to effectively update customers’ cloud-based products. Our data centers and networks may experience technical failures and downtime, may fail to distribute appropriate updates, or may fail to meet the increased requirements of a growing customer base, any of which could temporarily or permanently expose our customers’ computing environments, leaving their computing environments unprotected against cyber threats. Any of these situations could result in negative publicity to us, damage our reputation, and increase expenses and customer relations issues, which would adversely affect our business, financial condition, and operating results.

Advances in computer capabilities, discoveries of new weaknesses and other developments with software generally used by the Internet community may increase the risk we will suffer a security breach. Furthermore, our platform may fail to detect or prevent malware, ransomware, viruses, worms or similar threats for any number of reasons, including our failure to enhance and expand our platform to reflect industry trends, new technologies and new operating environments, the complexity of the environment of our clients and the sophistication of malware, viruses and other threats. Our platform may fail to detect or prevent threats in any particular test for a number of reasons. We or our service providers may also suffer security breaches or unauthorized access to personal information, financial account information, and other confidential information due to employee error, rogue employee activity, unauthorized access by third parties acting with malicious intent or who commit an inadvertent mistake or social engineering. If we experience, or our service providers experience, any breaches of security

measures or sabotage or otherwise suffer unauthorized use or disclosure of, or access to, personal information, financial account information or other confidential information, we might be required to expend significant capital and resources to address these problems. We may not be able to remedy any problems caused by hackers or other similar actors in a timely manner, or at all. To the extent potential customers, industry analysts or testing firms believe that the failure to detect or prevent any particular threat is a flaw or indicates that our platform does not provide significant value, our reputation and business would be harmed. Any real or perceived defects, errors or vulnerabilities in our platform, or any other failure of our platform to detect an advanced threat, could result in:

- a loss of existing or potential customers;
- delayed or lost revenue and adverse impacts to our business, operating results, and financial condition;
- a delay in attaining, or the failure to attain, market acceptance;
- the expenditure of significant financial and research and development resources in efforts to analyze, correct, eliminate, or work around errors or defects, and address and eliminate vulnerabilities;
- an increase in resources devoted to customer service and support, which could adversely affect our gross margin;
- harm to our reputation or brand; and
- claims and litigation, regulatory inquiries, or investigations, enforcement actions, and other claims and liabilities, all of which may be costly and burdensome and further harm our reputation.

Because techniques used to obtain unauthorized access or to sabotage systems change frequently and generally are not recognized until after they are launched against a target, we and our service providers may be unable to anticipate these techniques or to implement adequate preventative measures. Moreover, if a high-profile cybersecurity incident occurs with respect to another SaaS provider, customers may lose trust in the security of the SaaS business model generally, which could adversely affect our ability to retain existing customers or attract new ones. In the last few years there have been many successful advanced cybersecurity incidents that have damaged several prominent companies in spite of strong information security measures. We expect that the risks associated with cybersecurity incidents and the costs of preventing such attacks will continue to increase in the future.

In addition, we cannot assure you that any limitation of liability provisions in our customer agreements, contracts with third-party vendors and service providers, or other contracts would be enforceable or adequate or would otherwise protect us from any liabilities or damages with respect to any particular claim relating to a security breach or other security-related matter or as a result of federal, state, or local laws or ordinances, or unfavorable judicial decisions in the U.S. or other countries. We maintain insurance to protect against certain claims associated with the use of our platform, but our insurance coverage may not adequately cover any claim asserted against us. In addition, even claims that ultimately are unsuccessful could result in our expenditure of funds in litigation, divert management's time and other resources, and harm our reputation. We also cannot be certain that our insurance coverage will be adequate for data handling or data security liabilities actually incurred, that insurance will continue to be available to us on economically reasonable terms, or at all, or that any future claim will not be excluded or otherwise be denied coverage by any insurer. The successful assertion of one or more large claims against us that exceed available insurance coverage, or the occurrence of changes in our insurance policies, including premium increases or the imposition of large deductible or co-insurance requirements, could adversely affect our business, operating results and financial condition.

Existing and future acquisitions, strategic investments, partnerships or alliances could be difficult to identify and integrate, divert the attention of key management personnel, disrupt our business, dilute stockholder value and adversely affect our business, operating results, and financial condition.

As part of our business strategy, we have in the past and expect to continue to make investments in and/or acquire complementary companies, services, products, technologies, or talent. For example, in February 2021 we acquired Scalyr, a data analytics company and in May 2022 we acquired Attivo, a leading identity security and

lateral movement protection company. We have also invested in certain privately held companies through our S Ventures fund. Our ability as an organization to acquire and integrate other companies, services or technologies in a successful manner is not guaranteed.

In the future, we may not be able to find suitable acquisition candidates, and we may not be able to complete such acquisitions on favorable terms, if at all. Our due diligence efforts may fail to identify all of the challenges, problems, liabilities or other shortcomings involved in an acquisition. If we do complete acquisitions, we may not ultimately strengthen our competitive position or ability to achieve our business objectives, and any acquisitions we announce or complete could be viewed negatively by our customers or investors.

In addition, if we are unsuccessful at integrating existing and future acquisitions, or the technologies and personnel associated with such acquisitions, into our company, the revenue and operating results of the combined company could be adversely affected. Any integration process may require significant time and resources, and we may not be able to manage the process successfully. We may not successfully evaluate or utilize the acquired technology or personnel, or accurately forecast the financial impact of an acquisition transaction, causing unanticipated write-offs or accounting charges. Additionally, integrations could take longer than expected, or if we move too quickly in trying to integrate an acquisition, strategic investment, partnership, or other alliance, we may fail to achieve the desired efficiencies.

We have, and may in the future have, to pay cash, incur debt or issue equity securities to pay for any such acquisition, each of which could adversely affect our financial condition and the market price of our Class A common stock. The sale of equity or issuance of debt to finance any such acquisitions could result in dilution to our stockholders, which depending on the size of the acquisition, may be significant. The incurrence of indebtedness would result in increased fixed obligations and could also include covenants or other restrictions that would impede our ability to manage our operations.

Additional risks we may face in connection with acquisitions include:

- diversion of management’s time and focus from operating our business to addressing acquisition integration challenges;
- the inability to coordinate research and development and sales and marketing functions;
- the inability to integrate product and service offerings;
- retention of key employees from the acquired company;
- changes in relationships with strategic partners or the loss of any key customers or partners as a result of product acquisitions or strategic positioning resulting from the acquisition;
- cultural challenges associated with integrating employees from the acquired company into our organization;
- integration of the acquired company’s accounting, CRM, management information, human resources and other administrative systems;
- the need to implement or improve controls, procedures and policies at a business that prior to the acquisition may have lacked sufficiently effective controls, procedures and policies;
- unexpected security risks or higher than expected costs to improve the security posture of the acquired company;
- higher than expected costs to bring the acquired company’s IT infrastructure up to our standards;
- additional legal, regulatory or compliance requirements;
- financial reporting, revenue recognition or other financial or control deficiencies of the acquired company that we don’t adequately address and that cause our reported results to be incorrect;

- liability for activities of the acquired company before the acquisition, including intellectual property infringement claims, violations of laws, commercial disputes, tax liabilities and other known and unknown liabilities;
- failing to achieve the expected benefits of the acquisition or investment; and
- litigation or other claims in connection with the acquired company, including claims from or against terminated employees, customers, current and former stockholders or other third parties.

Our failure to address these risks or other problems encountered in connection with acquisitions and investments could cause us to fail to realize the anticipated benefits of these acquisitions or investments, cause us to incur unanticipated liabilities, and harm our business generally.

If we are unable to retain our customers, renew and expand our relationships with them, and add new customers, we may not be able to sustain revenue growth, and we may not achieve or maintain profitability in the future.

In recent periods, we have experienced rapid growth in the adoption of our platform, customer base and revenue. However, we may not continue to grow or grow at the same rate in the future. Any success that we may experience in the future will depend, in large part, on our ability to, among other things:

- maintain, renew and expand our existing customer base;
- continue to attract new customers;
- induce customers to expand deployment of the initially adopted module(s) of our platform across their organizations and infrastructure, and to adopt additional modules of our platform and services;
- improve the capabilities of our platform through research and development;
- continue to successfully expand our business domestically and internationally; and
- successfully compete with other companies in the endpoint security industry.

Our customers have no obligation to renew their subscription for our platform after the expiration of their contractual subscription period, which is generally one to three years, and in the normal course of business, some customers have elected not to renew. In addition, our customers may renew for shorter contract subscription lengths or cease using certain features. Our customer retention and expansion may decline or fluctuate as a result of a number of factors, including our customers' satisfaction with our services, our pricing, customer security and networking issues and requirements, our customers' spending levels, decreases in the number of endpoints to which our customers deploy our solution, mergers and acquisitions involving our customers, industry developments, competition, general economic conditions, or the perceived decline in the incidence of cyberattacks. If our efforts to maintain and expand our relationships with our existing customers are not successful, our business, operating results, and financial condition will materially suffer.

If our platform is not effectively interoperated within our customers' IT infrastructure, deployments could be delayed or canceled, which would adversely impact our business, operating results, and financial condition.

Our platform must effectively interoperate with our customers' existing IT infrastructure, which often has different specifications, utilizes multiple protocol standards, deploys products and services from multiple vendors, and contains multiple generations of products and services that have been added over time. As a result, our solutions can sometimes encounter interoperability issues on deployment or over time, which require additional support and problem solving with customers, in some cases, at a substantial cost to us. We may modify our software or introduce new capabilities so that our platform interoperates with a customer's infrastructure. These issues could cause longer deployment and integration times for our platform, leading to customer churn, which would adversely affect our business, operating results, and financial condition. In addition, government and other customers may require our platform to comply with certain security or other certifications and standards. If we are unable to achieve, or are delayed in achieving, compliance with these certifications and standards, we may be disqualified from selling our

platform to such customers, or may otherwise be at a competitive disadvantage, either of which could adversely affect our business, operating results, and financial condition.

Disruptions or other business interruptions that affect the availability of our platform could adversely impact our customer relationships and overall business.

Our platform is hosted by third-party cloud hosting providers including Amazon Web Services (AWS). Our software and systems are designed to use computing, storage capabilities, bandwidth, and other services provided by such cloud hosting providers, and currently our cloud service infrastructure is primarily run on AWS. We have experienced, and expect in the future that we may experience from time to time, interruptions, delays or outages in service availability due to a variety of factors. Capacity constraints could arise from a number of causes such as technical failures, natural disasters, fraud, or security attacks. The level of service provided by our cloud hosting providers, or regular or prolonged interruptions in that service, could also impact the use of, and our customers' satisfaction with, our platform and could harm our business and reputation. In addition, hosting costs are expected to increase as our customer base grows, which could adversely affect our business, operating results and financial condition.

Furthermore, AWS has discretion to change and interpret its terms of service and other policies with respect to us, including on contract renewal, and those actions may be unfavorable to our business operations. AWS, and other cloud hosting providers, may also take actions beyond our control that could seriously harm our business, including discontinuing or limiting our access to one or more services, increasing pricing terms, competing with us, terminating or seeking to terminate our contractual relationship altogether, or altering how we are able to process data on their system in a way that is unfavorable or costly to us. Although we obtain services from other cloud hosting providers, if our current arrangement with AWS were terminated, we could experience interruptions on our platform and in our ability to make our content available to customers, as well as delays and additional expenses in arranging for expansion and transition to alternative cloud hosting and infrastructure services. Such a transition could require further technical changes to our platform, including, but not limited to, our cloud service infrastructure which was initially designed to run on AWS. Making such changes could be costly in terms of time and financial resources.

Any of these factors could reduce our revenue, subject us to liability, and cause our customers to decline to renew their subscriptions, any of which would harm our business and operating results.

We may not timely and cost-effectively scale and adapt our existing technology to meet our customers' performance and other requirements.

Our future growth is dependent upon our ability to continue to meet the needs of new customers and the expanding needs of our existing customers as their use of our solutions grows. As our customers gain more experience with our platform, the number of endpoints and events, the amount of data transferred, processed and stored by us, and the number of locations where our platform is being accessed, have in the past, and may in the future, expand rapidly. In order to meet the performance and other requirements of our customers, we intend to continue to make significant investments to increase capacity and to develop and implement new technologies in our service and cloud infrastructure operations. These technologies, which include databases, applications, and server optimizations, network and hosting strategies, and automation, are often advanced, complex, new and untested. We may not be successful in developing or implementing these technologies. In addition, it takes a significant amount of time to plan, develop and test improvements to our technologies and infrastructure, and we may not be able to accurately forecast demand or predict the results we will realize from such improvements. In some circumstances, we may also determine to scale our technology through the acquisition of complementary businesses and technologies rather than through internal development, which may divert management's time and resources. To the extent that we do not effectively scale our operations to meet the needs of our growing customer base and to maintain performance as our customers expand their use of our solution, we will not be able to grow as quickly as we anticipate, our customers may reduce or cancel use of our solutions and we will be unable to compete as effectively and our business and operating results will be adversely affected.

If we do not accurately anticipate and promptly respond to changes in our customers' technologies, business plans or security needs, our competitive position and prospects will be adversely impacted.

The cybersecurity market has grown quickly and is expected to continue to evolve rapidly. Moreover, many of our customers operate in markets characterized by rapidly changing technologies and business plans, which require them to add numerous network-connected endpoints and adapt to increasingly complex IT environments, incorporating a variety of hardware, software applications, operating systems, and networking protocols. As their technologies and business plans grow more complex, we expect these customers to face new and increasingly sophisticated methods of attack. We face significant challenges in ensuring that our platform effectively identifies and responds to these advanced and evolving attacks. As a result of the continued rapid innovations in the technology industry, including the rapid growth of smartphones, tablets and other devices, enterprise employees using personal devices for work, and the rapidly evolving Internet of Things, we expect the networks of our customers to continue to change rapidly and become more complex. There can be no assurance that we will be successful in developing and marketing, on a timely basis, enhancements to our platform that adequately address the changing needs of our customers. In addition, any enhancements to our platform could involve research and development processes that are more complex, expensive and time-consuming than we anticipate. We may experience unanticipated delays in the availability of enhancements to our platform and may fail to meet customer expectations with respect to the timing of such availability. If we do not quickly respond to the rapidly changing and rigorous needs of our customers by developing and releasing updates to our platform on a timely basis that can adequately respond to advanced threats and our customers' evolving needs, our business, operating results, and financial condition will be adversely affected.

If we are not able to maintain and enhance our brand and reputation, our business and operating results may be adversely affected.

We believe that maintaining and enhancing our brand and our reputation as a leading provider of endpoint security solutions is critical to our relationship with our existing customers, channel partners, and alliance partners and our ability to attract new customers and partners. The successful promotion of our brand will depend on a number of factors, including our ability to continue to develop additional features for our platform, our ability to successfully differentiate our platform from competitive cloud-based or legacy security solutions, our marketing efforts, and, ultimately, our ability to detect and stop breaches. Although we believe it is important for our growth, our brand promotion activities may not be successful or yield increased revenue.

Under certain circumstances, our employees may have access to our customers' platforms. An employee may take advantage of such access to conduct malicious activities. Any such misuse of our platform could result in negative press coverage and negatively affect our reputation, which could result in harm to our business, reputation, and operating results.

In addition, independent industry and research firms often evaluate our solutions and provide reviews of our platform, as well as the products of our competitors, and perception of our platform in the marketplace may be significantly influenced by these reviews. If these reviews are negative, or less positive as compared to those of our competitors' products, our brand may be adversely affected. Our solutions may fail to detect or prevent threats in any particular test for a number of reasons that may or may not be related to the efficacy of our solutions in real world environments. To the extent potential customers, industry analysts or research firms believe that the occurrence of a failure to detect or prevent any particular threat is a flaw or indicates that our solutions or services do not provide significant value, we may lose customers, and our reputation, financial condition and business would be harmed.

Moreover, the performance of our channel partners and alliance partners may affect our brand and reputation if customers do not have a positive experience with these partners. In addition, we have in the past worked, and continue to work, with high profile customers as well as assist in analyzing and remediating high profile cyberattacks. Our work with such customers has exposed us to publicity and media coverage. Negative publicity about us, including about our management, the efficacy and reliability of our platform, our products offerings, our professional services, and the customers we work with, even if inaccurate, could adversely affect our reputation and brand.

If we are unable to maintain successful relationships with our channel partners and alliance partners, or if our channel partners or alliance partners fail to perform, our ability to market, sell and distribute our platform will be limited, and our business, operating results, and financial condition will be harmed.

Substantially all of our sales are fulfilled through our channel partners, including resellers, distributors, MSPs, MSSPs, MDRs, OEMs, and IR firms, and we expect that we will continue to generate a significant portion of our revenue from channel partners for the foreseeable future. Our channel partners generated 90%, 92%, and 96% of our revenue for fiscal 2023, 2022, and 2021, respectively. Our largest channel partner for fiscal 2023, 2022, and 2021, was Exclusive Networks. We generated 18%, 18%, and 19% of our revenue from Exclusive Networks for fiscal 2023, 2022, and 2021, respectively. Our agreements with our channel partners, including agreements with Exclusive Networks, are non-exclusive, do not last for set terms, and may be terminated by either party at any time. Further, channel partners fulfill our sales on a purchase order basis and do not impose minimum purchase requirements or related terms on sales. Additionally, we have entered, and intend to continue to enter, into alliance partnerships with third parties to support our future growth plans. The loss of a substantial number of our channel partners or alliance partners, or the failure to recruit additional partners, would adversely affect our business, operating results, and financial condition.

To the extent our partners are unsuccessful in selling our platform, or if we are unable to enter into arrangements with and retain a sufficient number of high-quality partners in each of the regions in which we sell or plan to sell our platform, we are unable to keep them motivated to sell our platform, or our partners shift focus to other vendors and/or our competitors, our ability to sell our platform and operating results will be harmed. The termination of our relationship with any significant partner may adversely affect our sales and operating results. Our ability to achieve revenue growth in the future will depend in part on our ability to maintain successful relationships with our channel partners and in training our channel partners to independently sell and deploy our platform.

We are also exposed to credit and liquidity risks and our operating results will be harmed if our partners were to become unable or unwilling to pay us at all or in a timely manner, terminate their relationships with us or go out of business. Although we have programs in place that are designed to monitor and mitigate such risks, we cannot guarantee these programs will be effective in reducing our risks. If we are unable to adequately control these risks, our business, operating results, and financial condition would be harmed. If partners fail to pay us under the terms of our agreements or we are otherwise unable to collect on our accounts receivable from these partners, we may be adversely affected both from the inability to collect amounts due and the cost of enforcing the terms of our contracts, including litigation. Our partners may seek bankruptcy protection or other similar relief and fail to pay amounts due to us, or pay those amounts more slowly, either of which would adversely affect our business, operating results, and financial condition. We may be further impacted by consolidation of our existing channel partners. In such instances, we may experience changes to our overall business and operational relationships due to dealing with a larger combined entity, and our ability to maintain such relationships on favorable contractual terms may be more limited. We may also become increasingly dependent on a more limited number of channel partners, as consolidation increases the relative proportion of our business for which each channel partner is responsible, which may magnify the risks described in the preceding paragraphs.

Our business depends, in part, on sales to government organizations, and significant changes in the contracting or fiscal policies of such government organizations could adversely affect our business and operating results.

Our future growth depends, in part, on increasing sales to government organizations. Demand from government organizations is often unpredictable and subject to budgetary uncertainty. We have made significant investments to address the government sector, but we cannot assure you that these investments will be successful, or that we will be able to maintain or grow our revenue from the government sector. Although we anticipate that they may increase in the future, sales to governmental organizations have not accounted for, and may never account for, a significant portion of our revenue. Sales to governmental organizations are subject to a number of challenges and risks that may adversely affect our business and operating results, including the following risks:

- selling to governmental agencies can be highly competitive, expensive, and time consuming, often requiring significant upfront time and expense without any assurance that such efforts will generate a sale;

- government certification, software supply chain or source code transparency requirements applicable to us or our platform may change and, in doing so, restrict our ability to sell into the governmental sector until we have attained the revised certification or meet other new requirements. For example, although SentinelOne is currently FedRAMP authorized, such authorization is costly to maintain and subject to rigorous compliance and if we lose our authorization, it would restrict our ability to sell to government customers;

- government demand and payment for our platform may be impacted by public sector budgetary cycles and funding authorizations, with funding reductions or delays adversely affecting public sector demand for our platform, including as a result of sudden, unforeseen and disruptive events such as government shut downs, war, incidents of terrorism, natural disasters, and public health concerns or epidemics;

- governments routinely investigate and audit government contractors' administrative processes, and any unfavorable audit could result in the government refusing to continue buying our platform, which would adversely impact our revenue and operating results, or institute fines or civil or criminal liability if an investigation, audit, or other review, were to uncover improper or illegal activities;

- governments may require certain products to be manufactured, produced, hosted or accessed solely in their country or in other relatively high-cost locations, and we may not produce or host all products in locations that meet these requirements, affecting our ability to sell these products to governmental agencies; and

- refusal to grant certain certifications or clearance by one government agency, or decision by one government agency that our products do not meet certain standards, may cause reputational harm and cause concern with other government agencies.

The occurrence of any of the foregoing could cause governmental organizations to delay or refrain from purchasing our solutions in the future or otherwise adversely affect our business and operating results.

Our long-term success depends, in part, on our ability to expand the sale of our platform to customers located outside of the United States and our current, and any further, expansion of our international operations exposes us to risks that could have a material adverse effect on our business, operating results, and financial condition.

We are generating a growing portion of our revenue outside of the United States, and conduct our business activities in various foreign countries, including some emerging markets where we have limited experience, where the challenges of conducting our business can be significantly different from those we have faced in more developed markets and where business practices may create internal control risks including:

- fluctuations in foreign currency exchange rates, which could add volatility to our operating results;

- new, or changes in, regulatory requirements;

- tariffs, export and import restrictions, restrictions on foreign investments, sanctions, and other trade barriers or protection measures;

- exposure to numerous, increasing, stringent (particularly in the European Union), and potentially inconsistent laws and regulations relating to privacy, data protection, and information security;

- costs of localizing products and services;

- lack of acceptance of localized products and services;

- the need to make significant investments in people, solutions and infrastructure, typically well in advance of revenue generation;

- challenges inherent in efficiently managing an increased number of employees over large geographic distances, including the need to implement appropriate systems, policies, benefits, and compliance programs;

- difficulties in maintaining our corporate culture with a dispersed and distant workforce;
- treatment of revenue from international sources, evolving domestic and international tax environments, and other potential tax issues, including with respect to our corporate operating structure and intercompany arrangements;
- different or weaker protection of our intellectual property, including increased risk of theft of our proprietary technology and other intellectual property;
- economic weakness or currency-related crises;
- compliance with multiple, conflicting, ambiguous or evolving governmental laws and regulations, including employment, tax, data privacy, anti-corruption, import/export, antitrust, data transfer, storage and protection, and industry-specific laws and regulations, including rules related to compliance by our third-party resellers and our ability to identify and respond timely to compliance issues when they occur;
- vetting and monitoring our third-party channel partners in new and evolving markets to confirm they maintain standards consistent with our brand and reputation;
- generally longer payment cycles and greater difficulty in collecting accounts receivable;
- our ability to adapt to sales practices and customer requirements in different cultures;
- the lack of reference customers and other marketing assets in regional markets that are new or developing for us, as well as other adaptations in our market generation efforts that we may be slow to identify and implement;
- dependence on certain third parties, including channel partners with whom we do not have extensive experience;
- natural disasters, acts of war, terrorism, or pandemics, including the COVID-19 pandemic and the conflict in Ukraine;
- instability in the global banking system;
- corporate espionage; and
- political instability and security risks in the countries where we are doing business and changes in the public perception of governments in the countries where we operate or plan to operate.

We have undertaken, and will continue to undertake, additional corporate operating restructurings from time to time that involve our group of foreign country subsidiaries through which we do business abroad. We consider various factors in evaluating these restructurings, including the alignment of our corporate legal entity structure with our organizational structure and its objectives, the operational and tax efficiency of our group structure, and the long-term cash flows and cash needs of our business. Such restructurings increase our operating costs, and if ineffectual, could increase our income tax liabilities and our global effective tax rate.

We have experienced rapid growth in recent periods, and if we do not effectively manage our future growth, our business, operating results, and financial condition may be adversely affected.

We have experienced rapid growth in recent periods, and we expect to continue to invest broadly across our organization to support our growth. For example, our headcount grew from over 1,200 employees as of January 31, 2022, to over 2,100 employees as of January 31, 2023. Although we have experienced rapid growth historically, we may not sustain our current growth rates, nor can we assure you that our investments to support our growth will be successful. The growth and expansion of our business will require us to invest significant financial and operational resources and the continuous dedication of our management team.

In addition, as we have grown, our number of customers has also increased significantly, and we have increasingly managed more complex deployments of our platform in more complex computing environments. The rapid growth and expansion of our business places a significant strain on our management, operational, and financial resources. To manage any future growth effectively, we must continue to improve and expand our information technology and financial infrastructure, our operating and administrative systems and controls, and our ability to manage headcount, capital, and processes in an efficient manner.

If we continue to experience rapid growth, we may not be able to successfully implement or scale improvements to our systems, processes, and controls in an efficient or timely manner. For example, as we grow, we may experience difficulties in managing improvements to our systems, processes, and controls or in connection with third-party software licensed to help us with such improvements. As we grow, our existing systems, processes, and controls may not prevent or detect all errors, omissions, or fraud. Any future growth will continue to add complexity to our organization and require effective coordination throughout our organization. Failure to manage any future growth effectively could result in increased costs, cause difficulty or delays in deploying new customers, reduce demand for our platform, cause difficulties in introducing new features or other operational difficulties, and any of these difficulties would adversely affect our business, operating results, and financial condition.

Our sales cycles can be long and unpredictable, and our sales efforts require considerable time and expense.

Our revenue recognition is difficult to predict because of the length and unpredictability of the sales cycle for our platform, particularly with respect to large organizations and government entities. For example, in light of current macroeconomic conditions, we have observed a lengthening of the sales cycle for some prospective customers that we attribute to higher cost-consciousness around IT budgets. Customers often view the subscription to our platform as a significant strategic decision and, as a result, frequently require considerable time to evaluate, test and qualify our platform prior to entering into or expanding a relationship with us. Large enterprises and government entities in particular, often undertake a significant evaluation process that further lengthens our sales cycle.

Our direct sales team develops relationships with our customers, and works with our channel partners on account penetration, account coordination, sales and overall market development. We spend substantial time and resources on our sales efforts without any assurance that our efforts will produce a sale. Security solution purchases are frequently subject to budget constraints, multiple approvals and unanticipated administrative, processing and other delays. As a result, it is difficult to predict whether and when a sale will be completed. The failure of our efforts to secure sales after investing resources in a lengthy sales process would adversely affect our business, operating results and financial condition.

The sales prices of our platform may decrease, or the mix of our sales may change, which may reduce our gross profits and adversely affect our business, operating results, and financial condition.

We have limited experience with respect to determining the optimal prices for our platform. As the market for endpoint security matures, or as new competitors introduce new products or services that are similar to or compete with ours, we may be unable to effectively optimize our prices through increases or decreases, attract new customers at our offered prices or based on the same pricing model as we have used historically. Further, competition continues to increase in the market segments in which we participate, and we expect competition to further increase in the future, thereby leading to increased pricing pressures. Larger competitors with more diverse product and service offerings may reduce the price of products or services that compete with ours or may bundle them with other products and services. This could lead customers to demand greater price concessions or additional functionality at the same price levels. As a result, in the future we may be required to reduce our prices or provide more features without corresponding increases in price, which would adversely affect our business, operating results, and financial condition.

Because we recognize revenue from subscriptions to our platform over the term of the subscription, downturns or upturns in new business will not be immediately reflected in our operating results.

We generally recognize revenue from customers ratably over the term of their subscription, which is generally one to three years. As a result, a substantial portion of the revenue we report in each period is attributable to the

recognition of deferred revenue relating to agreements that we entered into during previous periods. Consequently, any increase or decrease in new sales or renewals in any one period will not be immediately reflected in our revenue for that period. Any such change, however, would affect our revenue in future periods. Accordingly, the effect of downturns or upturns in new sales and potential changes in our rate of renewals will not be fully reflected in our operating results until future periods. We may also be unable to timely reduce our cost structure in line with a significant deterioration in sales or renewals that would adversely affect our business, operating results, and financial condition.

We provide service level commitments under some of our customer contracts. If we fail to meet these contractual commitments, we could be obligated to provide partial refunds or our customers could be entitled to terminate their contracts and our business would suffer.

Certain of our customer agreements contain service level commitments, which contain specifications regarding the availability of our platform and our support services. Failure of or disruption to our infrastructure or third-party hosting service providers could impact the performance of our platform and the availability of services to customers. If we are unable to meet our stated service level commitments or if we suffer extended periods of poor performance or unavailability of our platform, we may be contractually obligated to provide affected customers with credit, partial refunds or termination rights. To date, there has not been a material failure to meet our service level commitments, and we do not currently have any material liabilities accrued on our consolidated balance sheets for such commitments. Our business, operating results, and financial condition would be adversely affected if we suffer performance issues or downtime that exceeds the service level commitments under our agreements with our customers.

Our business is subject to the risks of warranty claims, product returns and product defects from real or perceived defects in our solutions or their misuse by our customers or third parties and indemnity provisions in various agreements potentially expose us to substantial liability for intellectual property infringement and other losses.

We may be subject to liability claims for damages related to errors or defects in our solutions. A material liability claim or other occurrence that harms our reputation or decreases market acceptance of our platform will harm our business and operating results. Although we generally have limitation of liability provisions in our terms and conditions of sale, they may not fully or effectively protect us from claims as a result of federal, state or local laws or ordinances, or unfavorable judicial decisions in the United States or other countries. The sale and support of our platform also entails the risk of product liability claims. We employ measures in the form of policy and technical controls to limit unauthorized access to our platform by our employees, customers and third-parties, however, these measures may not fully or effectively protect our platform from unauthorized access.

Additionally, we typically provide indemnification to customers, partners or other third parties we do business with for certain losses suffered or expenses incurred as a result of third-party claims arising from our infringement of a third party's intellectual property. We also provide unlimited liability for certain breaches of confidentiality, as defined in our master subscription agreement. We also provide limited liability in the event of certain breaches of our master subscription agreement. Certain of these contractual provisions survive termination or expiration of the applicable agreement. To date, we have not incurred any material costs because of such obligations. However, as we continue to grow, indemnification claims against us for the obligations listed will increase.

When our customers or other third parties we do business with make intellectual property rights or other indemnification claims against us, we will incur significant legal expenses and may have to pay damages, license fees and/or stop using technology found to be in violation of the third party's rights. We may also have to seek a license for the technology. Such licenses may not be available on reasonable terms, if at all, and may significantly increase our operating expenses or may require us to restrict our business activities and limit our ability to deliver certain solutions or features. We may also be required to develop alternative non-infringing technology, which could require significant effort and expense and/or cause us to alter our platform, which could harm our business. Large indemnity obligations, whether for intellectual property or in certain limited circumstances, other claims, would harm our business, operating results and financial condition.

Additionally, our platform may be used by our customers and other third parties who obtain access to our solutions for purposes other than for which our platform was intended.

We maintain insurance to protect against certain claims associated with the use of our platform, but our insurance coverage may not adequately cover the claims asserted against us. In addition, even claims that ultimately are unsuccessful could result in our expenditure of funds in litigation, divert management's time and other resources, and harm our business and reputation. We have offered some of our customers a limited warranty, subject to certain conditions. Any failure or refusal of our insurance providers to provide the expected insurance benefits to us after we have remediated warranty claims would cause us to incur significant expense or cause us to cease offering warranties which could damage our reputation, cause us to lose customers, expose us to liability claims by our customers, negatively impact our sales and marketing efforts, and have an adverse effect on our business, operating results, and financial condition. Further, although the terms of the warranty do not allow those customers to use warranty claim payments to fund payments to persons on the U.S. Treasury Department's Office of Foreign Assets Control (OFAC), list of Specially Designated Nationals and Blocked Persons or who are otherwise subject to U.S. sanctions, we cannot assure you that all of our customers will comply with our warranty terms or refrain from taking actions, in violation of our warranty and applicable law.

Risks Related to our People

We rely on our management team and other key employees and will need additional personnel to grow our business, and the loss of one or more key employees or our inability to hire, integrate, train, manage, retain, and motivate qualified personnel, including members of our board of directors, could harm our business.

Our future success is dependent, in part, on our ability to hire, integrate, train, manage, retain, and motivate the members of our management team and other key employees throughout our organization. The loss of key personnel, including key members of our management team or members of our board of directors, as well as certain of our key marketing, sales, finance, support, product development, people team, or technology personnel, could disrupt our operations and have an adverse effect on our ability to grow our business. In particular, we are highly dependent on the services of Tomer Weingarten, our co-founder, Chairman of the Board of Directors, President, and Chief Executive Officer, who is critical to the development of our technology, platform, future vision, and strategic direction. From time to time, there have been and may in the future be changes in our management team. While we seek to manage any such transitions carefully, such changes may result in a loss of institutional knowledge, cause disruptions to our business and negatively affect our business.

Competition for highly skilled personnel is intense, especially in the San Francisco Bay Area and in Israel, where we have a substantial presence and need for highly skilled personnel, and we may not be successful in hiring or retaining qualified personnel to fulfill our current or future needs. More generally, the technology industry, and the cybersecurity industry more specifically, is also subject to substantial and continuous competition for engineers with high levels of experience in designing, developing and managing software and related services. Moreover, the industry in which we operate generally experiences high employee attrition. We have, from time to time, experienced, and we expect to continue to experience, difficulty in hiring and retaining highly skilled employees with appropriate qualifications. For example, in recent years, recruiting, hiring and retaining employees with expertise in the cybersecurity industry has become increasingly difficult as the demand for cybersecurity professionals has increased as a result of the recent cybersecurity attacks on global corporations and governments. We may be required to provide more training to our personnel than we currently anticipate. Further, labor is subject to external factors that are beyond our control, including our industry's highly competitive market for skilled workers and leaders, cost inflation, the continuing effects of the COVID-19 pandemic, overall macroeconomics and workforce participation rates.

Restrictive immigration policies or legal or regulatory developments relating to immigration may also negatively affect our efforts to attract and hire new personnel as well as retain our existing personnel. Changes in U.S. immigration and work authorization laws and regulations can be significantly affected by political forces and levels of economic activity. Our business may be adversely affected if legislative or administrative changes to immigration or visa laws and regulations impair our hiring processes.

Moreover, many of the companies with which we compete for experienced personnel have greater resources than we have. Our competitors also may be successful in recruiting and hiring members of our management team, sales team or other key employees, and it may be difficult for us to find suitable replacements on a timely basis, on competitive terms, or at all. We have in the past, and may in the future, be subject to allegations that employees we hire have been improperly solicited, or that they have divulged proprietary or other confidential information or that their former employers own such employees' inventions or other work product, or that they have been hired in violation of non-compete provisions or non-solicitation provisions.

In addition, job candidates and existing employees often consider the value of the equity awards and other compensation they receive in connection with their employment. If the perceived value of our compensatory package declines, it may adversely affect our ability to attract and retain highly skilled employees. If we fail to attract new personnel or fail to retain and motivate our current personnel, our business and future growth prospects would be severely harmed. Further, our competitors may be successful in recruiting and hiring members of our management team or other key employees, and it may be difficult for us to find suitable replacements on a timely basis, on competitive terms, or at all. In recent years, the increased availability of hybrid or remote working arrangements has expanded the pool of companies that can compete for our employees and employment candidates. Although we have entered into employment agreements with our key employees, these agreements are on an "at-will" basis, meaning they are able to terminate their employment with us at any time. If we fail to attract new personnel or fail to retain and motivate our current personnel, our business and future growth prospects would be severely harmed.

If we do not effectively hire, integrate, train, manage, and retain additional sales personnel, and expand our sales and marketing capabilities, we may be unable to increase our customer base and increase sales to our existing customers.

Our ability to increase our customer base and achieve broader market adoption of our platform will depend to a significant extent on our ability to continue to expand our sales and marketing operations. We have and plan to continue to dedicate significant resources to sales and marketing programs and to expand our sales and marketing capabilities to target additional potential customers, but there is no guarantee that we will be successful in attracting and maintaining additional customers. If we are unable to find efficient ways to deploy our sales and marketing investments or if our sales and marketing programs are not effective, our business and operating results would be adversely affected.

Furthermore, we plan to continue expanding our sales force and there is significant competition for sales personnel with the skills and technical knowledge that we require. Our ability to achieve revenue growth will depend, in part, on our success in hiring, integrating, training, managing, and retaining sufficient numbers of sales personnel to support our growth, particularly in international markets. New hires require significant training and may take extended time before they are productive. Our recent hires and planned hires may not become productive as quickly as we expect, or at all, and we may be unable to hire or retain sufficient numbers of qualified individuals in the markets where we do business or plan to do business. Moreover, our international expansion may be slow or unsuccessful if we are unable to retain qualified personnel with international experience, language skills and cultural competencies in the geographic markets in which we target.

If we are unable to hire, integrate, train, manage, and retain a sufficient number of effective sales personnel, or the sales personnel we hire are not successful in obtaining new customers or increasing sales to our existing customer base, our business, operating results and financial condition will be adversely affected.

Any inability to maintain a high-quality customer support organization could lead to a lack of customer satisfaction, which could hurt our customer relationships and adversely affect our business, operating results, and financial condition.

Once our platform is deployed within our customers' computing environments, our customers rely on our technical support services to assist with service customization and optimization and to resolve certain issues relating to the implementation and maintenance of our platform and advanced services. If we do not effectively assist our customers in deploying our platform, succeed in helping our customers quickly resolve technical issues, or provide

effective ongoing support, our ability to sell additional products and services as part of our platform to existing customers would be adversely affected and our reputation with potential customers could be damaged.

In addition, our sales process is highly dependent on our product and business reputation and on positive recommendations, referrals, and peer promotions from our existing customers. Any failure to maintain high-quality technical support, or a market perception that we do not maintain high-quality support, could adversely affect our reputation, our ability to sell our services to existing and prospective customers, and our business, operating results and financial condition.

We believe that our corporate culture has contributed to our success, and if we cannot maintain this culture as we grow, we could lose the innovation, creativity, and teamwork fostered by our culture, and our business may be harmed.

We believe that our corporate culture has been, and will continue to be a key contributor to our success. If we do not continue to develop our corporate culture as we grow and evolve, it could harm our ability to foster the innovation, inclusion, creativity, and teamwork that we believe is important to support our growth. As we implement more complex organizational structures, we may find it increasingly difficult to maintain the beneficial aspects of our corporate culture, which could negatively impact our future success. We are also taking steps to develop a more inclusive and diverse workforce, however, there is no guarantee that we will be able to do so.

Risks Related to Our Intellectual Property

Our proprietary rights may be difficult to enforce, which could enable others to copy or use aspects of our platform without compensating us.

We rely primarily on patent, trademark, copyright and trade secrets laws, and confidentiality agreements and contractual provisions to protect our technology. Valid patents may not issue from our pending applications, and the claims eventually allowed on any patents may not be sufficiently broad to protect our technology or platform. Any issued patents may be challenged, invalidated or circumvented, and any rights granted under these patents may not actually provide adequate defensive protection or competitive advantages to us. Patent applications in the United States are typically not published until at least 18 months after filing, or, in some cases, not at all, and publications of discoveries in industry-related literature lag behind actual discoveries. We cannot be certain that we were the first to make the inventions claimed in our pending patent applications or that we were the first to file for patent protection. Additionally, the process of obtaining patent protection is expensive and time-consuming, and we may not be able to prosecute all necessary or desirable patent applications at a reasonable cost or in a timely manner. In addition, recent changes to the patent laws in the United States may bring into question the validity of certain software patents and may make it more difficult and costly to prosecute patent applications. Such changes may lead to uncertainties or increased costs and risks surrounding the prosecution, validity, ownership, enforcement, and defense of our issued patents and patent applications and other intellectual property, the outcome of third-party claims of infringement, misappropriation, or other violation of intellectual property brought against us and the actual or enhanced damages (including treble damages) that may be awarded in connection with any such current or future claims, and could have a material adverse effect on our business, operating results, and financial condition.

Despite our efforts to protect our proprietary rights, unauthorized parties may attempt to copy aspects of our platform or obtain and use information that we regard as proprietary. We generally enter into confidentiality or license agreements with our employees, consultants, vendors, and customers, and generally limit access to and distribution of our proprietary information. However, such agreements may not be enforceable in full or in part in all jurisdictions and any breach could negatively affect our business and our remedy for such breach may be limited. The contractual provisions that we enter into may not prevent unauthorized use or disclosure of our proprietary technology or intellectual property rights and may not provide an adequate remedy in the event of unauthorized use or disclosure of our proprietary technology or intellectual property rights. Lastly, the measures we employ to limit the access and distribution of our proprietary information may not prevent unauthorized use or disclosure of our proprietary technology or intellectual property. As such, we cannot guarantee that the steps taken by us will prevent misappropriation of our technology. Policing unauthorized use of our technology or platform is difficult. In addition, the laws of some foreign countries do not protect our proprietary rights to the same extent as the laws of the United

States, and many foreign countries do not enforce these laws as diligently as government agencies and private parties in the United States. For example, many foreign countries limit the enforceability of patents against certain third parties, including government agencies or government contractors. In these countries, patents may provide limited or no benefit. Effective trade secret protection may also not be available in every country in which our products are available or where we have employees or independent contractors. The loss of trade secret protection could make it easier for third parties to compete with our products by copying functionality. In addition, any changes in, or unexpected interpretations of, the trade secret and employment laws in any country in which we operate may compromise our ability to enforce our trade secret and intellectual property rights. From time to time, legal action by us may be necessary to enforce our patents and other IP rights, to protect our trade secrets, to determine the validity and scope of the proprietary rights of others or to defend against claims of infringement or invalidity. Such litigation could result in substantial costs and diversion of resources and could negatively affect our business, operating results and financial condition. If we are unable to protect our proprietary rights (including aspects of our software and platform protected other than by patent rights), we will find ourselves at a competitive disadvantage to others who need not incur the additional expense, time and effort required to create our platform and other innovative products that have enabled us to be successful to date. Moreover, we may need to expend additional resources to defend our intellectual property rights in foreign countries, and our inability to do so could impair our business or adversely affect our international expansion.

Third parties have claimed and may claim that our platform infringes their intellectual property rights and this may create liability for us or otherwise adversely affect our business, operating results, and financial condition.

Third parties have claimed, and may claim in the future, that our current or future products and services infringe their intellectual property rights, and such claims may result in legal claims against our channel partners, our alliance partners, our customers and us. These claims may damage our brand and reputation, harm our customer relationships, and create liability for us. We expect the number of such claims to increase as the number of products and services and the level of competition in our market grows, as the functionality of our platform overlaps with that of other products and services, and as the volume of issued software patents and patent applications continues to increase. We generally agree in our customer and partner contracts to indemnify customers for certain expenses or liabilities they incur as a result of third-party intellectual property infringement claims associated with our platform. To the extent that any claim arises as a result of third-party technology we have licensed for use in our platform, we may be unable to recover from the appropriate third party any expenses or other liabilities that we incur.

Companies in the software and technology industries, including some of our current and potential competitors, own large numbers of patents, copyrights, trademarks, and trade secrets and frequently enter into litigation based on allegations of infringement or other violations of intellectual property rights. In addition, many of these companies have the capability to dedicate substantially greater resources to enforce their intellectual property rights and to defend claims that may be brought against them. Furthermore, patent holding companies, non-practicing entities, and other adverse patent owners that are not deterred by our existing intellectual property protections may seek to assert patent claims against us. From time to time, third parties, including certain of these leading companies, have invited us to license their patents and may, in the future, assert patent, copyright, trademark, or other intellectual property rights against us, our channel partners, our alliance partners, or our customers. We have received, and may in the future receive, notices that claim we have misappropriated, misused, or infringed other parties' intellectual property rights, and, to the extent we gain greater market visibility, we face a higher risk of being the subject of intellectual property infringement claims. In May 2021, and thereafter, we have received communications from International Business Machines Corporation (IBM), alleging that we infringe on U.S. patents held by IBM. We have also asserted that IBM infringes certain patents held by us. To date, no litigation has been filed in this matter. Based on our review of the patents at issue, we believe we have meritorious defenses to IBM's allegations, although there can be no assurance that litigation will not commence, or that we will be successful in such litigation or reaching a business resolution that is satisfactory to us. In November 2022 we received communications from AT&T alleging that our platform integrated into an AT&T offering is subject to a third-party patent infringement claim and that we may be required to indemnify AT&T. To date, no litigation has been filed in this matter. Based on our review and analysis of the matter and allegations at issue, we are vigorously contesting the indemnity claim, although, there can be no assurances that litigation will not commence, that we will be successful in such litigation, or that we will reach a satisfactory business resolution.

There may be third-party intellectual property rights, including issued or pending patents and trademarks, that cover significant aspects of our technologies or business methods and assets. We may also face exposure to third-party intellectual property infringement, misappropriation, or violation actions if we engage software engineers or other personnel who were previously engaged by competitors or other third parties and those personnel inadvertently or deliberately incorporate proprietary technology of third parties into our products. In addition, we may lose valuable intellectual property rights or personnel. A loss of key personnel or their work product could hamper or prevent our ability to develop, market, and support potential products or enhancements, which could severely harm our business. Any intellectual property claims, with or without merit, could be very time-consuming, could be expensive to settle or litigate, and could divert our management's attention and other resources. These claims could also subject us to significant liability for damages, potentially including treble damages if we are found to have willfully infringed patents or copyrights, and may require us to indemnify our customers for liabilities they incur as a result of such claims. These claims could also result in our having to stop using technology found to be in violation of a third party's rights. We might be required to seek a license for the intellectual property, which may not be available on reasonable terms or at all. Even if a license were available, we could be required to pay significant royalties, which would increase our operating expenses. Alternatively, we could be required to develop alternative non-infringing technology, which could require significant time, effort, and expense, and may affect the performance or features of our platform. If we cannot license or develop alternative non-infringing substitutes for any infringing technology used in any aspect of our business, we would be forced to limit or stop sales of our platform and may be unable to compete effectively. Any of these results would adversely affect our business, operating results, and financial condition.

We license technology from third parties, and our inability to maintain those licenses could harm our business.

We currently incorporate, and will in the future incorporate, technology that we license from third parties, including software, into our solutions. Licensing technologies from third parties exposes us to increased risk of being the subject of intellectual property infringement and vulnerabilities due to, among other things, our lower level of visibility into the development process with respect to such technology and the care taken to safeguard against risks. We cannot be certain that our licensors do not or will not infringe on the intellectual property rights of third parties or that our licensors have or will have sufficient rights to the licensed intellectual property in all jurisdictions in which we may sell our platform. Some of our agreements with our licensors may be terminated by them for convenience, or otherwise provide for a limited term. If we are unable to continue to license technology because of intellectual property infringement claims brought by third parties against our licensors or against us, or if we are unable to continue our license agreements or enter into new licenses on commercially reasonable terms, our ability to develop and sell solutions and services containing or dependent on that technology would be limited, and our business, including our financial conditions, cash flows and results of operations could be harmed. Additionally, if we are unable to license technology from third parties, we may be forced to acquire or develop alternative technology, which we may be unable to do in a commercially feasible manner, or at all, and may require us to use alternative technology of lower quality or performance standards. This could limit or delay our ability to offer new or competitive solutions and increase our costs. Third-party software we rely on may be updated infrequently, unsupported or subject to vulnerabilities that may not be patched in a timely manner, any of which may expose our solutions to vulnerabilities. As a result, our business, operating results, and financial condition would be adversely affected.

Some of our technology incorporates "open source" software, which could negatively affect our ability to sell our platform and subject us to possible litigation.

Our platform contains third-party open source software components, and failure to comply with the terms of the underlying open source software licenses could restrict our ability to sell our products and subscriptions. The use and distribution of open source software may entail greater risks than the use of third-party commercial software, as open source licensors generally do not provide warranties or other contractual protections regarding infringement claims or the quality of the code, which they are not typically required to maintain and update, and they can change the license terms on which they offer the open source software. Although we monitor our use of open source software in an effort both to comply with the terms of the applicable open source licenses and to avoid subjecting our products to conditions we do not intend, many of the risks associated with use of open source software cannot be

eliminated and could negatively affect our business. In addition, the wide availability of source code used in our solutions could expose us to security vulnerabilities.

Some open source licenses contain requirements that we make available source code for modifications or derivative works we create based upon our use and distribution of the open source software. If we combine and distribute our proprietary software with open source software in a certain manner, we could, under certain open source licenses, be required to release combined the source code of our proprietary software to the public, including authorizing further modification and redistribution, or otherwise be limited in the licensing of our services, each of which could provide an advantage to our competitors or other entrants to the market, create security vulnerabilities in our solution, require us to re-engineer all or a portion of our platform, and reduce or eliminate the value of our services. This would allow our competitors to create similar products with lower development effort and time and ultimately could result in a loss of sales for us.

The terms of many open source licenses have not been interpreted by U.S. courts, and there is a risk that these licenses could be construed in ways that could impose unanticipated conditions or restrictions on our ability to commercialize products and subscriptions incorporating such software. Moreover, we cannot assure you that our processes for controlling our use of open source software in our products and subscriptions will be effective. From time to time, we may face claims from third parties asserting ownership of, or demanding release of, the open source software or derivative works that we developed using such software (which could include our proprietary source code), or otherwise seeking to enforce the terms of the applicable open source license. These claims, regardless of validity, could result in time consuming and costly litigation, divert management's time and attention away from developing the business, expose us to customer indemnity claims, or force us to disclose source code. Litigation could be costly for us to defend, result in paying damages, entering into unfavorable licenses, have a negative effect on our operating results and financial condition, or cause delays by requiring us to devote additional research and development resources to change our solution.

Risks Related to Legal and Regulatory Matters

We are subject to laws and regulations, including governmental export and import controls, sanctions and anti-corruption laws, that could impair our ability to compete in our markets and subject us to liability if we are not in full compliance with applicable laws.

We are subject to laws and regulations, including governmental export and import controls, that could subject us to liability or impair our ability to compete in our markets. Our platform and related technology is subject to U.S. export controls, including the U.S. Department of Commerce's Export Administration Regulations (EAR), and we and our employees, representatives, contractors, agents, intermediaries, and other third parties are also subject to various economic and trade sanctions regulations administered by OFAC and other U.S. government agencies. We incorporate standard encryption algorithms into our platform, which, along with the underlying technology, may be exported outside of the U.S. only with the required export authorizations, including by license, license exception or other appropriate government authorizations, which may require the filing of an encryption registration and classification request. We also offer certain customers a ransomware warranty in addition to their subscriptions, providing coverage in the form of a limited monetary payment if they are affected by a ransomware attack (as specified in our ransomware warranty agreement), and though the terms of the warranty do not allow those customers to use warranty claim payments to fund payments to persons on OFAC's list of Specially Designated Nationals and Blocked Persons or who are otherwise prohibited to receive such payments under U.S. sanctions, we cannot assure you that all of our customers will comply with our warranty terms or refrain from taking actions in violation of our warranty and applicable law. Furthermore, U.S. export control laws and economic sanctions prohibit the export and re-export of certain hardware and software and the provision of certain cloud-based solutions to certain countries, governments and persons targeted by U.S. sanctions and for certain end-uses. As an example, following Russia's invasion of Ukraine, the United States and other countries imposed economic sanctions and severe export control restrictions against Russia and Belarus. The United States and its allies could expand and strengthen these sanctions and export restrictions and take other actions should the conflict further escalate. These restrictions would further impact our ability to do business in certain parts of the world and to do business with certain persons and entities, including selling our services and using local developers. We also collect information about cyber threats from open sources, intermediaries and third parties that we make available to our customers in

our threat industry publications. While we have implemented certain procedures to facilitate compliance with applicable laws and regulations in connection with the collection and distribution of this information, we cannot assure you that these procedures have been effective or that we, or third parties who we do not control, have complied with all laws or regulations in this regard. Failure by our employees, representatives, contractors, channel partners, agents, intermediaries, or other third parties to comply with applicable laws and regulations in the collection and distribution of this information also could have negative consequences to us, including reputational harm, government investigations, and penalties.

Although we take precautions to prevent our information collection practices and services from being provided in violation of such laws, our information collection practices and services may have been in the past, and could in the future be, provided in violation of such laws. If we or our employees, representatives, contractors, channel partners, agents, intermediaries, or other third parties fail to comply with these laws and regulations, we could be subject to civil or criminal penalties, including the possible loss of export privileges and fines. We may also be adversely affected through reputational harm, loss of access to certain markets or otherwise. Obtaining the necessary authorizations, including any required license, for a particular transaction may be time-consuming, is not guaranteed and may result in the delay or loss of sales opportunities.

Various countries regulate the import of certain encryption technology, including through import permit and license requirements, and have enacted laws that could limit our ability to distribute our platform or could limit our customers' ability to implement our platform in those countries. Additionally, export restrictions recently imposed on Russia and Belarus specifically limit the export of encryption hardware, software and related source code and technology to these locations which could limit our ability to provide our software and services to these countries. Changes in our platform or changes in export and import regulations may create delays in the introduction of our platform into international markets, prevent our customers with international operations from deploying our platform globally or, in some cases, prevent the export or import of our platform to certain countries, governments or persons altogether. Any change in export or import regulations, economic sanctions or related legislation, shift in the enforcement or scope of existing regulations, or change in the countries, governments, persons or technologies targeted by such regulations, could result in decreased use of our platform by, or in our decreased ability to export or sell our platform to, existing or potential customers with international operations. Any decreased use of our platform or limitation on our ability to export or sell our platform would adversely affect our business, operating results, and financial condition.

We are also subject to the United States Foreign Corrupt Practices Act of 1977 (FCPA), as amended, the United Kingdom Bribery Act 2010 (the Bribery Act), and other anti-corruption, sanctions, anti-bribery, anti-money laundering and similar laws in the United States and other countries in which we conduct activities. Anti-corruption and anti-bribery laws, which have been enforced aggressively and are interpreted broadly, prohibit companies and their employees, agents, intermediaries and other third parties from promising, authorizing, making or offering improper payments or other benefits to government officials and others in the public, and in certain cases, private sector. We leverage third parties, including intermediaries, agents and channel partners, to conduct our business in the United States and abroad, to sell subscriptions to our platform and to collect information about cyber threats. We and these third parties may have direct or indirect interactions with officials and employees of government agencies or state-owned or affiliated entities and we may be held liable for the corrupt or other illegal activities of these third-party business partners and intermediaries, our employees, representatives, contractors, channel partners, agents, intermediaries and other third parties, even if we do not explicitly authorize such activities. While we have policies and procedures to address compliance with FCPA, Bribery Act and other anti-corruption, sanctions, anti-bribery, anti-money laundering and similar laws, we cannot assure you that they will be effective, or that all of our employees, representatives, contractors, channel partners, agents, intermediaries or other third parties have not taken, or will not take actions, in violation of our policies and applicable law, for which we may be ultimately held responsible. As we increase our international sales and business, including our business with government organizations, our risks under these laws may increase. Noncompliance with these laws could subject us to investigations, severe criminal or civil sanctions, settlements, prosecution, loss of export privileges, suspension or debarment from U.S. government contracts, other enforcement actions, disgorgement of profits, significant fines, damages, other civil and criminal penalties or injunctions, whistleblower complaints, adverse media coverage and

other consequences. Any investigations, actions or sanctions could harm our reputation, business, operating results, and financial condition.

If we fail to adequately protect personal information or other information we collect, process, share or maintain under applicable laws, our business, operating results, and financial condition could be adversely affected.

We receive, store, and process some personal information from our employees, customers, the employees of our customers, and our end users. This personal information is hosted by our third-party service providers. A wide variety of state, national, and international laws, as well as regulations and industry standards apply to the collection, use, retention, protection, disclosure, transfer and other processing of personal information and other information, the scope of which are changing, subject to differing interpretations, and may be inconsistent across countries or conflict with other rules. Data protection and privacy-related laws and regulations are evolving and may result in ever increasing regulatory and public scrutiny and escalating levels of enforcement and sanctions. Failure to comply with laws, regulations and industry standards regarding personal information or other information could adversely affect our business, operating results and financial condition.

Complying with these various laws and regulations could cause us to incur substantial costs or require us to change our business practices, systems, and compliance procedures in a manner adverse to our business.

In the United States, there are numerous federal and state consumer, privacy and data security laws and regulations governing the collection, use, disclosure, and protection of personal information, including security breach notification laws and consumer protection laws. Each of these laws is subject to varying interpretations and constantly evolving. Notably, but not necessarily limited to, we may be subject to:

- Controlling the Assault of Non-Solicited Pornography And Marketing Act (CAN-SPAM) and similar state consumer protection laws regarding the use of telephones and text messaging for marketing purposes.
- Section 5(a) of the Federal Trade Commission (FTC) Act for violating consumers' privacy rights or failing to take appropriate steps to keep consumers' personal information secure, resulting in a finding of an unfair act or practice.
- The CCPA, effective since January 1, 2020, which created new data privacy obligations for covered companies and provided new privacy rights to California residents, including the right to opt out of certain disclosures of their information and receive detailed information about how their personal information is used. The CCPA provides for civil penalties for violations, as well as a private right of action for data breaches that is expected to increase data breach litigation. A ballot initiative called the California Privacy Rights Act, or CPRA, took effect January 1, 2023 (with a look back to January 2022), with enforcement beginning on July 1, 2023, and significantly modifies the CCPA, including by expanding consumers' rights with respect to certain sensitive personal data. The CPRA also creates a new state agency, known as the California Privacy Protection Agency, that will be vested with authority to implement and enforce the CCPA and the CPRA. Potential uncertainty surrounding the CCPA and CPRA may increase our compliance costs and potential liability, particularly in the event of a data breach, and could have a material adverse effect on our business.
- Other states have followed California: Virginia enacted the Virginia Consumer Data Protection Act that also became effective January 1, 2023; Colorado enacted its Colorado Privacy Act, which will become effective July 1, 2023; Connecticut passed the Connecticut Data Privacy Act (CDPA), which will become effective July 1, 2023; and Utah enacted the Utah Consumer Privacy Act (UCPA), which will become effective December 31, 2023; and as the year 2023 began, four states had pending consumer privacy legislation under review, which if enacted, would add additional costs and expense of resources to maintain compliance.

In certain circumstances, we may be subject to the EU General Data Protection Regulation (GDPR) (established in 2018 and implemented by countries in the EEA) and the U.K. General Data Protection Regulation and U.K. Data Protection Act 2018 (U.K. GDPR), which respectively govern the collection, use, disclosure, transfer or other processing of personal data of natural persons, and it applies extra-territorially and imposes onerous requirements on

controllers and processors of personal data, including, for example: (i) accountability and transparency requirements, and enhanced requirements for obtaining valid consent; (ii) obligations to consider data protection as any new products or services are developed and to limit the amount of personal data processed; (iii) obligations to comply with data protection rights of data subjects; and (iv) reporting of personal data breaches to the supervisory authority without undue delay (and no later than 72 hours).

Companies that must comply with the GDPR face increased compliance obligations and risk, including more robust regulatory enforcement of data protection requirements and potential fines for noncompliance of up to €20 million or 4 percent of the annual global revenues of the noncompliant company, whichever is greater. Additionally, following the withdrawal by the United Kingdom (U.K.) from the European Union and the EEA, companies must comply with both the GDPR and the U.K. GDPR as incorporated into United Kingdom national law, the latter regime having the ability to separately fine up to the greater of £17.5 million or 4 percent of global turnover. In addition to the foregoing, a breach of the GDPR or U.K. GDPR could result in regulatory investigations, reputational damage, orders to cease or change our processing of our data, enforcement notices, and/or assessment notices (for a compulsory audit). We may also face civil claims including representative actions and other class action type litigation (where individuals have suffered harm), potentially amounting to significant compensation or damages liabilities, as well as associated costs, diversion of internal resources, and reputational harm.

The GDPR and U.K. GDPR requires, among other things, that personal information only be transferred outside of the EEA, or the U.K., respectively to jurisdictions that have been deemed adequate (also known as “Third Countries,” which at present time includes the United States) by the European Commission or by the U.K. data protection regulator, respectively. Accordingly, personal information may not be transferred to those jurisdictions that have not been deemed adequate, unless steps are taken to legitimize those data transfers. Switzerland follows similar legal practices. Previously, we relied on the E.U.-U.S. Privacy Shield framework to provide a mechanism for the transfer of data from E.U. Member States to the United States, but this was invalidated by the European Court of Justice (CJEU) on July 16, 2020, on the grounds that the Privacy Shield failed to offer adequate protections to E.U. personal information transferred to the United States. We previously relied on our own, as well as our vendors’, Privacy Shield certification for the purposes of transferring personal data from the EEA to the United States in compliance with the GDPR/U.K. GDPR’s data export conditions, which are no longer allowed.

One such alternative to the Privacy Shield is the use of Standard Contractual Clauses (SCCs), a standard form of contract approved by the European Commission as an adequate personal data transfer mechanism, may not be alone sufficient to protect data transferred to the United States or other Third Countries under certain circumstances without making a case-by-case basis assessment of the legal regime applicable in the destination country according to the CJEU. On June 28, 2021, the European Commission issued an adequacy decision for personal information transfers from the EEA to the U.K., with a sunset clause of four years, meaning that the European Commission will review and renew only if the European Commission considers that the U.K. continues to ensure an adequate level of data protection. Notably, the European Commission reserved a right to intervene at any time during the four-year adequacy period if the U.K. deviates from the level of protection then in place. If this adequacy decision is reversed by the European Commission, we would have to implement protection measures such as the SCCs for data transfers between the E.U. and the U.K. or find alternative solutions for the compliant transfer of personal data from the E.U. into the U.K.

Some countries (including some outside the EEA) also are considering or have passed legislation requiring local storage and processing of data, or similar requirements, which could increase the cost and complexity of delivering our products and services if we were to operate in those countries. If we are required to implement additional measures to transfer data from the EEA, this could increase our compliance costs, and could adversely affect our business, financial condition and results of operations.

The myriad international and U.S. privacy and data breach laws are not consistent, and compliance in the event of a widespread data breach is difficult and may be costly. In many jurisdictions, enforcement actions and consequences for noncompliance are also rising. In addition to government regulation, privacy advocates and industry groups may propose new and different self-regulatory standards that either legally or contractually apply to us.

As supervisory authorities continue to issue further guidance on personal information transfers (including regarding data export and circumstances in which we cannot use the SCCs), we could suffer additional costs, complaints, or regulatory investigations or fines. If we are otherwise unable to transfer personal data between and among countries and regions in which we operate, it could affect the manner in which we provide our services, adversely affecting our financial results, and possibly making it necessary to establish systems in the EEA, Switzerland, and the U.K. to maintain personal data originating from those jurisdictions that adds expenses and may create distractions from our other business pursuits. Loss, retention or misuse of certain information and alleged violations of laws and regulations relating to privacy and data security, and any relevant claims, may expose us to potential liability and may require us to expend significant resources on data security and in responding to and defending such allegations and claims.

We are also subject to evolving E.U. and U.K. privacy laws on cookies and electronic marketing. In the E.U. and the U.K., informed opt-in consent is required for the placement of a cookie or similar technologies on a user's device and for direct electronic marketing. The GDPR also imposes conditions on obtaining valid consent, such as a prohibition on pre-checked consents and a requirement to ensure separate consents are sought for each type of cookie or similar technology. While we anticipate the development of the ePrivacy Regulation to govern cookies and e-marketing, recent European court decisions and regulators' guidance are driving increased attention to cookies and tracking technologies. If regulators start to enforce the strict approach in recent guidance, this could lead to substantial costs, require significant systems changes, limit the effectiveness of our marketing activities, divert the attention of our technology personnel, adversely affect our margins, increase costs and subject us to additional liabilities. Regulation of cookies and similar technologies, and any decline of cookies or similar online tracking technologies as a means to identify and potentially target users, may lead to broader restrictions and impairments on our marketing and personalization activities and may negatively impact our efforts to understand users. Similar concerns may happen under the new CPRA regime in California.

Additionally, by expanding into the E.U. and U.K., we may also trigger Article 3(2) of the GDPR/U.K. GDPR directly as we may be considered to be monitoring data subjects. To the extent we process personal data on behalf of our customers for the provision of services, we have, and may in the future, also be required to enter into data processing agreements which comply with Article 28 of the GDPR/U.K. GDPR.

We depend on a number of third parties in relation to the operation of our business, a number of which process personal data on our behalf or as our sub-processor. To the extent required by applicable law, we attempt to mitigate the associated risks of using third parties by performing security assessments and detailed due diligence, entering into contractual arrangements to ensure that providers only process personal data according to our instructions or comparable instructions to the instructions of our customer (as applicable), and that they have sufficient technical and organizational security measures in place. There is no assurance that these contractual measures and our own privacy and security-related safeguards will protect us from the risks associated with the third-party processing, storage and transmission of such information. Any violation of data or security laws by our third-party processors could have a material adverse effect on our business and result in the fines and penalties under the GDPR and the U.K. GDPR outlined above.

In recent years, some regulators have proposed or introduced cybersecurity licensing requirements or certification regimes for specific sectors, such as critical infrastructure. These may impose new requirements on us or our current or prospective customer including, but not limited to, data processing locations, breach notification, and security standards. Such requirements may cause us to incur significant organizational costs and increase barriers of entry into new markets. New worldwide data protection laws, including the U.S. and European jurisdictions described above, may lead to ever changing definitions of personal information and other sensitive information which may also limit or inhibit our ability to operate or expand our business, including limiting strategic partnerships that may involve the sharing of data. Notably some foreign jurisdictions require that certain types of data be retained on servers within these respective jurisdictions. Our failure to comply with applicable laws, directives, and regulations may result in enforcement action against us, including fines, and damage to our reputation, any of which may have an adverse effect on our business and operating results.

Any failure or perceived failure by us, even if unfounded, to comply with applicable privacy and data security laws and regulations, our privacy policies, or our privacy-related obligations to customers, users or other third

parties, or any compromise of security that results in the unauthorized release or transfer of personal information or other customer data, may result in governmental enforcement actions, litigation, or public statements against us by consumer advocacy groups or others and could cause our users to lose trust in us, which would have an adverse effect on our reputation and business. For example, in 2017, we reached a consent agreement with the FTC, to resolve an investigation relating to certain disclosures in our privacy policy. The consent agreement requires us, among other things, to provide information about our compliance with the FTC order and about representations made in our marketing materials. We may be subject to future investigations and legal proceedings by the FTC or other regulators. A such, it is possible that a regulatory inquiry might result in changes to our policies or business practices. Violation of existing or future regulatory orders or consent decrees could subject us to substantial monetary fines and other penalties that could negatively affect our operating results and financial condition. In addition, it is possible that future orders issued by, or enforcement actions initiated by, regulatory authorities could cause us to incur substantial costs or require us to change our business practices in a manner materially adverse to our business.

Any significant change to applicable laws, regulations or industry practices regarding the use or disclosure of our customers' data, or regarding the manner in which the express or implied consent of customers for the use and disclosure of such data is obtained – or in how these applicable laws, regulations or industry practices are interpreted and enforced by state, federal and international privacy regulators – could require us to modify our services and features, possibly in a material manner, may subject us to regulatory enforcement actions and fines, and may limit our ability to develop new products, services and features that make use of the data that our customers voluntarily share with us.

Any security breach or incident, including those resulting from a cybersecurity attack, phishing attack, unauthorized access, unauthorized usage, virus, malware, ransomware, denial of service, credential stuffing attack, supply chain attack, hacking or similar breach involving our networks and systems, or those of third parties upon which we rely, could result in the loss of customer data, including personal information, disruption to our operations, significant remediation costs, lost revenue, increased insurance premiums, damage to our reputation, litigation, regulatory investigations, or other liabilities. These attacks may come from individual hackers, criminal groups, and state-sponsored organizations, and security breaches and incidents may arise from other sources, such as employee or contractor error or malfeasance. Cyber threats are evolving and becoming increasingly sophisticated and complex, increasing the difficulty of detecting and successfully defending against them. As a cybersecurity company, we have been and may continue to be specifically targeted by bad actors for attacks intended to circumvent our security capabilities as an entry point into customers' endpoints, networks, or systems. Our industry is experiencing an increase in phishing attacks and unauthorized scans of systems searching for vulnerabilities or misconfigurations to exploit. If our security measures are breached or otherwise compromised as a result of third-party action, employee or contractor error, defect, vulnerability or bug in our products or products of third parties upon which we rely, malfeasance or otherwise, including any such breach or compromise resulting in someone obtaining unauthorized access to our confidential information, including personal information or the personal information of our customers or others, or if any of these are perceived or reported to occur, we may suffer the loss, compromise, corruption, unavailability, or destruction of our or others' confidential information and personal information, we may face a loss in intellectual property protection, our reputation may be damaged, our business may suffer and we could be subject to claims, demands, regulatory investigations and other proceedings, indemnity obligations, and otherwise incur significant liability. Even the perception of inadequate security may damage our reputation and negatively impact our ability to win new customers and retain existing customers. Further, we could be required to expend significant capital and other resources to address any security incident or breach, and we may face difficulties or delays in identifying and responding to any security breach or incident.

Techniques used to sabotage or obtain unauthorized access to systems or networks are constantly evolving and, in some instances, are not identified until launched against a target. We and our third-party vendors and service providers may be unable to anticipate these techniques, react in a timely manner, or implement adequate preventative measures. Due to political uncertainty and military actions associated with Russia's invasion of Ukraine, we and our third-party vendors and service providers are vulnerable to a heightened risk of cybersecurity attacks, phishing attacks, viruses, malware, ransomware, hacking or similar breaches from nation-state and affiliated actors, including attacks that could materially disrupt our systems and operations, supply chain, and ability to

produce, sell and distribute our products and services as well as retaliatory cybersecurity attacks from Russian and Russian-affiliated actors against companies with a U.S. presence. In addition, laws, regulations, government guidance, and industry standards and practices in the United States and elsewhere are rapidly evolving to combat these threats. We may face increased compliance burdens regarding such requirements with regulators and customers regarding our products and services and also incur additional costs for oversight and monitoring of our own supply chain. We and our customers may also experience increased costs associated with security measures and increased risk of suffering cyberattacks, including ransomware attacks. Should we or the third-party vendors and service providers upon which we rely experience such attacks, including from ransomware or other security breaches or incidents, our operations may also be hindered or interrupted due to system disruptions or otherwise, with foreseeable secondary contractual, regulatory, financial and reputational harms that may arise from such an incident.

Further, we cannot assure that any limitations of liability provisions in our customer agreements, contracts with third-party vendors and service providers or other contracts would be enforceable or adequate or would otherwise protect us from any liabilities or damages with respect to any particular claim relating to a security breach or other security incident. We also cannot be sure that our existing insurance coverage will continue to be available on acceptable terms or will be available in sufficient amounts to cover claims related to a security incident or breach, or that the insurer will not deny coverage as to any future claim. The successful assertion of claims against us that exceed available insurance coverage, or the occurrence of changes in our insurance policies, including premium increases or the imposition of large deductible or coinsurance requirements, could have a material adverse effect on our business, including our financial condition, operating results, and reputation.

We may become involved in litigation that may adversely affect us.

From time to time, we have been subject to claims, suits and other proceedings. For example, we are currently the subject of litigation with BlackBerry Corp. For additional information regarding this litigation, see the section titled “Part I—Legal Proceedings.” Regardless of the outcome, legal proceedings can have an adverse impact on us because of legal costs and diversion of management attention and resources, and could cause us to incur significant expenses or liability, adversely affect our brand recognition or require us to change our business practices. The expense of litigation and the timing of this expense from period to period are difficult to estimate, subject to change and could adversely affect our business, operating results and financial condition. It is possible that a resolution of one or more such proceedings could result in substantial damages, settlement costs, fines and penalties that would adversely affect our business, consolidated financial condition, operating results or cash flows in a particular period. These proceedings could also result in reputational harm, sanctions, consent decrees or orders requiring a change in our business practices. Because of the potential risks, expenses and uncertainties of litigation, we may, from time to time, settle disputes, even where we have meritorious claims or defenses, by agreeing to settlement agreements. Because litigation is inherently unpredictable, we cannot assure you that the results of any of these actions will not have a material adverse effect on our business, operating results, financial condition, and prospects. Any of these consequences could adversely affect our business, operating results, and financial condition.

Risks Related to Financial and Accounting Matters

The requirements of being a public company, including maintaining adequate internal control over our financial and management systems, result in significant costs and may strain our resources, divert management’s attention, and affect our ability to attract and retain executive management and qualified board members.

As a public company we incur significant legal, accounting, and other expenses. We are subject to the reporting requirements of the Exchange Act, the Sarbanes-Oxley Act, Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 and the rules and regulations of the applicable listing standards of the New York Stock Exchange (NYSE). We expect that the requirements of these rules and regulations will continue to increase our legal, accounting, and financial compliance costs, make some activities more difficult, time-consuming, and costly, and place significant strain on our personnel, systems, and resources.

The Sarbanes-Oxley Act requires, among other things, that we maintain effective disclosure controls and procedures and internal control over financial reporting. We are continuing to develop and refine our disclosure

controls, internal control over financial reporting and other procedures that are designed to ensure information required to be disclosed by us in our financial statements and in the reports that we will file with the SEC is recorded, processed, summarized and reported within the time periods specified in SEC rules and forms, and information required to be disclosed in reports under the Exchange Act is accumulated and communicated to our principal executive and financial officers.

Our current controls and any new controls we develop may become inadequate because of changes in conditions in our business. Additionally, to the extent we acquire other businesses, the acquired companies may not have a sufficiently robust system of internal controls and we may uncover new deficiencies. Further, weaknesses in our internal controls may be discovered in the future. Any failure to develop or maintain effective controls, or any difficulties encountered in their implementation or improvement, could harm our operating results, may result in a restatement of our financial statements for prior periods, cause us to fail to meet our reporting obligations, and could adversely affect the results of periodic management evaluations and annual independent registered public accounting firm attestation reports regarding the effectiveness of our internal control over financial reporting that we are required to include in our annual reports on Form 10-K filed with the SEC beginning in fiscal year 2023. Ineffective disclosure controls and procedures and internal control over financial reporting could also cause investors to lose confidence in our reported financial and other information, which would likely have a negative effect on the market price of our Class A common stock. Our management is also required, pursuant to Section 404 of the Sarbanes-Oxley Act, to certify financial and other information in our quarterly and annual reports and provide an annual report on the effectiveness of our internal control over financial reporting.

In addition, changing laws, regulations, and standards relating to corporate governance and public disclosure, including those related to climate change and other ESG-focused disclosures, are creating uncertainty for public companies, increasing legal and financial compliance costs, and making some activities more time consuming. These laws, regulations, and standards are subject to varying interpretations, in many cases due to their lack of specificity, and, as a result, their application in practice may evolve over time as new guidance is provided by regulatory and governing bodies. This could result in continuing uncertainty regarding compliance matters and higher costs necessitated by ongoing revisions to disclosure and governance practices. We intend to continue to invest resources to comply with evolving laws, regulations, and standards, and this investment may result in increased general and administrative expenses and a diversion of management's time and attention from revenue-generating activities to compliance activities. If our efforts to comply with new laws, regulations, and standards differ from the activities intended by regulatory or governing bodies due to ambiguities related to their application and practice, regulatory authorities may initiate legal proceedings against us, and our business may be adversely affected.

We have incurred significant costs with respect to our directors' and officers' insurance coverage. In the future, it may be more expensive or more difficult for us to obtain director and officer liability insurance, and we may be required to accept reduced coverage or incur substantially higher costs to obtain coverage. These factors would also make it more difficult for us to attract and retain qualified members of our board of directors, particularly to serve on our audit committee and compensation committee, and qualified executive officers.

Being a public company requires significant resources and management oversight. As a result, management's attention may be diverted from other business concerns, which could harm our business, operating results, and financial condition.

We could be subject to additional tax liabilities and United States federal and global income tax reform could adversely affect us.

We are subject to U.S. federal, state, local and sales taxes in the United States and foreign income taxes, withholding taxes and transaction taxes in numerous foreign jurisdictions. Significant judgment is required in evaluating our tax positions and our worldwide provision for income taxes. During the ordinary course of business, there are many activities and transactions for which the ultimate tax determination is uncertain. In addition, our future income tax obligations could be adversely affected by changes in, or interpretations of, tax laws in the United States or in other jurisdictions in which we operate.

For example, the United States tax law legislation commonly referred to as the Tax Cuts and Jobs Act of 2017 (the Tax Act) (as modified by the Coronavirus Aid, Relief, Economic Security Act, the Families First Coronavirus Response Act and the American Rescue Plan Act), significantly reformed the Internal Revenue Code of 1986, as amended (or the Internal Revenue Code), reducing U.S. federal tax rates, making sweeping changes to rules governing international business operations, and imposing significant additional limitations on tax benefits, including the deductibility of interest and the use of net operating loss carryforwards. On August 16, 2022, President Biden signed the Inflation Reduction Act of 2022 (IRA) into law. The IRA contains certain tax measures, including a corporate alternative minimum tax of 15% on some large corporations and an excise tax of 1% on certain corporate stock buy-backs taking place after December 31, 2022. We are currently evaluating the various provisions of the IRA and currently anticipate that its impact, if any, will not be material to our operating results or cash flows. In the United States, Congress and the Biden administration continue to consider other proposed legislation to make various tax law changes. These proposals, could include changes to the existing framework in respect of income taxes, limitations on the ability of taxpayers to claim and utilize foreign tax credits, as well as add new types of non-income taxes (such as taxes based on a percentage of revenue or taxes applicable to digital services). In addition, the Organization for Economic Cooperation and Development (OECD) Inclusive Framework of 137 jurisdictions have joined a two-pillar plan to reform international taxation rules. The first pillar is focused on the allocation of taxing rights between countries for in-scope multinational enterprises that sell goods and services into countries with little or no local physical presence and is intended to apply to multinational enterprises with global turnover above 20 billion euros. The second pillar is focused on developing a global minimum tax rate of at least 15 percent applicable to in-scope multinational enterprises and is intended to apply to multinational enterprises with annual consolidated group revenue in excess of 750 million euro. While substantial work remains to be completed by the OECD and national governments on the implementation of these proposals, future tax reform resulting from these developments may result in changes to long-standing tax principles, which could adversely affect our effective tax rate or result in higher cash tax liabilities.

Due to the large and expanding scale of our international business activities, these types of changes to the taxation of our activities could impact the tax treatment of our foreign earnings, increase our worldwide effective tax rate, increase the amount of taxes imposed on our business, and harm our financial position. Such changes may also apply retroactively to our historical operations and result in taxes greater than the amounts estimated and recorded in our financial statements.

Our ability to use our net operating loss carryforwards and certain other tax attributes may be limited.

As of January 31, 2023, we had aggregate U.S. federal and state net operating loss carryforwards of $651.1 million and $338.3 million, respectively, which may be available to offset future taxable income for U.S. income tax purposes. If not utilized, the federal net operating loss carryforwards will begin to expire in 2031, and the state net operating loss carryforwards will begin to expire in 2024. In addition, as of January 31, 2023, we had federal research and development credit carryforwards of $2.0 million, which will begin to expire in 2037, and state research and development credit carryforwards of $2.0 million, which do not expire. We also had foreign net operating loss carryforwards of $289.8 million, as of January 31, 2023, which do not expire. Realization of these net operating loss and research and development credit carryforwards depends on future income, and there is a risk that certain of our existing carryforwards could expire unused and be unavailable to offset future income tax liabilities, which could adversely affect our operating results and financial condition.

In addition, under Sections 382 and 383 of the Internal Revenue Code, if a corporation undergoes an “ownership change,” generally defined as a greater than 50% change (by value) in ownership by “5 percent shareholders” over a rolling three-year period, the corporation’s ability to use its pre-change net operating loss carryovers and other pre-change tax attributes, such as research and development credits, to offset its post-change income or taxes may be limited. Similar rules apply under U.S. state tax laws. We have, and may in the future, experience ownership changes as a result of shifts in our stock ownership. As a result, if we earn net taxable income, our ability to use our pre-change U.S. net operating loss carryforwards to offset U.S. federal taxable income may be subject to limitations, which could potentially result in increased future tax liability to us.

We could be required to collect additional sales, use, value added, digital services, or other similar taxes or be subject to other liabilities with respect to past or future sales, that may increase the costs our customers would have to pay for our solutions and adversely affect our business, operating results, and financial condition.

We do not collect sales and use, value added, or similar taxes in all jurisdictions in which we have sales because we have been advised that such taxes are not applicable to our services in certain jurisdictions. Sales and use, value added, and similar tax laws and rates vary greatly by jurisdiction. Certain jurisdictions in which we do not collect such taxes may seek to impose incremental or new sales, use, value added, digital services, or assert other tax collection obligations on us that such taxes are applicable, which could result in tax assessments, penalties and interest, to us or our customers for the past amounts, and we may be required to collect such taxes in the future. If we are unsuccessful in collecting such taxes from our customers, we could be held liable for such costs, which may adversely affect our results of operations.

Further, an increasing number of U.S. states have considered or adopted laws that attempt to impose tax collection obligations on out-of-state companies. A successful assertion by one or more U.S. states requiring us to collect taxes where we presently do not do so, or to collect more taxes in a jurisdiction in which we currently do collect some taxes, could result in substantial liabilities, including taxes on past sales, as well as interest and penalties. Furthermore, certain jurisdictions, such as the U.K. and France, have recently introduced a digital services tax, which is generally a tax on gross revenue generated from users or customers located in in those jurisdictions, and other jurisdictions have enacted or are considering enacting similar laws. A successful assertion by a U.S. state or local government, or other country or jurisdiction that we should have been or should be collecting additional sales, use, value added, digital services or other similar taxes could, among other things, result in substantial tax payments, create significant administrative burdens for us, discourage potential customers from subscribing to our platform due to the incremental cost of any such sales or other related taxes, or otherwise harm our business.

Our corporate structure and intercompany arrangements are subject to the tax laws of various jurisdictions, and we could be obligated to pay additional taxes, which would harm our operating results and financial condition.

We are expanding our international operations and staff to support our business and growth in international markets. We generally conduct our international operations through wholly-owned subsidiaries and are or may be required to report our taxable income in various jurisdictions worldwide based upon our business operations in those jurisdictions. Our corporate structure and associated transfer pricing policies contemplate future growth in international markets, and consider the functions, risks, and assets of the various entities involved in intercompany transactions. The amount of taxes we pay in different jurisdictions will depend on the application of the tax laws of the various jurisdictions, including the United States, to our intercompany transactions, international business activities, and our ability to operate our business in a manner consistent with our corporate structure and intercompany arrangements. Furthermore, increases in tax rates, new or revised tax laws, and new interpretations of existing tax laws and policies by taxing authorities and courts in various jurisdictions, could result in an increase in our overall tax obligations which could adversely affect our business. Our intercompany relationships and intercompany transactions are subject to complex transfer pricing rules administered by taxing authorities in various jurisdictions in which we operate with potentially divergent tax laws. The amount of taxes we pay in different jurisdictions will depend on the application of the tax laws of the various jurisdictions, including the United States, to our intercompany transactions, international business activities, changes in tax rates, new or revised tax laws or interpretations of existing tax laws and policies by taxing authorities and courts in various jurisdictions, and our ability to operate our business in a manner consistent with our corporate structure and intercompany arrangements.

It is not uncommon for tax authorities in different countries to have conflicting views, for instance, with respect to, among other things, the manner in which the arm’s length standard is applied for transfer pricing purposes, the transfer pricing and charges for intercompany services and other intercompany transactions, or with respect to the valuation of our intellectual property and the manner in which our intellectual property is utilized within our group. In 2022, we began negotiating a bilateral Advance Pricing Agreement (APA) with the United States and the Israeli governments, covering various transfer pricing matters for intercompany transactions relating to the intergroup utilization of our intellectual property among our group enterprises. An APA, if obtained, will provide us with a more predictable future business operating model, and preclude the relevant tax authorities from making certain transfer pricing adjustments within the scope of these agreements. These transfer pricing matters may be significant to our consolidated financial statements. If taxing authorities in any of the jurisdictions in which we conduct our

international operations were to successfully challenge our transfer pricing, we could be required to reallocate part or all of our income to reflect transfer pricing adjustments, which could result in an increased tax liability to us. In such circumstances, if the country from where the income was reallocated did not agree to the reallocation, we could become subject to tax on the same income in both countries, resulting in double taxation. Furthermore, the relevant taxing authorities may disagree with our determinations as to the income and expenses attributable to specific jurisdictions. We believe that our tax and financial accounting positions are reasonable and our tax reserves are adequate to cover any potential liability. We also believe that our assumptions, judgements, and estimates are reasonable and that our transfer pricing for these intercompany transactions are on arm's-length terms. However, the relevant tax authorities may disagree with our tax positions, including any assumptions, judgements or estimates used for these transfer pricing matters and intercompany transactions. If any of these tax authorities determine that our transfer pricing for these intercompany transactions do not meet arm's-length criteria, and were successful in challenging our positions, we could be required to pay additional taxes, interest and penalties related thereto, which could be in excess of any reserves established therefor, and which could result in higher effective tax rates, reduced cash flows and lower overall profitability of our operations. Our financial statements could fail to reflect adequate reserves to cover such a contingency.

We may be audited in various jurisdictions, including in jurisdictions in which we are not currently filing, and such jurisdictions may assess new or additional taxes, sales taxes and value added taxes against us. Although we believe our tax estimates are reasonable, the final determination of any tax audits or litigation could be materially different from our historical tax provisions and accruals, which could have an adverse effect on our operating results or cash flows in the period or periods for which a determination is made.

If our estimates or judgments relating to our critical accounting policies prove to be incorrect or financial reporting standards or interpretations change, our operating results could be adversely affected.

The preparation of financial statements in conformity with GAAP requires management to make estimates and assumptions that affect the amounts reported in our consolidated financial statements and accompanying notes. We base our estimates on historical experience and on various other assumptions that we believe to be reasonable under the circumstances, as discussed in the section titled "Management's Discussion and Analysis of Financial Condition and Results of Operations." The results of these estimates form the basis for making judgments about the carrying values of assets, liabilities and equity, and the amount of revenue and expenses that are not readily apparent from other sources. Significant assumptions and estimates used in preparing our consolidated financial statements include but are not limited to those related to stock-based compensation, the period of benefit for deferred contract acquisition costs, standalone selling prices for each performance obligation, useful lives of long-lived assets, the incremental borrowing rate used for operating lease liabilities, and accounting for income taxes. Our operating results may be adversely affected if our assumptions change or if actual circumstances differ from those in our assumptions, which could cause our operating results to fall below the expectations of industry or financial analysts and investors, resulting in a potential decline in the market price of our Class A common stock.

Additionally, we regularly monitor our compliance with applicable financial reporting standards and review new pronouncements and drafts thereof that are relevant to us. As a result of new standards, changes to existing standards and changes in their interpretation, we might be required to change our accounting policies, alter our operational policies and implement new or enhance existing systems so that they reflect new or amended financial reporting standards, or we may be required to restate our published financial statements. For example, SEC proposals on climate-related disclosures may require us to update our accounting or operational policies, processes, or systems to reflect new or amended financial reporting standards. Such changes to existing standards or changes in their interpretation may have an adverse effect on our reputation, business, financial condition and profit, or cause an adverse deviation from our revenue and operating profit target, which may adversely affect our financial results.

We are exposed to fluctuations in currency exchange rates, which could negatively affect our business, operating results, and financial condition.

Our sales contracts are denominated in U.S. dollars, and therefore our revenue is not subject to foreign currency risk. However, strengthening of the U.S. dollar increases the real cost of our platform to our customers outside of the United States, which could lead to delays in the purchase of our platform and the lengthening of our sales cycle. If the U.S. dollar continues to strengthen, this could adversely affect our operating results and financial condition. In

addition, increased international sales in the future, including through continued international expansion, our channel partners and other partnerships, could result in foreign currency denominated sales, which would increase our foreign currency risk.

Our operating expenses incurred outside the U.S. and denominated in foreign currencies are increasing and are subject to fluctuations due to changes in foreign currency exchange rates. These expenses are denominated in foreign currencies and are subject to fluctuations due to changes in foreign currency exchange rates. We do not currently hedge against the risks associated with currency fluctuations but may do so, or use other derivative instruments, in the future.

We may require additional capital to fund our business and support our growth, and any inability to generate or obtain such capital may adversely affect our operating results and financial condition.

In order to support our growth and respond to business challenges, such as developing new features or enhancements to our platform to stay competitive, acquiring new technologies, and improving our infrastructure, we have made significant financial investments in our business and we intend to continue to make such investments. As a result, we may need to engage in additional equity or debt financings to provide the funds required for these investments and other business endeavors. If we raise additional funds through equity or convertible debt issuances, our existing stockholders may suffer significant dilution and these securities could have rights, preferences, and privileges that are superior to those of holders of our Class A common stock. We expect that our existing cash and cash equivalents will be sufficient to meet our anticipated cash needs for working capital and capital expenditures for at least the next 12 months. If we obtain additional funds through debt financing, we may not be able to obtain such financing on terms favorable to us. Such terms may involve restrictive covenants making it difficult to engage in capital raising activities and pursue business opportunities, including potential acquisitions. The trading prices of technology companies have been highly volatile as a result of the continuing effects of the COVID-19 pandemic, the conflict in Ukraine, inflation, rising interest rates, instability in the banking system, and market downturns, which may reduce our ability to access capital on favorable terms or at all. In addition, a recession, depression, or other sustained adverse market event could adversely affect our business and the value of our Class A common stock. If we are unable to obtain adequate financing or financing on terms satisfactory to us when we require it, our ability to continue to support our business growth and to respond to business challenges could be significantly impaired and our business may be adversely affected, requiring us to delay, reduce, or eliminate some or all of our operations.

Risks Related to Ownership of Our Class A Common Stock

The market price of our Class A common stock may be volatile, and you could lose all or part of your investment.

Our Class A common stock price is likely to continue to be volatile and could be subject to wide fluctuations. The market price of our Class A common stock depends on a number of factors, including those described in this “Risk Factors” section, many of which are beyond our control and may not be related to our operating performance. These fluctuations could cause you to lose all or part of your investment in our Class A common stock. Factors that could cause fluctuations in the market price of our Class A common stock include the following:

- actual or anticipated changes or fluctuations in our operating results;
- the financial projections we may provide to the public, any changes in these projections or our failure to meet these projections;
- announcements by us or our competitors of new products or new or terminated significant contracts, commercial relationships, acquisitions or capital commitments;
- rumors and market speculation involving us or other companies in our industry;
- the overall performance of the stock market or technology companies;
- the number of shares of our Class A common stock publicly owned and available for trading;

- failure of industry or financial analysts to maintain coverage of us, changes in financial estimates by any analysts who follow our company, or our failure to meet these estimates or the expectations of investors;
- litigation or other proceedings involving us, our industry or both, or investigations by regulators into our operations or those of our competitors;
- developments or disputes concerning our intellectual property rights or our solutions, or third-party proprietary rights;
- new laws or regulations or new interpretations of existing laws or regulations applicable to our business;
- any major changes in our management or our board of directors;
- interest rate changes or fluctuations; and
- other events or factors, including those resulting from the COVID-19 pandemic, war, such as Russia's invasion of Ukraine, armed conflict, incidents of terrorism or responses to these events.

In addition, the stock market in general, and the market for technology companies in particular, has experienced extreme price and volume fluctuations that have often been unrelated or disproportionate to the operating performance of those companies, particularly during the current period of macroeconomic uncertainty, including rising inflation, increasing interest rates, labor shortages and fluctuations in international currency rates, as well as the impacts of the current conflict in Ukraine and the COVID-19 pandemic. These economic, political, regulatory and market conditions have and may continue to negatively impact the market price of our Class A common stock, regardless of our actual operating performance. In addition, in the past, following periods of volatility in the overall market and the market prices of a particular company's securities, securities class action litigation has often been instituted against that company. Securities litigation, if instituted against us, could result in substantial costs and divert our management's attention and resources from our business. This could have an adverse effect on our business, operating results, and financial condition.

Sales of substantial amounts of our Class A common stock in the public markets, or the perception that they might occur, could cause the market price of our Class A common stock to decline.

Sales of a substantial number of shares of our Class A common stock into the public market, including shares of Class A common stock held by our existing stockholders that have been converted from shares of Class B common stock, and particularly sales by our directors, executive officers, and principal stockholders, or the perception that these sales might occur, could cause the market price of our Class A common stock to decline.

In addition, pursuant to our amended and restated investors' rights agreement, dated October 28, 2020, certain stockholders have the right, subject to certain conditions, to require us to file a registration statement for the public resale of such capital stock or to include such shares in registration statements that we may file for us or other stockholders. Any registration statement we file to register additional shares, whether as a result of registration rights or otherwise, could cause the market price of our Class A common stock to decline or be volatile.

We may also issue our shares of our capital stock or securities convertible into shares of our capital stock from time to time in connection with a financing, an acquisition, an investment, or otherwise. Any such issuance could result in substantial dilution to our existing stockholders and cause the market price of our Class A common stock to decline.

The dual class structure of our common stock has the effect of concentrating voting control with the holders of our Class B common stock who held, in the aggregate, approximately 85% of the voting power of our capital stock as of January 31, 2023, which will limit or preclude your ability to influence corporate matters, including the election of directors and the approval of any change of control transaction.

Our Class B common stock has 20 votes per share, and our Class A common stock has one vote per share. As of January 31, 2023, the holders of our outstanding Class B common stock held approximately 85% of the voting power of our outstanding capital stock. Because of the twenty-to-one voting ratio between our Class B and Class A

common stock, the holders of our Class B common stock collectively are expected to continue to control a majority of the combined voting power of our common stock and therefore will be able to control all matters submitted to our stockholders for approval until the earlier of (i) the date specified by a vote of the holders of 66 2/3% of the then outstanding shares of Class B common stock, (ii) seven years from the date of our Final Prospectus, or June 29, 2028, (iii) the first date following the completion of our IPO on which the number of shares of outstanding Class B common stock (including shares of Class B common stock subject to outstanding stock options) held by Tomer Weingarten, including certain permitted entities that Mr. Weingarten controls, is less than 25% of the number of shares of outstanding Class B common stock (including shares of Class B common stock subject to outstanding stock options) that Mr. Weingarten originally held as of the date of our Final Prospectus, (iv) the date fixed by our board of directors, following the first date following the completion of our IPO when Mr. Weingarten is no longer providing services to us as an officer, employee, consultant or member of our board of directors, (v) the date fixed by our board of directors following the date on which, if applicable, Mr. Weingarten is terminated for cause, as defined in our restated certificate of incorporation, and (vi) the date that is 12 months after the death or disability, as defined in our restated certificate of incorporation, of Mr. Weingarten. This concentrated control will limit or preclude your ability to influence corporate matters for the foreseeable future, including the election of directors, amendments of our organizational documents, and any merger, consolidation, sale of all or substantially all of our assets, or other major corporate transaction requiring stockholder approval. In addition, this may prevent or discourage unsolicited acquisition proposals or offers for our capital stock that you may feel are in your best interest as one of our stockholders.

Future transfers by holders of our Class B common stock will generally result in those shares converting to Class A common stock, subject to limited exceptions, such as certain transfers effected for estate planning purposes. The conversion of Class B common stock to Class A common stock will have the effect, over time, of increasing the relative voting power of those holders of our Class B common stock who retain their shares in the long term.

The dual class structure of our common stock may adversely affect the trading market for our Class A common stock.

We cannot predict whether our dual class structure will, over time, result in a lower or more volatile market price of our Class A common stock, adverse publicity, or other adverse consequences. Certain stock index providers, such as S&P Dow Jones, exclude companies with multi-class share structures from being added to certain of its indices, including the S&P 500. In addition, several stockholder advisory firms and large institutional investors oppose the use of multiple class structures. As a result, the dual class structure of our common stock may make us ineligible for inclusion in certain indices and may discourage such indices from selecting us for inclusion, notwithstanding our automatic termination provision, may cause stockholder advisory firms to publish negative commentary about our corporate governance practices or otherwise seek to cause us to change our capital structure, and may result in large institutional investors not purchasing shares of our Class A common stock. Any exclusion from certain stock indices could result in less demand for our Class A common stock. Any actions or publications by stockholder advisory firms or institutional investors critical of our corporate governance practices or capital structure could also adversely affect the value of our Class A common stock.

General Risk Factors

Adverse economic conditions or reduced information technology spending could adversely affect our business, operating results, and financial condition.

Our business depends on the overall demand for information technology and on the economic health of our current and prospective customers. In addition, the purchase of our platform is often discretionary and may involve a significant commitment of capital and other resources. Weak global and regional economic conditions, including U.S. and global macro-economic issues, including global banking and finance related issues, labor shortages, supply chain disruptions, rising interest rates and inflation, spending environments, geopolitical instability, warfare and uncertainty, weak economic conditions in certain regions or a reduction in information technology spending regardless of macro-economic conditions, including the effects of the COVID-19 pandemic and the war in Ukraine, and proposed judicial reform in Israel, could adversely affect our business, operating results, and financial condition, including resulting in longer sales cycles, a negative impact on our ability to attract and retain new customers or

expand our platform or sell additional products and services to our existing customers, lower prices for our platform, higher default rates among our channel partners, reduced sales to new or existing customers and slower or declining growth. For example, as a result of current uncertainty in macroeconomic conditions, we have recently observed a lengthening of the sales cycle for some prospective customers that we attribute to higher cost-consciousness around IT budgets. We expect the macroeconomic conditions impacting demand to persist in the near-term. Deterioration in economic conditions in any of the countries in which we do business could also cause slower or impaired collections on accounts receivable, which may adversely impact our liquidity and financial condition.

Moreover, the U.S. capital markets have experienced and continue to experience extreme volatility and disruption. Inflation rates in the U.S. significantly increased in 2022 resulting in federal action to increase interest rates, adversely affecting capital markets activity. Further deterioration of the macroeconomic environment and regulatory action may adversely affect our business, operating results, and financial condition. Moreover, there has been recent turmoil in the global banking system. For example, on March 10, 2023, Silicon Valley Bank (SVB), one of our banking partners, was closed by the California Department of Financial Protection and Innovation, which appointed the Federal Deposit Insurance Corporation (FDIC), as receiver. While we only had a minimal amount of our cash directly at SVB and, since that date, the FDIC has stated that all depositors of SVB will be made whole, there is no guarantee that the federal government would guarantee all depositors as they did with SVB depositors in the event of further bank closures and continued instability in the global banking system may negatively impact us or our customers, including our customers' ability to pay for our platform, and adversely impact our business and financial condition. Moreover, events such as the closure of SVB, in addition to global macroeconomic conditions discussed above, may cause further turbulence and uncertainty in the capital markets.

We may be adversely affected by natural disasters, pandemics and other catastrophic events, and by man-made problems such as war, that could disrupt our business operations, and our business continuity and disaster recovery plans may not adequately protect us from a serious disaster.

Natural disasters or other catastrophic events may cause damage or disruption to our operations, international commerce, and the global economy, and thus could have an adverse effect on us. Our business operations are also subject to interruption by fire, power shortages, flooding, and other events beyond our control. In addition, our global operations expose us to risks associated with public health crises, such as pandemics and epidemics, which could harm our business and cause our operating results to suffer. For example, the ongoing effects of the COVID-19 pandemic and the measures that we, our customers and governmental authorities have adopted, as described in detail elsewhere in these risk factors, have and could continue to have an adverse effect on our business and operating results. In addition, our growth rate may actually slow or decline as the impact of the COVID-19 pandemic tapers as people continue to return to offices and other workplaces. Further, acts of war, armed conflict, terrorism and other geopolitical unrest, such as Russia's invasion of Ukraine, could cause disruptions in our business or the businesses of our partners or the economy as a whole. In the event of a natural disaster, including a major earthquake, blizzard, or hurricane, or a catastrophic event such as a fire, power loss, cyberattack, or telecommunications failure, we may be unable to continue our operations and may endure system interruptions, reputational harm, delays in development of our platform, lengthy interruptions in service, breaches of data security, and loss of critical data, all of which could have an adverse effect on our future operating results. Climate change could result in an increase in the frequency or severity of such natural disasters. For example, our corporate offices are located in California, a state that frequently experiences earthquakes, wildfires, heatwaves and droughts. Additionally, all the aforementioned risks will be further increased if we do not implement an effective disaster recovery plan or our partners' disaster recovery plans prove to be inadequate.

The COVID-19 pandemic could adversely affect our business, operating results, and financial condition.

The COVID-19 pandemic continues to impact worldwide economic activity and financial markets. We have experienced, and may continue to experience negative impacts on certain parts of our business. The full extent to which the COVID-19 pandemic will directly or indirectly impact our business, operating results, cash flows, and financial condition will depend on future developments that are uncertain and cannot be accurately predicted.

Measures we have taken to mitigate the spread of the virus could negatively affect our customer success efforts, delay and lengthen our sales cycle for some prospective customers and delay the delivery of professional services and trainings to our customers, impact our marketing, sales and support efforts, reduce employee efficiency and

productivity, increase employee attrition, and create operational or other challenges, any of which could harm our business and results of operations.

We do not yet know the full extent of potential impacts on our business, operations or on the global economy as a whole, particularly if the COVID-19 pandemic persists for an extended period of time. Potential impacts include but are not limited to:

- our customer prospects and our existing customers may experience slowdowns in their businesses, which in turn may result in reduced demand for our platform, lengthening of sales cycles, loss of customers, and difficulties in collections;
- we have opened our offices in accordance with local ordinances, however, most of our employees continue to work from home and a substantial number may continue to do so for the foreseeable future, which may present challenges to employee collaboration, productivity and retention;
- we continue to incur fixed costs, particularly for real estate, and are deriving reduced or no benefit from those costs;
- we may continue to experience disruptions to our growth planning, such as for facilities and international expansion;
- we anticipate incurring costs in returning to work from our facilities around the world, including changes to the workplace, such as space planning, food service, and amenities;
- we may be subject to legal liability for safe workplace claims; and
- our critical vendors could go out of business;

Any of the foregoing could adversely affect our business, financial condition, and operating results.

Investors' expectations of our performance relating to environmental, social and governance factors may impose additional costs and expose us to new risks.

There is an increasing focus from certain investors, employees, users and other stakeholders concerning corporate responsibility, specifically related to environmental, social and governance matters (ESG). Some investors may use these non-financial performance factors to guide their investment strategies and, in some cases, may choose not to invest in us if they believe our policies and actions relating to corporate responsibility are inadequate. We may face reputational damage in the event that we do not meet the ESG standards set by various constituencies.

Furthermore, if our competitors' corporate social responsibility performance is perceived to be better than ours, potential or current investors may elect to invest with our competitors instead. In addition, in the event that we communicate certain initiatives and goals regarding environmental, social and governance matters, we could fail, or be perceived to fail, in our achievement of such initiatives or goals, or we could be criticized for the scope of such initiatives or goals. If we fail to satisfy the expectations of investors, employees and other stakeholders or our initiatives are not executed as planned, our reputation and business, operating results and financial condition could be adversely affected.

If industry or financial analysts do not publish research or reports about our business, or if they issue inaccurate or unfavorable research regarding our Class A common stock, our stock price and trading volume could decline.

The trading market for our Class A common stock may be influenced by the research and reports that industry or financial analysts publish about us, our business, our market and our competitors. We do not control these analysts or the content and opinions included in their reports. If any of the analysts who cover us issues an inaccurate or unfavorable opinion regarding our stock price, our stock price would likely decline. If our financial results fail to meet, or significantly exceed, our announced guidance or the expectations of analysts or public investors, analysts could downgrade our Class A common stock or publish unfavorable research about us. If one or more of these analysts cease coverage of our Class A common stock or fail to publish reports on us regularly, our

visibility in the financial markets could decrease, which in turn could cause our stock price or trading volume to decline.

We could be subject to securities class action litigation.

In the past, securities class action litigation has often been instituted against companies following periods of volatility in the market price of a company's securities. This type of litigation, if instituted, could result in substantial costs and a diversion of management's attention and resources, which could adversely affect our business, operating results, or financial condition. Additionally, the dramatic increase in the cost of directors' and officers' liability insurance may make it more expensive for us to obtain directors' and officers' liability insurance in the future and may require us to opt for lower overall policy limits and coverage or to forgo insurance that we may otherwise rely on to cover significant defense costs, settlements, and damages awarded to plaintiffs, or incur substantially higher costs to maintain the same or similar coverage. These factors could make it more difficult for us to attract and retain qualified executive officers and members of our board of directors.

We do not intend to pay dividends in the foreseeable future. As a result, your ability to achieve a return on your investment will depend on appreciation in the price of our Class A common stock.

We have never declared or paid any cash dividends on our capital stock. We currently intend to retain all available funds and any future earnings for use in the operation of our business and do not anticipate paying any dividends in the foreseeable future. Any determination to pay dividends in the future will be at the discretion of our board of directors. Accordingly, investors must rely on sales of their Class A common stock after price appreciation, which may never occur, as the only way to realize any future gains on their investments.

Provisions in our charter documents and under Delaware law could make an acquisition of us, which may be beneficial to our stockholders, more difficult and may limit attempts by our stockholders to replace or remove our current management.

Provisions in our restated certificate of incorporation and amended and restated bylaws may have the effect of delaying or preventing a merger, acquisition or other change of control of the company that the stockholders may consider favorable. In addition, because our board of directors is responsible for appointing the members of our management team, these provisions may frustrate or prevent any attempts by our stockholders to replace or remove our current management by making it more difficult for stockholders to replace members of our board of directors. Among other things, our restated certificate of incorporation and amended and restated bylaws include provisions that:

- provide that our board of directors is classified into three classes of directors with staggered three-year terms;
- permit our board of directors to establish the number of directors and fill any vacancies and newly created directorships;
- require super-majority voting to amend some provisions in our restated certificate of incorporation and amended and restated bylaws;
- authorize the issuance of "blank check" preferred stock that our board of directors could use to implement a stockholder rights plan;
- provide that only our chief executive officer or a majority of our board of directors will be authorized to call a special meeting of stockholders;
- eliminate the ability of our stockholders to call special meetings of stockholders;
- do not provide for cumulative voting;
- provide that directors may only be removed "for cause" and only with the approval of two-thirds of our stockholders;

- provide for a dual class common stock structure in which holders of our Class B common stock may have the ability to control the outcome of matters requiring stockholder approval, even if they own significantly less than a majority of the outstanding shares of our common stock, including the election of directors and other significant corporate transactions, such as a merger or other sale of our company or its assets;
- prohibit stockholder action by written consent, which requires all stockholder actions to be taken at a meeting of our stockholders;
- provide that our board of directors is expressly authorized to make, alter, or repeal our amended and restated bylaws; and
- establish advance notice requirements for nominations for election to our board of directors or for proposing matters that can be acted upon by stockholders at annual stockholder meetings.

Moreover, Section 203 of the Delaware General Corporation Law (DGCL), may discourage, delay, or prevent a change in control of our company. Section 203 imposes certain restrictions on mergers, business combinations, and other transactions between us and holders of 15% or more of our common stock.

Our restated certificate of incorporation contains exclusive forum provisions for certain claims, which may limit our stockholders' ability to obtain a favorable judicial forum for disputes with us or our directors, officers, or employees.

Our restated certificate of incorporation provides that the Court of Chancery of the State of Delaware, to the fullest extent permitted by law, will be the exclusive forum for any derivative action or proceeding brought on our behalf, any action asserting a breach of fiduciary duty, any action asserting a claim against us arising pursuant to the DGCL, our restated certificate of incorporation, or our amended and restated bylaws, or any action asserting a claim against us that is governed by the internal affairs doctrine.

Moreover, Section 22 of the Securities Act creates concurrent jurisdiction for federal and state courts over all claims brought to enforce any duty or liability created by the Securities Act or the rules and regulations thereunder. Our restated certificate of incorporation provides that the federal district courts of the United States will, to the fullest extent permitted by law, be the exclusive forum for resolving any complaint asserting a cause of action arising under the Securities Act, or Federal Forum Provision. Our decision to adopt a Federal Forum Provision followed a decision by the Supreme Court of the State of Delaware holding that such provisions are facially valid under Delaware law. While there can be no assurance that federal or state courts will follow the holding of the Delaware Supreme Court or determine that the Federal Forum Provision should be enforced in a particular case, application of the Federal Forum Provision means that suits brought by our stockholders to enforce any duty or liability created by the Securities Act must be brought in federal court and cannot be brought in state court.

Section 27 of the Exchange Act creates exclusive federal jurisdiction over all claims brought to enforce any duty or liability created by the Exchange Act or the rules and regulations thereunder. In addition, the Federal Forum Provision applies to suits brought to enforce any duty or liability created by the Exchange Act. Accordingly, actions by our stockholders to enforce any duty or liability created by the Exchange Act or the rules and regulations thereunder must be brought in federal court.

Our stockholders will not be deemed to have waived our compliance with the federal securities laws and the regulations promulgated thereunder.

Any person or entity purchasing or otherwise acquiring or holding any interest in any of our securities shall be deemed to have notice of and consented to our exclusive forum provisions, including the Federal Forum Provision. These provisions may limit a stockholders' ability to bring a claim in a judicial forum of their choosing for disputes with us or our directors, officers, or employees, which may discourage lawsuits against us and our directors, officers, and employees. Alternatively, if a court were to find the choice of forum provision contained in our restated certificate of incorporation or amended and restated bylaws to be inapplicable or unenforceable in an action, we may incur additional costs associated with resolving such action in other jurisdictions, which could harm our business, financial condition, and operating results.

ITEM 1B. UNRESOLVED STAFF COMMENTS

None.

ITEM 2. PROPERTIES

We are headquartered in Mountain View, California, where we occupy over 10,000 square feet of office space pursuant to a lease that expires in February 2028 subject to the terms thereof. Our headquarters was built to reflect our corporate culture, operational needs, and dedication to employee happiness. We lease additional offices in the United States and around the world, including in the Czech Republic, France, Israel, and United Arab Emirates. We believe that our current facilities are adequate to meet our current needs.

ITEM 3. LEGAL PROCEEDINGS

We are currently a party to, and may from time to time in the future, be involved in, various litigation matters and subject to claims that arise in the ordinary course of business, including claims asserted by third parties in the form of letters and other communications. For more information regarding legal proceedings and other claims in which we are involved, see Note 13 to our consolidated financial statements included in Part II, Item 8 of this Annual Report on Form 10-K, and is incorporated herein by reference.

ITEM 4. MINE SAFETY DISCLOSURES

Not applicable.

PART II.

ITEM 5. MARKET FOR REGISTRANT'S COMMON EQUITY, RELATED STOCKHOLDER MATTER AND ISSUER PURCHASES OF EQUITY SECURITIES

Market Information for Class A Common Stock

Our Class A common stock has been traded on the NYSE under the symbol "S" since June 30, 2021. Prior to that date, there was no public trading market for our common stock. Our Class B common stock is not listed or traded on any stock exchange.

Holders of Record

As of March 24, 2023, we had 70 holders of record of our Class A common stock and 69 holders of record of our Class B common stock. Because many of our shares of common stock are held in street name by brokers, institutions, and other nominees on behalf of stockholders, we are unable to estimate the total number of beneficial owners of our common stock represented by these holders of record.

Dividend Policy

We currently intend to retain all available funds and any future earnings for use in the operation and growth of our business and do not anticipate paying any dividends on our capital stock in the foreseeable future. Any future determination to declare dividends will be made at the discretion of our board of directors, subject to applicable laws, and will depend on our financial condition, results of operations, capital requirements, general business conditions, and other factors that our board of directors may deem relevant.

Securities Authorized for Issuance Under Equity Compensation Plans

The information required by this item will be included in our Proxy Statement for the 2023 Annual Meeting to be filed with the SEC within 120 days of the fiscal year ended January 31, 2023, and is incorporated herein by reference.

Unregistered Sales of Equity Securities

None.

Issuer Purchases of Equity Securities

None.

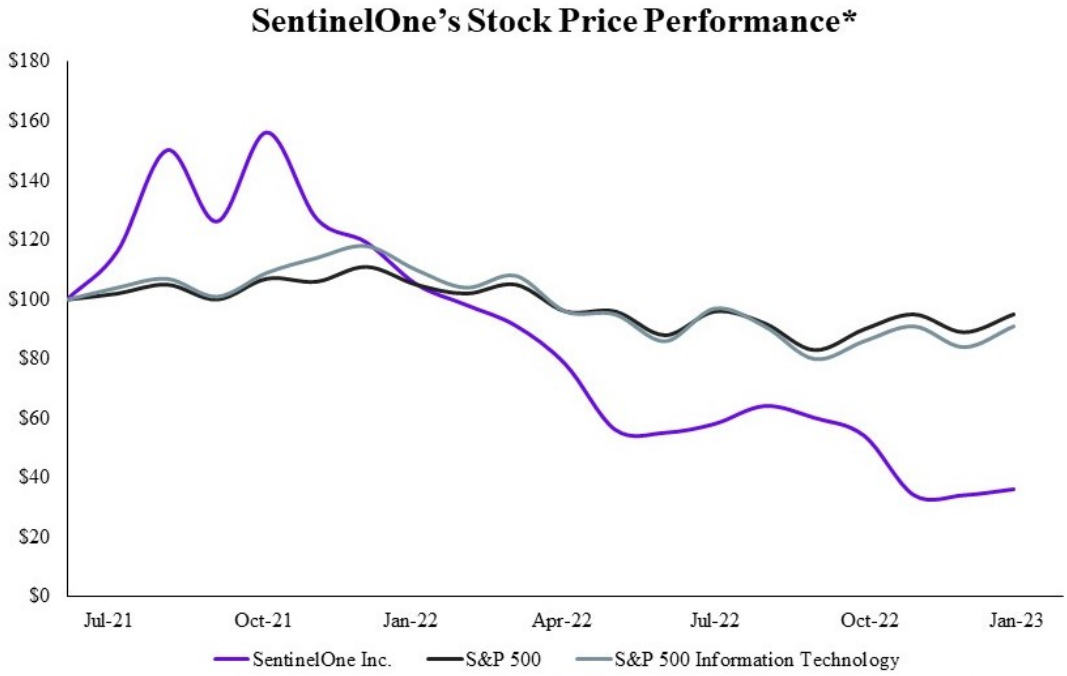
Use of Proceeds from Initial Public Offering of Common Stock and Concurrent Private Placement

None.

Stock Performance Graph

This performance graph shall not be deemed "soliciting material" or be "filed" with the SEC for purposes of Section 18 of the Exchange Act, or otherwise subject to the liability under that Section, and shall not be deemed to be incorporated by reference into any filing of SentinelOne, Inc. under the Securities Act or Exchange Act generally.

We have presented below the cumulative total return to our stockholders between June 30, 2021 (the date our Class A common stock commenced trading on the NYSE) through January 31, 2023 in comparison to the Standard & Poor's 500 Index and Standard & Poor Information Technology Index. All values assume a $100 initial investment and data for the Standard & Poor's 500 Index and Standard & Poor Information Technology Index assume reinvestment of dividends. Such returns are based on historical data and are not indicative of, nor intended to forecast, the future performance of our Class A common stock.



ITEM 6. [RESERVED]

ITEM 7. MANAGEMENT'S DISCUSSION AND ANALYSIS OF FINANCIAL CONDITION AND RESULTS OF OPERATIONS

The following discussion and analysis of our financial condition and results of operations should be read in conjunction with our consolidated financial statements and related notes appearing elsewhere in this Annual Report on Form 10-K. Some of the information contained in this discussion and analysis or set forth elsewhere in this Annual Report on Form 10-K, particularly information with respect to our future results of operations or financial condition, business strategy and plans, and objectives of management for future operations, includes forward-looking statements that involve risks and uncertainties as described under the heading "Special Note About Forward-Looking Statements" in this Annual Report on Form 10-K. You should review the disclosure under the heading "Risk Factors" in this Annual Report on Form 10-K for a discussion of important factors that could cause our actual results to differ materially from those anticipated in these forward-looking statements. Our fiscal year ends on January 31, and our fiscal quarters end on April 30, July 31, October 31, and January 31. Our fiscal years ended January 31, 2023, 2022, and 2021 are referred to herein as fiscal 2023, fiscal 2022, and fiscal 2021, respectively.

Unless the context otherwise requires, all references in this report to "SentinelOne," the "Company," "we" "our" "us," or similar terms refer to SentinelOne, Inc. and its subsidiaries.

A discussion regarding our financial condition and results of operations for fiscal 2023 compared to fiscal 2022 is presented below. A discussion regarding our financial condition and results of operations for fiscal 2022 compared to fiscal 2021 can be found in "Management's Discussion and Analysis of Financial Condition and Results of Operations" in the Form 10-K for the fiscal year ended January 31, 2022 filed with the SEC on April 7, 2022.

Overview

We founded SentinelOne in 2013 with a dramatically new approach to cybersecurity.

We pioneered the world's first purpose-built AI-powered Singularity Platform to make cybersecurity defense truly autonomous, from the endpoint and beyond. Our Singularity Platform instantly defends against cyberattacks - performing at a faster speed, greater scale, and higher accuracy than otherwise possible from a human-powered approach.

Our Singularity Platform ingests, correlates, and queries petabytes of structured and unstructured data from a myriad of ever-expanding disparate external and internal sources in real-time. We build rich context and deliver greater visibility by constructing a dynamic representation of data across an organization. As a result, our AI models are highly accurate, actionable, and autonomous. Our distributed AI models run both locally on every endpoint and every cloud workload, as well as on our cloud platform. Our Static and vector-agnostic Behavioral AI models, which run on the endpoints themselves, provide our customers with protection even when their devices are not connected to the cloud. In the cloud, our Streaming AI detects anomalies that surface when multiple data feeds are correlated. By providing full visibility into the Storyline of every secured device across the organization through one console, our platform makes it very fast for analysts to easily search through petabytes of data to investigate incidents and proactively hunt threats. We have extended our control and visibility planes beyond the traditional endpoint to unmanaged IoT devices.

Our Singularity Platform can be flexibly deployed on the environments that our customers choose, including public, private, or hybrid clouds. Our feature parity across Windows, macOS, Linux, and Kubernetes offers best-of-breed protection, visibility, and control across today's heterogeneous IT environments. Together, these capabilities make our platform the logical choice for organizations of all sizes, industry verticals, and compliance requirements. Our platform offers true multi-tenancy, which enables some of the world's largest organizations and our managed security providers and incident response partners with an excellent management experience. Our customers realize improved cybersecurity outcomes with fewer people.

We generate substantially all of our revenue by selling subscriptions to our Singularity Platform. Our subscription tiers include Singularity Core, Singularity Control, and Singularity Complete. Additionally, customers can extend the functionality of our platform through our subscription Singularity Modules. We generally price our subscriptions and modules on a per agent basis, and each agent generally corresponds with an endpoint, server, virtual machine, or container.

Our subscription contracts typically range from one to three years. We recognize subscription revenue ratably over the term of a contract. Most of our contracts are for terms representing annual increments, therefore contracts generally come up for renewal in the same period in subsequent years. The timing of large multi-year enterprise contracts can create some variability in subscription order levels between periods, though the impact to our revenue in any particular period is limited as a result of ratable revenue recognition.

Our go-to-market strategy is focused on acquiring new customers and driving expanded usage of our platform by existing customers. Our sales organization is comprised of our enterprise sales, inside sales and customer solutions engineering teams. It leverages our global network of ISVs, alliance partners, and channel partners for prospect access. Additionally, our sales teams work closely with our customers, channel partners, and alliance partners to drive adoption of our platform, and our software solutions are fulfilled through our channel partners. Our channel partners include some of the world's largest resellers and distributors, MSPs, MSSPs, MDRs, OEMs, and IR firms. Once customers experience the benefits of our platform, they often upgrade their subscriptions to benefit from the full range of our XDR and IT and security operations capabilities. Additionally, many of our customers adopt Singularity Modules over time to extend the functionality of our platform and increase their coverage footprint. The combination of platform upgrades and extended modules drives our powerful land-and-expand motion.

Our Singularity Platform is used globally by organizations of all sizes across a broad range of industries. As of January 31, 2023, we had over 10,000 customers, increasing from over 6,700 customers as of January 31, 2022. We had 905 customers with ARR of $100,000 or more as of January 31, 2023, up from 520 customer with ARR of $100,000 or more as of January 31, 2022. As of January 31, 2023 and 2022, no single end customer accounted for

more than 4% of our ARR. We define ARR as the annualized revenue run rate of our subscription and capacity contracts at the end of a reporting period, assuming contracts are renewed on their existing terms for customers that are under contracts with us. Our revenue outside of the United States represented 35% and 32% for fiscal 2023 and 2022, respectively, illustrating the global nature of our solutions.

We have grown rapidly since our inception. Our revenue was $422.2 million, $204.8 million, and $93.1 million for fiscal 2023, 2022, and 2021, respectively, representing year-over-year growth of 106% and 120%, respectively. During this period, we continued to invest in growing our business to capitalize on our market opportunity. As a result, our net loss for fiscal 2023, 2022, and 2021 was $378.7 million, $271.1 million, and $117.6 million, respectively.

Key Business Metrics

We monitor the following key metrics to help us evaluate our business, identify trends affecting our business, formulate business plans, and make strategic decisions.

Annualized Recurring Revenue (ARR)

We believe that ARR is a key operating metric to measure our business because it is driven by our ability to acquire new subscription and capacity customers and to maintain and expand our relationship with existing customers. ARR represents the annualized revenue run rate of our subscription and capacity contracts at the end of a reporting period, assuming contracts are renewed on their existing terms for customers that are under contracts with us. ARR is not a forecast of future revenue, which can be impacted by contract start and end dates and renewal rates.

	As of January 31,		
	2023	2022	2021
		(in thousands)	
Annualized recurring revenue	$ 548,652	$ 292,341	$ 130,825

ARR grew 88% year-over-year to $548.7 million for fiscal 2023, primarily due to high growth in the number of new customers purchasing our subscriptions and to additional purchases by existing customers. ARR is an operational metric, and there is no comparable GAAP financial measure to which we can reconcile this particular key metric.

Customers with ARR of $100,000 or More

We believe that our ability to increase the number of customers with ARR of $100,000 or more is an indicator of our market penetration and strategic demand for our platform. We define a customer as an entity that has an active subscription for access to our platform. We count MSPs, MSSPs, MDRs, and OEMs, who may purchase our products on behalf of multiple companies, as a single customer. We do not count our reseller or distributor channel partners as customers.

	As of January 31,		
	2023	2022	2021
	(in thousands)		
Customers with ARR of $100,000 or more	905	520	219

Customers with ARR of $100,000 or more grew 74% year-over-year to 905 for fiscal 2023, primarily due to growth in the ARR of existing customers from additional purchases and to growth in the average size of purchases by new customers.

Dollar-Based Net Retention Rate (NRR)

We believe that our ability to retain and expand our revenue generated from our existing customers is an indicator of the long-term value of our customer relationships and our potential future business opportunities. NRR measures the percentage change in our ARR derived from our customer base at a point in time.

	As of January 31,		
	2023	2022	2021
Dollar-based net retention rate	132 %	129 %	117 %

Our dollar-based net retention rate was 132% as of January 31, 2023, driven by existing customers primarily from expansion of the number of endpoints and purchases of additional modules. NRR is an operational metric, and there is no comparable GAAP financial measure to which we can reconcile this particular key metric.

Components of Our Results of Operations

Revenue

We generate substantially all of our revenue from subscriptions to our Singularity Platform. Customers can extend the functionality of their subscription to our platform by subscribing to additional Singularity Modules. Subscriptions provide access to hosted software. The nature of our promise to the customer under the subscription is to provide protection for the duration of the contractual term and as such is considered as a series of distinct services. Our arrangements may include fixed consideration, variable consideration, or a combination of the two. Fixed consideration is recognized over the term of the arrangement or longer if the fixed consideration relates to a material right. Variable consideration in these arrangements is typically a function of transaction volume or another usage-based measure. Depending upon the structure of a particular arrangement, we (1) allocate the variable amount to each distinct service period within the series and recognize revenue as each distinct service period is performed (i.e. direct allocation), (2) estimate total variable consideration at contract inception (giving consideration to any constraints that may apply and updating the estimates as new information becomes available) and recognizes the total transaction price over the period to which it relates, or (3) apply the ‘right to invoice’ practical expedient and recognize revenue based on the amount invoiced to the customer during the period. Premium support and maintenance and other Singularity Modules are distinct from subscriptions and are recognized ratably over the term as the performance obligations are satisfied.

We invoice our customers upfront upon signing for the entire term of the contract, periodically, or in arrears. Most of our subscription contracts have a term of one to three years.

Cost of Revenue

Cost of revenue consists primarily of third-party cloud infrastructure expenses incurred in connection with the hosting and maintenance of our platform. Cost of revenue also consists of personnel-related costs associated with our customer support and services organization, including salaries, benefits, bonuses, and stock-based compensation, amortization of acquired intangible assets, amortization of capitalized internal-use software, software and subscription services used by our customer support and services team, and allocated overhead costs.

Our third-party cloud infrastructure costs are driven primarily by the number of customers, the number of endpoints per customer, the number of modules, and the incremental costs for storing additional data collected for such cloud modules. We plan to continue to invest in our platform infrastructure and additional resources in our customer support and services organization as we grow our business. The level and timing of investment in these areas could affect our cost of revenue from period to period.

Operating Expenses

Our operating expenses consist of research and development, sales and marketing, and general and administrative expenses. Personnel-related expenses are the most significant component of operating expenses and consist of salaries, benefits, bonuses, stock-based compensation, and sales commissions. Operating expenses also include allocated facilities and IT overhead costs.

Research and Development

Research and development expenses consist primarily of employee salaries, benefits, bonuses, and stock-based compensation. Research and development expenses also include consulting fees, software and subscription services, and third-party cloud infrastructure expenses incurred in developing our platform and modules.

We expect research and development expenses to increase in absolute dollars as we continue to increase investments in our existing products and services. However, we anticipate research and development expenses to decrease as a percentage of our total revenue over time, although our research and development expenses may fluctuate as a percentage of our total revenue from period to period depending on the timing of these expenses. In addition, research and development expenses that qualify as internal-use software are capitalized, the amount of which may fluctuate significantly from period to period.

Sales and Marketing

Sales and marketing expenses consist primarily of employee salaries, commissions, benefits, bonuses, stock-based compensation, travel and entertainment related expenses, advertising, branding and marketing events, promotions, and software and subscription services. Sales and marketing expenses also include sales commissions paid to our sales force and referral fees paid to independent third parties that are incremental to obtain a subscription contract. Such costs are capitalized and amortized over an estimated period of benefit of four years, and any such expenses paid for the renewal of a subscription are capitalized and amortized over the average contractual term of the renewal.

We expect sales and marketing expenses to increase in absolute dollars as we continue to make significant investments in our sales and marketing organization to drive additional revenue, further penetrate the market, and expand our global customer base, but to decrease as a percentage of our revenue over time.

General and Administrative

General and administrative expenses consist primarily of salaries, benefits, bonuses, stock-based compensation, and other expenses for our executive, finance, legal, people team, and facilities organizations. General and administrative expenses also include external legal, accounting, other consulting, and professional services fees, software and subscription services, and other corporate expenses.

We expect to continue to incur additional expenses as a result of operating as a public company, including costs to comply with the rules and regulations applicable to companies listed on a national securities exchange, costs related to compliance and reporting obligations, and increased expenses for insurance, investor relations, and professional services. We expect that our general and administrative expenses will increase in absolute dollars as our business grows but will decrease as a percentage of our revenue over time.

Interest Income, Interest Expense, and Other Income (Expense), Net

Interest income consists primarily of interest earned on our cash equivalents and investments.

Interest expense consists primarily of the amortization of the discount related to Attivo indemnity escrow liability.

Other income (expense), net consists primarily of foreign currency transaction gains and losses.

Provision for Income Taxes

Provision for (benefit from) income taxes consists primarily of income taxes in certain foreign and state jurisdictions in which we conduct business and a one-time benefit from the release of valuation allowance as a result of the Attivo business combination. In connection with our global consolidated losses, we maintain a full valuation allowance against our U.S. and Israel deferred tax assets because we have concluded that it is more likely than not that the deferred tax assets will not be realized.

Results of Operations

The following table sets forth our results of operations for the periods presented:

	Year Ended January 31,		
	2023	2022	2021
		(in thousands)	
Revenue	$ 422,179	$ 204,799	$ 93,056
Cost of revenue[(1)]	144,177	81,677	39,332
Gross profit	278,002	123,122	53,724
Operating expenses:			
Research and development[(1)]	207,008	136,274	62,444
Sales and marketing[(1)]	310,848	160,576	77,740
General and administrative[(1)]	162,722	93,504	29,059
Total operating expenses	680,578	390,354	169,243
Loss from operations	(402,576)	(267,232)	(115,519)
Interest income	21,408	202	231
Interest expense	(1,830)	(787)	(1,401)
Other expense, net	(1,293)	(2,280)	(424)
Loss before income taxes	(384,291)	(270,097)	(117,113)
Provision (benefit) for income taxes	(5,613)	1,004	460
Net loss	$ (378,678)	$ (271,101)	$ (117,573)

(1) Includes stock-based compensation expense as follows:

	Year Ended January 31,		
	2023	2022	2021
		(in thousands)	
Cost of revenue	$ 10,093	$ 3,618	$ 308
Research and development	51,771	35,358	6,590
Sales and marketing	40,115	15,460	3,835
General and administrative	62,487	33,453	5,179
Total stock-based compensation expense	$ 164,466	$ 87,889	$ 15,912

The following table sets forth the components of our consolidated statements of operations as a percentage of revenue for each of the periods presented:

	Year Ended January 31,		
	2023	2022	2021
	(as a percentage of total revenue)		
Revenue	100	100%	100%
Cost of revenue	34	40	42
Gross profit	66	60	58
Operating expenses:			
Research and development	49	67	67
Sales and marketing	74	78	84
General and administrative	39	46	31
Total operating expenses	161	191	182
Loss from operations	(95)	(130)	(124)
Interest income	5	—	—
Interest expense	—	—	(2)
Other expense, net	—	(1)	—
Loss before income taxes	(91)	(132)	(126)
Provision (benefit) for income taxes	(1)	—	—
Net loss	(90)%	(132)%	(126)%

Note: Certain figures may not sum due to rounding.

Comparison of the Years Ended January 31, 2023 and 2022

Revenue

	Year Ended January 31,		Change	
	2023	2022	$	%
	(dollars in thousands)			
Revenue	$ 422,179	$ 204,799	$ 217,380	106 %

Revenue increased by $217.4 million, or 106%, from $204.8 million for fiscal 2022 to $422.2 million for fiscal 2023, which was primarily driven by a combination of the addition of new customers and the sale of additional endpoints and modules to existing customers. In addition, there was an increase of $28.6 million derived from revenue resulting from the Attivo acquisition.

Cost of Revenue, Gross Profit, and Gross Margin

	Year Ended January 31,		Change	
	2023	2022	$	%
	(dollars in thousands)			
Cost of revenue	$ 144,177	$ 81,677	$ 62,500	77 %
Gross profit	$ 278,002	$ 123,122	$ 154,880	126 %
Gross margin	66 %	60 %		

Cost of revenue increased by $62.5 million from $81.7 million for fiscal 2022 to $144.2 million for fiscal 2023, primarily due to an increase of $26.4 million in overhead costs due to increase in our personnel to support overall growth, higher third-party cloud infrastructure expenses from increased data usage of $17.7 million, and an increase of $13.8 million from amortization of intangible assets. Gross margin increased from 60% for fiscal 2022 to 66% for fiscal 2023, primarily due to revenue growth from existing and new customers outpacing growth in cost of revenue.

Research and Development

	Year Ended January 31,		Change	
	2023	2022	$	%
	(dollars in thousands)			
Research and development expenses	$ 207,008	$ 136,274	$ 70,734	52 %

Research and development expenses increased from $136.3 million in fiscal 2022 to $207.0 million in fiscal 2023, primarily due to an increase in personnel-related expenses of $45.7 million, including an increase of $15.7 million related to stock-based compensation expense as a result of increased headcount, an increase of $16.8 million in third-party cloud infrastructure expenses incurred in developing our platform and modules, and an increase of $6.1 million related to allocated overhead costs as a result of increased headcount.

Sales and Marketing

	Year Ended January 31,		Change	
	2023	2022	$	%
	(dollars in thousands)			
Sales and marketing expenses	$ 310,848	$ 160,576	$ 150,272	94 %

Sales and marketing expenses increased from $160.6 million in fiscal 2022 to $310.8 million in fiscal 2023, primarily due to an increase in personnel-related expenses of $103.2 million, including an increase of $24.7 million in stock-based compensation expense as a result of increased headcount. In addition, there was an increase of $17.4 million in marketing-related expenses, an increase of $9.6 million related to allocated overhead costs as a result of increased headcount, and the remaining increase is primarily a result of increased travel and entertainment expenses.

General and Administrative

	Year Ended January 31,		Change	
	2023	2022	$	%
	(dollars in thousands)			
General and administrative expenses	$ 162,722	$ 93,504	$ 69,218	74 %

General and administrative expenses increased from $93.5 million in fiscal 2022 to $162.7 million in fiscal 2023, primarily due to an increase in personnel-related expenses of $57.0 million, including an increase of $29.0 million in stock-based compensation expense as a result of increased headcount. In addition, there was an increase of $14.1 million in outside consulting services, legal, audit, tax and software subscription expenses.

Interest Income, Interest Expense, and Other Income (Expense), Net

	Year Ended January 31,		Change	
	2023	2022	$	%
	(dollars in thousands)			
Interest income	$ 21,408	$ 202	$ 21,206	10498 %
Interest expense	$ (1,830)	$ (787)	$ (1,043)	133 %
Other income (expense), net	$ (1,293)	$ (2,280)	$ 987	(43)%

Interest income increased $21.2 million as a result of interest earned on investments, which we did not have in fiscal year 2022. Interest expense increased due to the amortization of the discount related to Attivo indemnity escrow liability. The decrease in other expense, net is primarily due to net foreign currency exchange gains.

Provision for Income Taxes

	Year Ended January 31,		Change	
	2023	2022	$	%
	(dollars in thousands)			
Provision (benefit) for income taxes	$ (5,613)	$ 1,004	$ (6,617)	(659)%

The provision for income taxes decreased primarily as a result of the application of our deferred tax assets with a full valuation allowance to net deferred tax liability of Attivo acquired intangibles.

Liquidity and Capital Resources

In July 2021, upon completion of our IPO and the concurrent private placement, we received net proceeds of $1.4 billion, after deducting underwriters' discounts and commissions and estimated offering expenses of $81.6 million. We did not pay any underwriting discounts or commissions with respect to shares that were sold in the private placement.

We have financed operations primarily through proceeds received from sales of equity securities, payments received from our customers, and borrowings under our loan and security agreement, and we have generated operating losses, as reflected in our accumulated deficit of $1,000.4 million and $621.7 million as of January 31, 2023 and 2022, respectively. We expect these losses and operating losses to continue for the foreseeable future. We also expect to incur significant research and development, sales and marketing, and general and administrative expenses over the next several years in connection with the continued development and expansion of our business. As of January 31, 2023 and 2022, our principal source of liquidity was cash, cash equivalents, and investments of $1.2 billion and $1.7 billion, respectively.

In the short term, we believe that our existing cash, cash equivalents, and investments will be sufficient to support working capital and capital expenditure requirements for at least the next 12 months. In the long term, our future capital requirements will depend on many factors, including our revenue growth rate, the timing and the amount of cash received from customers, the expansion of sales and marketing activities, the timing and extent of spending to support research and development efforts, the price at which we are able to purchase third-party cloud infrastructure, expenses associated with our international expansion, the introduction of platform enhancements, and the continuing market adoption of our platform. We have, and in the future, we may enter into arrangements to acquire or invest in complementary businesses, products, and technologies. We may be required to seek additional equity or debt financing. In the event that we require additional financing, we may not be able to raise such financing on terms acceptable to us or at all. If we are unable to raise additional capital or generate cash flows necessary to expand our operations and invest in continued innovation, we may not be able to compete successfully, which would harm our business, operating results, and financial condition.

On March 10, 2023, SVB was closed by the California Department of Financial Protection and Innovation, which also appointed the FDIC as receiver. While some of our cash, cash equivalents and short-term investments were held at SVB prior to its closure, in light of the FDIC's announcement that depositors of the institution will be made whole, we currently have full access to these funds. We hold our cash, cash equivalents, and investments with a diverse group of banking partners and, as a result, we have not experienced a material impact to our business as a result of SVB's closure. However, any instability in the global banking system may impact liquidity both in the short term and long term and may result in adverse impacts to our or our customers' business, including in our customers' ability to pay for our platform.

The following table shows a summary of our cash flows for the periods presented:

	Years Ended January 31,		
	2023	2022	2021
	(in thousands)		
Net cash used in operating activities	$ (193,287)	$ (95,588)	$ (66,570)
Net cash used in investing activities	$ (1,312,666)	$ (19,743)	$ (6,265)
Net cash provided by financing activities	$ 36,308	$ 1,387,124	$ 423,978

Operating Activities

Our largest source of operating cash is payments received from our customers. Our primary uses of cash from operating activities are for personnel-related expenses, sales and marketing expenses, third-party cloud infrastructure expenses, and overhead expenses. We have generated negative cash flows from operating activities and have supplemented working capital through net proceeds from the sale of equity securities.

Cash used in operating activities primarily consists of our net loss adjusted for certain non-cash items, including stock-based compensation expense, depreciation and amortization, amortization of deferred contract acquisition costs, and changes in operating assets and liabilities during each period.

Cash used in operating activities during fiscal 2023 was $193.3 million, primarily consisting of our net loss of $378.7 million, and $35.4 million used in net changes to our operating assets and liabilities, partially offset by non-cash items of $220.8 million. The main drivers of the changes in operating assets and liabilities were a $61.3 million increase in deferred contract acquisition costs, a $44.4 million increase in accounts receivable due to timing of cash received from customers, a $14.5 million increase in prepaid expenses and other assets primarily due to annual insurance renewal and prepaid sponsorship costs, and a $7.2 million decrease in accrued payroll and benefits. These amounts were partially offset by a $92.5 million increase in deferred revenue resulting primarily from increased subscription contracts.

Cash used in operating activities during fiscal 2022 was $95.6 million, primarily consisting of our net loss of $271.1 million, adjusted for non-cash items of $119.9 million and net cash inflows of $55.6 million provided by changes in our operating assets and liabilities. The main drivers of the changes in operating assets and liabilities were a $115.1 million increase in deferred revenue, resulting primarily from increased subscription contracts, a $41.5 million increase in accrued payroll and benefits due to increased headcount, a $24.2 million increase in accrued and other liabilities primarily due to net invoices received from vendors. These amounts were partially offset by a $59.1 million increase in accounts receivable due to an increase in sales, a $53.6 million increase in deferred contract acquisition costs, a $7.3 million increase in prepaid expenses and other assets, primarily due to annual insurance renewal and prepaid sponsorship costs and a $2.1 million decrease in accounts payable due to timing of payments.

Investing Activities

Cash used in investing activities during fiscal 2023 was $1,312.7 million, consisting of $1,938.0 million of investment purchases, $281.0 million of net cash paid for the acquisition of Attivo, $13.5 million of capitalized

internal-use software costs, and $5.0 million of purchases of property and equipment to support additional office facilities, partially offset by $925.2 million of investment maturities.

Cash used in investing activities during fiscal 2022 was $19.7 million, consisting of $6.0 million of cash paid for purchases of strategic investments, $3.4 million of cash paid for the acquisition of Scalyr, $5.8 million of capitalized internal-use software costs, and $3.7 million of purchases of property and equipment to support additional office facilities.

Financing Activities

Cash provided by financing activities during fiscal 2023 was $36.3 million, consisting of $19.2 million of proceeds from the issuance of common stock under our 2021 Employee Stock Purchase Plan, $17.3 million of proceeds from the exercise of employee stock options, partially offset by $0.2 million of payments of deferred offering costs.

Cash provided by financing activities during fiscal 2022 was $1.4 billion, consisting of $1.4 billion of aggregate net proceeds from our IPO and the concurrent private placement completed in July 2021, net of underwriting discounts and commissions, $14.6 million of proceeds from the exercise of stock options, $11.4 million of proceeds from issuance of common stock under the ESPP, partially offset by a $20.0 million repayment of our revolving line of credit and $7.4 million of payments of deferred offering costs.

Contractual Obligations and Commitments

Our operating lease obligations as of January 31, 2023 were approximately $30.4 million, with $4.8 million expected to be paid within 12 months and the remainder thereafter. Our operating leases are related to leased facilities under operating lease agreements expiring through fiscal 2029. We have office facility operating leases in the United States, the Czech Republic, France, Israel, United Arab Emirates, and other countries. See Note 7, *Leases*, to the consolidated financial statements included in Part II, Item 8, Financial Statements and Supplementary Data.

Our purchase obligations as of January 31, 2023 were approximately $871.5 million, with $81.9 million expected to be paid within 12 months and the remainder thereafter. Our purchase obligations primarily relate to a non-cancellable purchase commitment entered in February 2023 with our cloud infrastructure vendor for a total net value of $860.0 million over the next six years. See Note 17 to our consolidated financial statements included elsewhere in this Annual Report on Form 10-K for more information regarding this subsequent event.

Off-Balance Sheet Arrangements

We did not have during the periods presented, and we do not currently have, any off-balance sheet financing arrangements or any relationships with unconsolidated entities or financial partnerships, such as structured finance or special purpose entities, that were established for the purpose of facilitating off-balance sheet arrangements or other contractually narrow or limited purposes.

Critical Accounting Policies and Estimates

Our consolidated financial statements are prepared in accordance with GAAP. The preparation of consolidated financial statements requires us to make estimates and assumptions that affect the reported amounts of assets, liabilities, revenue, expenses, and related disclosures. We base our estimates on historical experience and on various other assumptions that we believe to be reasonable under the circumstances, and we evaluate our estimates and assumptions on an ongoing basis. Actual results could differ significantly from the estimates made by management. To the extent that there are differences between our estimates and actual results, our future financial statement presentation, financial condition, operating results, and cash flows will be affected.

The critical accounting policies requiring estimates, assumptions, and judgments that we believe have the most significant impact on our consolidated financial statements are described below.

Revenue Recognition

We recognize revenue in accordance with Accounting Standards Codification 606, *Revenue from Contracts with Customers*.

We consider the terms and conditions of contracts with customers and our customary business practices in identifying contracts. We determine we have a contract with a customer when the contract is approved, the payment terms for the services can be identified, each party's rights regarding the services to be transferred can be identified, the contract has commercial substance, and we have determined that the customer has the ability and intent to pay. We apply judgment in determining the customer's ability and intent to pay, which is based on a variety of factors, including the customer's historical payment experience or, in the case of a new customer, credit and financial information pertaining to such customer.

Our contracts with customers may contain multiple performance obligations, which are accounted for separately if they are capable of being distinct and are distinct in the context of the contract. Contracts that contain multiple performance obligations require an allocation of the transaction price to each performance obligation based on relative standalone selling price (SSP). We apply judgment in determining SSP for our performance obligations. To determine SSP, we maximize the use of observable standalone sales and observable data, where available. In instances where performance obligations do not have observable standalone sales, we utilize available information that may include but is not limited to product groupings, or applying the expected cost-plus margin approach to estimate the price we would charge if the service was sold separately. Certain sales arrangements may include variable consideration, which is recorded as part of the transaction price if, in our judgment, it is probable that no significant future reversal of cumulative revenue under the contract will occur.

Business Combinations

We account for our acquisitions using the acquisition method of accounting. We allocate the fair value of purchase consideration to the tangible and intangible assets acquired, and liabilities assumed, based on their estimated fair values. The excess of the fair value of purchase consideration over the values of these identifiable assets and liabilities is recorded as goodwill. When determining the fair value of assets acquired and liabilities assumed, management makes significant estimates and assumptions, especially with respect to intangible assets. Significant estimates in valuing certain identifiable assets include, but are not limited to, the selection of valuation methodologies, forecasted revenue, discount rates, and useful lives. Management's estimates of fair value are based upon assumptions believed to be reasonable, but which are inherently uncertain and unpredictable and, as a result, actual results may differ from estimates.

Recently Issued Accounting Pronouncements

See Note 2 to our consolidated financial statements included elsewhere in this Annual Report on Form 10-K for more information regarding recently issued accounting pronouncements.

ITEM 7A. QUANTITATIVE AND QUALITATIVE DISCLOSURES ABOUT MARKET RISK

We are exposed to market risk in the ordinary course of our business. Market risk represents the risk of loss that may impact our financial condition due to adverse changes in financial market prices and rates. Our market risk exposure is primarily the result of fluctuations in interest rates and foreign currency exchange rates.

Interest Rate Risk

As of January 31, 2023, we had $1.2 billion of cash, cash equivalents, and investments, which consist of money market funds, commercial paper, corporate notes and bonds and U.S. government securities. We also had $64.5 million of restricted cash as of January 31, 2023 primarily due to outstanding letters of credit established in connection with lease agreements for our facilities. Our cash, cash equivalents, and investments are held for working capital purposes. We do not enter into investments for trading or speculative purposes. The effect of a hypothetical 100 basis point change in interest rates would not have had a material effect on the fair market value of our portfolio

as of January 31, 2023. We therefore do not expect our results of operations or cash flows to be materially affected by a sudden change in market interest rates.

Foreign Currency Exchange Risk

To date, primarily all of our sales contracts have been denominated in U.S. dollars, therefore our revenue is not subject to foreign currency risk. Operating expenses within the United States are primarily denominated in U.S. dollars, while operating expenses incurred outside the United States are primarily denominated in each country's respective local currency. Our operating results and cash flows are, therefore, subject to fluctuations due to changes in foreign currency exchange rates. Foreign currency transaction gains and losses are recorded in other income (expense), net in the consolidated statements of operations. As the impact of foreign currency exchange rates has not been material to our historical operating results, we have not entered into derivative or hedging transactions, but we may do so in the future if our exposure to foreign currency becomes more significant. A hypothetical 10% adverse change in the U.S. dollar against other currencies would have resulted in an increase in operating loss of approximately $9.7 million for fiscal 2023. The hypothetical impact in fiscal 2022 and 2021 would not have been material.

ITEM 8. FINANCIAL STATEMENTS AND SUPPLEMENTARY DATA

INDEX TO CONSOLIDATED FINANCIAL STATEMENTS

REPORT OF INDEPENDENT REGISTERED PUBLIC ACCOUNTING FIRM

To the stockholders and the Board of Directors of SentinelOne, Inc.

Opinion on the Financial Statements

We have audited the accompanying consolidated balance sheets of SentinelOne, Inc. and subsidiaries (the "Company") as of January 31, 2023 and 2022, the related consolidated statements of operations, comprehensive loss, redeemable convertible preferred stock and stockholders' equity (deficit), and cash flows, for each of the three years in the period ended January 31, 2023, and the related notes (collectively referred to as the "financial statements"). In our opinion, the financial statements present fairly, in all material respects, the financial position of the Company as of January 31, 2023 and 2022, and the results of its operations and its cash flows for each of the three years in the period ended January 31, 2023, in conformity with accounting principles generally accepted in the United States of America.

We have also audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States) (PCAOB), the Company's internal control over financial reporting as of January 31, 2023, based on criteria established in *Internal Control — Integrated Framework (2013)* issued by the Committee of Sponsoring Organizations of the Treadway Commission and our report dated March 29, 2023, expressed an unqualified opinion on the Company's internal control over financial reporting.

Basis for Opinion

These financial statements are the responsibility of the Company's management. Our responsibility is to express an opinion on the Company's financial statements based on our audits. We are a public accounting firm registered with the Public Company Accounting Oversight Board (United States) (PCAOB) and are required to be independent with respect to the Company in accordance with the U.S. federal securities laws and the applicable rules and regulations of the Securities and Exchange Commission and the PCAOB.

We conducted our audits in accordance with the standards of the PCAOB. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether due to error or fraud. Our audits included performing procedures to assess the risks of material misstatement of the financial statements, whether due to error or fraud, and performing procedures that respond to those risks. Such procedures included examining, on a test basis, evidence regarding the amounts and disclosures in the financial statements. Our audits also included evaluating the accounting principles used and significant estimates made by management, as well as evaluating the overall presentation of the financial statements. We believe that our audits provide a reasonable basis for our opinion.

Critical Audit Matters

The critical audit matters communicated below are matters arising from the current-period audit of the financial statements that were communicated or required to be communicated to the audit committee and that (1) relate to accounts or disclosures that are material to the financial statements and (2) involved our especially challenging, subjective, or complex judgments. The communication of critical audit matters does not alter in any way our opinion on the financial statements, taken as a whole, and we are not, by communicating the critical audit matters below, providing separate opinions on the critical audit matters or on the accounts or disclosures to which they relate.

Acquisitions – Acquisition of Attivo — Refer to Notes 2 and 15 to the financial statements

Critical Audit Matter Description

On May 3, 2022, the Company completed the acquisition of Attivo Networks, Inc. for consideration of $534.8 million. The Company accounted for the acquisition as a business combination. Accordingly, the purchase price was allocated to the assets acquired and liabilities assumed based on their respective fair values, including $77.6 million of customer relationships and $63.2 million of developed technology.

We identified forecasted revenue used in the valuation of customer relationships and developed technology as a critical audit matter because it requires management to make significant estimates and assumptions. This required a high degree of auditor judgment and an increased extent of effort when performing audit procedures to evaluate the reasonableness of management's estimates and assumptions related to forecasted revenue.

How the Critical Audit Matter Was Addressed in the Audit

Our audit procedures related to the forecasted revenue included the following, among others:

- Assessed the reasonableness of forecasted revenue, by performing a retrospective review of the forecasted revenue and comparing it to (1) historical revenue results of the acquired business, (2) historical and forecasted revenue of peer companies in industry, and (3) communications with the Board of Directors.

Revenue Recognition — Refer to Notes 2 and 3 to the financial statements

Critical Audit Matter Description

The Company generates substantially all its revenue from subscriptions to its Singularity Platform. This includes subscription, premium support and maintenance and other Singularity Modules, which are distinct performance obligations and are recognized ratably over the subscription term as the performance obligations are satisfied. To determine the amount and pattern of revenue recognition, management identifies and evaluates the relevant contractual terms in its customer contracts based on its accounting policy (collectively "contract terms and conditions").

Given the significance of the proper identification and evaluation of contract terms and conditions to the amount and pattern of revenue recognition, performing audit procedures to evaluate whether management properly identified the relevant contract terms and conditions that impact the amount and pattern of revenue recognition required a high degree of auditor judgment and an increased extent of effort.

How the Critical Audit Matter Was Addressed in the Audit

Our audit procedures related to the evaluation of management's identification of the relevant contract terms and conditions that impact the amount and pattern of revenue recognition included the following, among others:

- We assessed management's significant accounting policies related to revenue recognition for compliance with Accounting Standards Codification (ASC) 606, Revenue from Contracts with Customers.
- We selected a sample of recorded revenue transactions and contracts entered into during the period and performed the following procedures:
  - Obtained and read customer source documents and the contract, including master agreements and related amendments, to evaluate if relevant contract terms and conditions have been appropriately identified by management.
  - Evaluated the appropriateness of management's determination of the impact of those terms and conditions on the amount and pattern of revenue recognition.

/s/ DELOITTE & TOUCHE LLP

San Jose, California
March 29, 2023

We have served as the Company's auditor since 2018.

REPORT OF INDEPENDENT REGISTERED PUBLIC ACCOUNTING FIRM

To the stockholders and the Board of Directors of SentinelOne, Inc.

Opinion on Internal Control over Financial Reporting

We have audited the internal control over financial reporting of SentinelOne, Inc. and subsidiaries (the "Company") as of January 31, 2023 and 2022, based on criteria established in *Internal Control — Integrated Framework (2013)* issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). In our opinion, the Company maintained, in all material respects, effective internal control over financial reporting as of January 31, 2023, based on criteria established in *Internal Control — Integrated Framework (2013)* issued by COSO.

We have also audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States) (PCAOB), the consolidated financial statements as of and for the year ended January 31, 2023, of the Company and our report dated March 29, 2023, expressed an unqualified opinion on those financial statements.

As described in Management's Report on Internal Control Over Financial Reporting, management excluded from its assessment the internal control over financial reporting at Attivo Networks, which was acquired in May 2022, and whose financial statements constitute approximately 0.5% of total assets as of January 31, 2023 and approximately 7% of total revenue during the year ended January 31, 2023. Accordingly, our audit did not include the internal control over financial reporting at Attivo Networks.

Basis for Opinion

The Company's management is responsible for maintaining effective internal control over financial reporting and for its assessment of the effectiveness of internal control over financial reporting, included in the accompanying Management's Report on Internal Control over Financial Reporting. Our responsibility is to express an opinion on the Company's internal control over financial reporting based on our audit. We are a public accounting firm registered with the PCAOB and are required to be independent with respect to the Company in accordance with the U.S. federal securities laws and the applicable rules and regulations of the Securities and Exchange Commission and the PCAOB.

We conducted our audit in accordance with the standards of the PCAOB. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether effective internal control over financial reporting was maintained in all material respects. Our audit included obtaining an understanding of internal control over financial reporting, assessing the risk that a material weakness exists, testing and evaluating the design and operating effectiveness of internal control based on the assessed risk, and performing such other procedures as we considered necessary in the circumstances. We believe that our audit provides a reasonable basis for our opinion.

Definition and Limitations of Internal Control over Financial Reporting

A company's internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. A company's internal control over financial reporting includes those policies and procedures that (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and (3) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

/s/ DELOITTE & TOUCHE LLP

San Jose, California
March 29, 2023

SENTINELONE, INC.

CONSOLIDATED BALANCE SHEETS
(in thousands, except share and per share data)

	January 31, 2023	January 31, 2022
Assets		
Current assets:		
Cash and cash equivalents	$ 137,941	$ 1,669,304
Short-term investments	485,584	374
Accounts receivable, net	151,492	101,491
Deferred contract acquisition costs, current	37,904	27,546
Prepaid expenses and other current assets	101,812	18,939
Total current assets	914,733	1,817,654
Property and equipment, net	38,741	24,918
Operating lease right-of-use assets	23,564	23,884
Long-term investments	535,422	6,000
Deferred contract acquisition costs, non-current	55,536	41,022
Intangible assets, net	145,093	15,807
Goodwill	540,308	108,193
Other assets	5,516	4,703
Total assets	$ 2,258,913	$ 2,042,181
Liabilities and Stockholders' Equity		
Current liabilities:		
Accounts payable	$ 11,214	$ 9,944
Accrued liabilities	100,015	22,657
Accrued payroll and benefits	54,955	61,150
Operating lease liabilities, current	3,895	4,613
Deferred revenue, current	303,200	182,957
Total current liabilities	473,279	281,321
Deferred revenue, non-current	103,062	79,062
Operating lease liabilities, non-current	23,079	24,467
Other liabilities	2,788	6,543
Total liabilities	602,208	391,393
Commitments and contingencies (Note 13)		
Stockholders' equity:		
Preferred stock; $0.0001 par value; 50,000,000 shares authorized as of January 31, 2023 and 2022, and no shares issued and outstanding as of January 31, 2023 and 2022	—	—
Class A common stock; $0.0001 par value; 1,500,000,000 shares authorized as of January 31, 2023 and 2022; 222,951,206 and 162,666,515 shares issued and outstanding as of January 31, 2023 and 2022, respectively	21	16
Class B common stock; $0.0001 par value; 300,000,000 shares authorized as of January 31, 2023 and 2022; 63,812,651 and 107,785,100 shares issued and outstanding as of January 31, 2023 and 2022, respectively	8	11
Additional paid-in capital	2,663,394	2,271,980
Accumulated other comprehensive income (loss)	(6,367)	454
Accumulated deficit	(1,000,351)	(621,673)
Total stockholders' equity	1,656,705	1,650,788
Total liabilities and stockholders' equity	$ 2,258,913	$ 2,042,181

The accompanying notes are an integral part of these consolidated financial statements.

SENTINELONE, INC.

CONSOLIDATED STATEMENTS OF OPERATIONS
(in thousands, except share and per share data)

	Year Ended January 31,		
	2023	2022	2021
Revenue	$ 422,179	$ 204,799	$ 93,056
Cost of revenue	144,177	81,677	39,332
Gross profit	278,002	123,122	53,724
Operating expenses:			
Research and development	207,008	136,274	62,444
Sales and marketing	310,848	160,576	77,740
General and administrative	162,722	93,504	29,059
Total operating expenses	680,578	390,354	169,243
Loss from operations	(402,576)	(267,232)	(115,519)
Interest income	21,408	202	231
Interest expense	(1,830)	(787)	(1,401)
Other expense, net	(1,293)	(2,280)	(424)
Loss before income taxes	(384,291)	(270,097)	(117,113)
Provision (benefit) for income taxes	(5,613)	1,004	460
Net loss	$ (378,678)	$ (271,101)	$ (117,573)
Net loss per share attributable to Class A and Class B common stockholders, basic and diluted	$ (1.36)	$ (1.56)	$ (3.31)
Weighted-average shares used in computing net loss per share attributable to Class A and Class B common stockholders, basic and diluted	277,802,861	174,051,203	35,482,444

The accompanying notes are an integral part of these consolidated financial statements.

SENTINELONE, INC.

CONSOLIDATED STATEMENTS OF COMPREHENSIVE LOSS
(in thousands)

	Year Ended January 31,		
	2023	2022	2021
Net loss	$ (378,678)	$ (271,101)	$ (117,573)
Other comprehensive income (loss):			
Changes in unrealized losses on investments	(6,821)	—	—
Foreign currency translation adjustments	—	289	366
Total comprehensive loss	$ (385,499)	$ (270,812)	$ (117,207)

The accompanying notes are an integral part of these consolidated financial statements.

SENTINELONE, INC.

CONSOLIDATED STATEMENTS OF REDEEMABLE CONVERTIBLE PREFERRED STOCK AND STOCKHOLDERS' EQUITY (DEFICIT)
(in thousands, except share data)

	Redeemable Convertible Preferred Stock		Class A and Class B Common Stock		Additional Paid-In Capital	Accumulated Other Comprehensive Income (Loss)	Accumulated Deficit	Total Stockholders' Equity (Deficit)
	Shares	Amount	Shares	Amount				
Balances as of January 31, 2020	113,523,948	$ 201,826	33,550,809	$ 1	$ 8,986	$ (201)	$ (232,999)	$ (224,213)
Issuance of Series E Preferred Stock, net of issuance costs of $0.1 million	31,405,183	152,539	—	—	—	—	—	—
Issuance of Series F Preferred Stock, net of issuance costs of $0.1 million	22,128,982	266,774	—	—	—	—	—	—
Issuance of common stock upon exercise of options	—	—	5,358,692	1	4,607	—	—	4,608
Issuance of common stock upon exercise of warrants	—	—	321,802	—	200	—	—	200
Issuance of common stock for services provided	—	—	11,013	—	47	—	—	47
Vesting of early exercised options	—	—	—	—	71	—	—	71
Stock based compensation expense	—	—	—	—	15,958	—	—	15,958
Foreign currency translation adjustments	—	—	—	—	—	366	—	366
Net loss	—	—	—	—	—	—	(117,573)	(117,573)
Balances as of January 31, 2021	167,058,113	$ 621,139	39,242,316	$ 2	$ 29,869	$ 165	$ (350,572)	$ (320,536)
Conversion of redeemable convertible preferred stock to common stock upon initial public offering	(167,058,113)	(621,139)	169,787,200	10	621,129	—	—	621,139
Issuance of common stock upon initial public offering and private placements, net of underwriting discounts and commissions	—	—	41,678,568	4	1,380,956	—	—	1,380,960
Issuance of common stock upon exercise of options	—	—	9,793,331	10	14,611	—	—	14,621
Issuance of common stock upon exercise of warrants	—	—	940,953	—	—	—	—	—
Vesting of restricted stock units	—	—	15,218	—	—	—	—	—
Issuance of common stock under employee stock purchase plan	—	—	381,716	—	11,356	—	—	11,356
Vesting of early exercised options	—	—	—	—	572	—	—	572
Issuance of common stock and awards assumed in connection with acquisition	—	—	7,277,214	1	120,319	—	—	120,320
Issuance of restricted stock awards	—	—	1,315,099	—	—	—	—	—
Stock-based compensation	—	—	—	—	92,668	—	—	92,668
Issuance of restricted stock for services provided	—	—	20,000	—	500	—	—	500
Foreign currency translation adjustments	—	—	—	—	—	289	—	289
Net loss	—	—	—	—	—	—	(271,101)	(271,101)
Balances as of January 31, 2022	—	—	270,451,615	$ 27	$ 2,271,980	$ 454	$ (621,673)	$ 1,650,788

SENTINELONE, INC.

CONSOLIDATED STATEMENTS OF REDEEMABLE CONVERTIBLE PREFERRED STOCK AND STOCKHOLDERS' EQUITY (DEFICIT)
(in thousands, except share data)

Issuance of common stock upon exercise of options	—	—	7,650,525	1	17,334	—	—	17,335
Vesting of restricted stock units	—	—	1,303,854	—	—	—	—	—
Issuance of common stock under employee stock purchase plan	—	—	1,335,183	—	19,159	—	—	19,159
Cancellation of holdback shares	—	—	(9,551)	—	—	—	—	—
Vesting of early exercised options	—	—	—	—	103	—	—	103
Issuance of common stock in connection with acquisition	—	—	6,032,231	1	186,332	—	—	186,333
Stock-based compensation	—	—	—	—	168,486	—	—	168,486
Other comprehensive loss	—	—	—	—	—	(6,821)	—	(6,821)
Net loss	—	—	—	—	—	—	(378,678)	(378,678)
Balance as of January 31, 2023	—	—	286,763,857	29	2,663,394	(6,367)	(1,000,351)	1,656,705

The accompanying notes are an integral part of these consolidated financial statements.

SENTINELONE, INC.

CONSOLIDATED STATEMENTS OF CASH FLOWS
(in thousands)

	Year Ended January 31,		
	2023	2022	2021
CASH FLOW FROM OPERATING ACTIVITIES:			
Net loss	$ (378,678)	$ (271,101)	$ (117,573)
Adjustments to reconcile net loss to net cash used in operating activities:			
Depreciation and amortization	29,721	7,909	2,837
Amortization of deferred contract acquisition costs	36,417	21,670	11,518
Non-cash operating lease costs	3,559	2,862	3,085
Stock-based compensation expense	164,466	87,889	15,912
Loss on investments, accretion of discounts, and amortization of premiums on investments, net	(12,217)	—	—
Other	(1,187)	(456)	(22)
Changes in operating assets and liabilities, net of effects of acquisition			
Accounts receivable	(44,442)	(59,082)	(8,320)
Prepaid expenses and other current assets	(14,499)	(7,319)	(9,438)
Deferred contract acquisition costs	(61,289)	(53,565)	(26,934)
Accounts payable	3,670	(2,076)	7,429
Accrued liabilities	4,976	18,080	1,374
Accrued payroll and benefits	(7,205)	41,462	7,758
Operating lease liabilities	(5,320)	(3,139)	(3,261)
Deferred revenue	92,496	115,142	49,065
Other liabilities	(3,755)	6,136	—
Net cash used in operating activities	(193,287)	(95,588)	(66,570)
CASH FLOW FROM INVESTING ACTIVITIES:			
Purchases of property and equipment	(4,953)	(3,653)	(3,283)
Purchases of intangible assets	(407)	(802)	(224)
Capitalization of internal-use software	(13,452)	(5,839)	(2,758)
Purchases of investments	(1,938,007)	(6,000)	—
Maturities of investments	925,185	—	—
Cash paid for acquisition, net of cash acquired	(281,032)	(3,449)	—
Net cash used in investing activities	(1,312,666)	(19,743)	(6,265)
CASH FLOW FROM FINANCING ACTIVITIES:			
Proceeds from issuance of Series E redeemable convertible preferred stock, net of issuance costs	—	—	152,539
Proceeds from issuance of Series F redeemable convertible preferred stock, net of issuance costs	—	—	266,774
Payments of deferred offering costs	(186)	(7,416)	—
Proceeds from revolving line of credit	—	—	19,857
Repayment of debt	—	(20,000)	(20,000)
Proceeds from exercise of stock options	17,335	14,622	4,608
Proceeds from exercise of warrants	—	—	200
Proceeds from issuance of common stock under the employee stock purchase plan	19,159	11,356	—
Proceeds from initial public offering and private placement, net of underwriting discounts and commissions	—	1,388,562	—
Net cash provided by financing activities	36,308	1,387,124	423,978
EFFECT OF EXCHANGE RATE CHANGES ON CASH AND CASH EQUIVALENTS	—	1,146	289
NET CHANGE IN CASH, CASH EQUIVALENTS, AND RESTRICTED CASH	(1,469,645)	1,272,939	351,432
CASH, CASH EQUIVALENTS, AND RESTRICTED CASH–Beginning of period	1,672,051	399,112	47,680
CASH, CASH EQUIVALENTS, AND RESTRICTED CASH–End of period	$ 202,406	$ 1,672,051	$ 399,112
SUPPLEMENTAL DISCLOSURE OF CASH FLOW INFORMATION:			
Interest paid	$ 17	$ 409	1,379
Income taxes paid, net	$ 500	$ 583	298
SUPPLEMENTAL DISCLOSURE OF NON-CASH INVESTING AND FINANCING ACTIVITIES:			
Stock-based compensation capitalized as internal-use software	$ 4,020	$ 4,779	46
Property and equipment purchased but not yet paid	$ 203	$ 913	78

SENTINELONE, INC.

CONSOLIDATED STATEMENTS OF CASH FLOWS
(in thousands)

Vesting of early exercised stock options	$	103	$	575		71
Deferred offering costs accrued but not yet paid	$	—	$	186		—
Issuance of common stock and assumed equity awards in connection with acquisition	$	186,332	$	120,319		—
Conversion of redeemable convertible preferred stock to common stock upon initial public offering	$	—	$	621,139		—

The accompanying notes are an integral part of these consolidated financial statements.

SENTINELONE, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS

1. ORGANIZATION AND DESCRIPTION OF BUSINESS

Business

SentinelOne, Inc. (SentinelOne, we, our, or us) was incorporated in January 2013 in the State of Delaware. On March 29, 2021, we amended our certificate of incorporation to change our name from Sentinel Labs, Inc. to SentinelOne, Inc. We are a cybersecurity provider that delivers an artificial intelligence-powered platform to enable autonomous cybersecurity defense. Our headquarters is located in Mountain View, California with various other global office locations.

2. SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES

Basis of Presentation

The consolidated financial statements have been prepared in accordance with accounting principles generally accepted in the United States of America (GAAP). The consolidated financial statements include the accounts of SentinelOne and our wholly-owned subsidiaries. All intercompany balances and transactions have been eliminated in consolidation.

Fiscal Year

Our fiscal year ends on January 31. References to fiscal 2023, 2022 and 2021 refer to the fiscal years ended January 31, 2023, January 31, 2022 and January 31, 2021, respectively.

Use of Estimates

The preparation of the consolidated financial statements in conformity with GAAP requires management to make estimates and assumptions that affect the amounts reported in the consolidated financial statements and accompanying notes. These estimates include, but are not limited to, stock-based compensation, the period of benefit for deferred contract acquisition costs, useful lives of long-lived assets and intangibles, the valuation of intangibles acquired as part of a business combination, and accounting for income taxes. Actual results could differ from those estimates.

As the impact of the COVID-19 pandemic continues to evolve, estimates and assumptions about future events and their effects cannot be determined with certainty and therefore require increased judgment. These estimates and assumptions may change in future periods and will be recognized in the consolidated financial statements as new events occur and additional information becomes known. To the extent our actual results differ materially from those estimates and assumptions, our future financial statements could be affected.

Segment and Geographic Information

We have a single operating and reportable segment. Our chief operating decision maker (CODM) is our Chief Executive Officer. The CODM reviews financial information presented on a consolidated basis for purposes of making operating decisions, allocating resources, and assessing financial performance. For information regarding our revenue and long-lived assets by geography, see Notes 3 and 12, respectively.

Foreign Currency

During fiscal 2022, we changed the functional currency of certain subsidiaries from their respective local currency to the U.S. dollar. The change in functional currency is due to increased exposure to the U.S. dollar as a result of a change in facts and circumstances in the primary economic environment in which these subsidiaries operate. The effects of the change in functional currency were not significant to our consolidated financial statements.

Subsequent to the change, our reporting currency and the functional currency of our foreign subsidiaries is the U.S. dollar. Foreign currency transaction gains and losses are recorded in other income (expense), net in the consolidated statements of operations and were not material for any periods presented.

Revenue Recognition

We recognize revenue in accordance with Accounting Standards Codification (ASC) 606, Revenue from Contracts with Customers.

Revenue is recognized when a customer obtains control of promised services. The amount of revenue recognized reflects the consideration that we expect to be entitled to receive in exchange for the subscriptions and services. We apply the following five-step approach to recognize revenue:

(i) **Identification of the Contract, or Contracts, with the Customer**—We determine that we have a contract with a customer when the contract is approved, the payment terms for the services can be identified, each party's rights regarding the services to be transferred can be identified, the customer has the ability and intent to pay, and the contract has commercial substance. We apply judgment in determining the customer's ability and intent to pay, which is based on a variety of factors, including the customer's historical payment experience or, in the case of a new customer, credit and financial information of the customer.

We sell through our indirect relationships with our channel partners or direct relationships with end customers through our internal sales force. Apart from certain sales arrangements where channel partners are determined to be our customers, we have concluded that the end customer is our customer.

(ii) **Identification of the Performance Obligations in the Contract**—Performance obligations in a contract are identified based on the services that will be transferred to a customer that are both capable of being distinct, where the customer can benefit from the service either on its own or together with other resources that are readily available to the customer, and are distinct in the context of the contract, whereby the transfer of the services is separately identifiable from other promises in the contract. To the extent a contract includes multiple promised services, we apply judgment to determine whether promised services are capable of being distinct and distinct in the context of the contract. If these criteria are not met, the promised services are accounted for as a combined performance obligation.

We have concluded that our contracts with customers do not contain warranties that give rise to a separate performance obligation.

(iii) **Determination of the Transaction Price**—The transaction price is the amount of consideration we expect to be entitled from a customer in exchange for providing the subscriptions and services. Variable consideration is included in the transaction price if, in our judgment, it is probable that no significant future reversal of cumulative revenue under the contract will occur.

Some of our end customers are entitled to receive service level commitment credits, in which we may be contractually obligated to provide partial refunds, and in rare instances, each representing a form of variable consideration. We have historically not experienced any significant incidents affecting the defined guarantees of performance levels or service response affecting the defined guarantees of performance levels or service response rates, and accordingly, estimated refunds related to service level commitment credits in the consolidated financial statements were not material during fiscal 2023, 2022 and 2021.

None of our contracts contain a significant financing component. The transaction price excludes amounts collected on behalf of third parties, such as sales taxes.

(iv) **Allocation of the Transaction Price to the Performance Obligations in the Contract**—If the contract contains a single performance obligation, the entire transaction price is allocated to the single performance obligation. Contracts that contain multiple performance obligations require an allocation

of the transaction price to each performance obligation based on relative SSP. Certain arrangements include variable consideration that is typically a function of transaction volume or another usage-based measure. Depending upon the structure of a particular arrangement, we may allocate the variable amount to each distinct service period within the series (i.e. direct allocation).

(v) **Recognition of Revenue when, or as, Performance Obligations are Satisfied**—Revenue is recognized when control of the related performance obligation is transferred to the customer in an amount that reflects the consideration expected to be received in exchange for the subscriptions or services.

We generate substantially all of our revenue from subscriptions to our Singularity Platform. Our Singularity Platform delivers artificial intelligence-powered threat prevention, detection, and response capabilities, enabling an automatic protection against a full spectrum of cyber threats. We built our Singularity Platform to be deployed as a cloud service or in private and hybrid clouds. Customers can extend the functionality of their subscription to our platform by subscribing to additional Singularity Modules. The nature of our promise to the customer under the subscription is to stand ready to provide protection for the duration of the contractual term. As a result, we recognize revenue for these performance obligations ratably over the contractual term. Premium support and maintenance and other Singularity Modules are distinct from subscriptions and are recognized ratably over the term as the performance obligations are satisfied.

Certain arrangements include variable consideration related either to transaction volume or another usage-based measure. Depending upon the structure of a particular arrangement, we (1) recognize revenue as each distinct service period is performed, (2) recognize the estimate of variable consideration ratably over the period to which it relates, or (3) apply the ‘right to invoice’ practical expedient and recognize revenue based on the amount invoiced to the customer during the period.

We generally invoice our customers upfront upon signing for the entire term of the contract, periodically, or in arrears. Most of our subscription contracts have a term of one to three years. Our payment terms typically range between 30 to 45 days. The invoiced amounts are treated as deferred revenue on the consolidated balance sheets and are recognized ratably over the term of the contract beginning on the date the customer is given access to our platform. Our contracts are generally non-cancelable over the contractual term.

Contracts with Multiple Performance Obligations

Our contracts with customers may contain multiple promised services consisting of subscriptions to our Singularity Platform, premium support and maintenance, and other Singularity Modules that are distinct and accounted for separately. The transaction price is allocated to separate performance obligations on a relative SSP basis. Our best evidence for SSP is the price we charge for the subscription or service when we sell it separately in similar circumstances to similar customers. In instances where performance obligations do not have observable standalone sales, we utilize available information that may include, but is not limited to, product groupings or applying the expected cost-plus margin approach to estimate the price we would charge if the service was sold separately.

Cost of Revenue

Cost of revenue consists primarily of third-party cloud infrastructure expenses incurred in connection with the hosting and maintenance of our platform, personnel-related costs associated with our customer support and services organization, including salaries, benefits, bonuses, and stock-based compensation, amortization of intangible assets, amortization of capitalized internal-use software, software and subscription services used by our customer support and services team, and allocated overhead costs.

Research and Development

Research and development costs are expensed as incurred, unless they qualify for recognition as capitalized internal-use software. Research and development expenses consist primarily of personnel-related costs, including

salaries, benefits, bonuses, and stock-based compensation, consulting fees, software and subscription services, third-party cloud infrastructure expenses incurred in developing our platform and modules, and allocated overhead costs.

Advertising Expenses

Advertising costs are expensed as incurred and included in sales and marketing expenses in the consolidated statements of operations. Advertising expenses were $12.3 million, $8.4 million, and $6.2 million for fiscal 2023, 2022 and 2021, respectively.

Stock-Based Compensation

We account for stock-based awards issued to employees, directors, and non-employee consultants based on the fair value of the awards at grant date. The fair value of stock option awards granted and rights to purchase shares under our employee stock purchase plan (ESPP) are generally estimated using the Black-Scholes option pricing model. Stock-based compensation expense for awards with only service-based vesting conditions is recognized on a straight-line basis over the requisite service period of the awards. Forfeitures are accounted for in the period in which they occur.

We granted certain awards that have both service-based vesting conditions and performance-based milestones. We recognize stock-based compensation expense on a graded basis over the total requisite service period for each separately vesting portion of the performance tranches related to these performance milestone options.

We also granted stock option awards with a service-based, performance-based, and market-based vesting conditions to our Chief Executive Officer and Chief Financial Officer. These stock options will vest upon the occurrence of our IPO (the performance-based vesting condition) and the achievement of certain milestone events and our share price targets (the market-based vesting conditions), subject to the executive's continued service to us from the grant date through the milestone events. For these options, we used a Monte Carlo simulation to determine the fair value at the grant date and the implied service period. For these awards, stock-based compensation expense is recognized using the accelerated attribution method over the requisite implied service period when it is probable the performance-based vesting condition will be achieved.

Income Taxes

We are subject to income taxes in the United States and other foreign jurisdictions.

We utilize the asset and liability method of accounting for income taxes whereby deferred tax assets and liabilities are determined based on differences between financial reporting and tax bases of assets and liabilities, as well as from net operating loss carryforwards, and are measured using the enacted tax rates and laws that will be in effect when the differences are expected to reverse.

A valuation allowance is established if, based upon the available evidence, it is more likely than not that some or all of the deferred tax assets will not be realized. We consider all available evidence, both positive and negative, including historical levels of income, expectations, and risks associated with estimates of future taxable income in assessing the need for a valuation allowance.

We recognize income tax benefits from uncertain tax positions only if we believe that it is more likely than not that the tax position will be sustained upon examination by the taxing authorities based on the technical merits of the position. We recognize penalties and accrued interest related to unrecognized tax benefits as income tax expense, in the consolidated statements of operations.

Net Loss per Share Attributable to Common Stockholders

We compute basic and diluted net loss per share attributable to common stockholders using the two-class method required for participating securities. We consider our redeemable convertible preferred stock, restricted common stock, and shares issued upon the early exercise of stock options subject to repurchase to be participating securities. Under the two-class method, net loss is not allocated to redeemable convertible preferred stock, restricted

common stock, and early exercised stock options as the holders do not have a contractual obligation to share in our losses.

Cash, Cash Equivalents, and Restricted Cash

We consider all highly liquid investments purchased with an original maturity of three months or less at the time of purchase to be cash equivalents. Cash equivalents consist of amounts invested in money market funds. Restricted cash consists of the Attivo indemnity escrow fund and collateralized letters of credit established in connection with lease agreements for our office facilities. Restricted cash, current and non-current, are included within prepaid expenses and other current assets and other assets, respectively, on our consolidated balance sheets.

The following table provides a reconciliation of cash, cash equivalents, and restricted cash to the total of these amounts shown in the consolidated statements of cash flows (in thousands):

	As of January 31,	
	2023	2022
Cash and cash equivalents	$ 137,941	$ 1,669,304
Restricted cash, current	61,264	—
Restricted cash, non-current	3,201	2,747
	$ 202,406	$ 1,672,051

Investments

We determine the appropriate classification of our investments at the time of purchase and reevaluate such determination at each balance sheet date. Investments not considered cash equivalents, and with maturities of one year or less from the consolidated balance sheet date, are classified as short-term investments. Investments with maturities greater than one year from the consolidated balance sheet date are classified as long-term investments. We classify our investments as available-for-sale securities and present them within assets. Our investments are recorded at fair value with unrealized gains and losses, if any, reported in accumulated other comprehensive income (loss). When evaluating whether an investment's unrealized losses are related to credit factors, we review factors such as the extent to which fair value is below its cost basis, any changes to the credit rating of the security, adverse conditions specifically related to the security, changes in market interest rates and our intent to sell, or whether it is more likely than not we will be required to sell, before recovery of cost basis. We invest in highly rated securities with a weighted average maturity of 18 months or less. In addition, our investment policy limits the amount of our credit exposure to any one issuer and requires investments to be investment grade, with the primary objective of preserving capital and maintaining liquidity. Fair values were determined for each individual security in the investment portfolio.

We did not identify any credit losses on investments as of January 31, 2023 and 2022. Realized gains and losses on the sale of investments are determined on a specific identification method and are recorded in other income (expense), net in the consolidated statements of operations. There were no realized gains or losses on the sale of investments during fiscal 2023, 2022 and 2021.

Strategic Investments

Our strategic investments consist of non-marketable equity and debt investments in privately held companies. We elect to apply the measurement alternative and record non-marketable equity investments at cost, less any impairment, plus or minus observable price changes in orderly transactions for identical or similar investments of the same issuer. Non-marketable debt securities are classified as available-for-sale and are recorded at their estimated fair value with changes in fair value recorded through accumulated other comprehensive income (loss).

Strategic investments are included within long-term investments on our consolidated balance sheets and adjustments to their carrying amounts are recorded in other income (expense), net in the consolidated statements of

operations. There were no material events or circumstances impacting the carrying amount of our strategic investments during fiscal 2023, 2022 and 2021.

Fair Value of Financial Instruments

Fair value is defined as the exchange price that would be received for an asset or an exit price paid to transfer a liability in the principal or most advantageous market for the asset or liability in an orderly transaction between market participants on the measurement date. The carrying amounts reported on the consolidated balance sheets for accounts receivable, accounts payable, accrued liabilities, and accrued payroll and benefits approximate their respective fair values due to their short-term nature.

Concentrations of Credit Risk

Financial instruments that potentially subject us to concentrations of credit risk consist primarily of cash and cash equivalents, restricted cash, investments, and accounts receivable. We maintain our cash, cash equivalents, restricted cash, and investments with high-credit-quality financial institutions mainly in the U.S. and Israel. We have not experienced any credit losses relating to our cash, cash equivalents, restricted cash, and investments. For accounts receivable, we are exposed to credit risk in the event of nonpayment by customers to the extent of the amounts recorded on the consolidated balance sheets. We perform periodic credit evaluations of our customers and generally do not require collateral.

The only channel partner that represented 10% or more of accounts receivable, net for the periods presented was as follows:

	As of January 31,	
	2023	2022
Channel partner A	20 %	18 %

There were no end customers that represented 10% or more of accounts receivable as of January 31, 2023 or 2022.

Channel partners that represented 10% or more of our total revenue for the periods presented were as follows:

	Year Ended January 31,		
	2023	2022	2021
Channel partner A	18 %	18 %	19 %
Channel partner B	*	*	13 %

*Less than 10%

There were no end customers that represented 10% or more of total revenue for fiscal 2023, 2022 and 2021.

Accounts Receivable

Accounts receivable are recorded at invoiced amounts and are non-interest bearing. We have a well-established collection history from our channel partners and end customers. We periodically evaluate the collectability of our accounts receivable and provide an allowance for doubtful accounts as necessary, based on the age of the receivable, expected payment ability, and collection experience. The allowance for doubtful accounts balance was $0.8 million and $0.3 million as of January 31, 2023 and 2022, respectively.

Deferred Contract Acquisition Costs

We capitalize sales commissions and associated payroll taxes that are incremental to obtaining a customer contract, which are recorded as deferred contract acquisition costs on the consolidated balance sheets. Sales

commissions for the renewal of a contract are not considered commensurate with commissions paid for the initial contracts, given the substantive difference in commission rates in proportion to their respective contract values. Commissions paid on a new contract are amortized on a straight-line basis over an estimated period of benefit of four years, while commissions paid on renewal contracts are amortized over the average contractual term of the renewal. We determine the estimated period of benefit based on both quantitative and qualitative factors, including the duration of our relationships with customers and the estimated useful life of our technology. Amortization of deferred contract acquisition costs is included in sales and marketing expenses in the consolidated statements of operations.

We periodically review these deferred contract acquisition costs to determine whether events or changes in circumstances have occurred that could impact the period of benefit. We did not recognize any impairment of deferred contract acquisition costs during fiscal 2023, 2022 and 2021.

Property and Equipment

Property and equipment are stated at cost, net of accumulated depreciation and amortization. Depreciation and amortization are calculated using the straight-line method over the estimated useful lives of the assets as follows:

	Estimated Useful Life
Office furniture and equipment	5 years
Computers, software, and electronic equipment	3 years
Capitalized internal-use software	4 years
Leasehold improvements	Shorter of useful life or remaining term of lease

Costs for maintenance and repairs are expensed as incurred.

Capitalized Internal-Use Software

We capitalize certain internal-use software development costs related to our cloud platform. Costs incurred in the preliminary stages of development and post-development are expensed as incurred. Internal and external costs incurred during the development phase, if direct, are capitalized until the software is substantially complete and ready for our intended use. We also capitalize costs related to specific upgrades and enhancements when it is probable the expenditures will result in additional functionality. Maintenance and training costs are expensed as incurred. Capitalized internal-use software is included in property and equipment and is amortized to cost of revenue on a straight-line basis over its expected useful life.

Impairment of Long-Lived Assets (Including Goodwill and Intangible Assets)

Long-lived assets, including intangible assets with finite lives, are reviewed for impairment when events or changes in circumstances indicate that the carrying amount of assets may not be recoverable. Recoverability of assets is measured by a comparison of the carrying amount of an asset to the future undiscounted cash flows expected to be generated by the asset. If such assets are considered to be impaired, the impairment to be recognized is measured by the amount by which the carrying amount of the assets exceeds the fair value of the asset group. No impairment loss was recorded during fiscal 2023, 2022 and 2021.

Goodwill is not amortized but tested for impairment at least annually in the fourth quarter, or more frequently if events or changes in circumstances indicate that impairment may exist. The impairment test consists of a qualitative assessment to determine if the quantitative assessment is required. Goodwill impairment is recognized when the quantitative assessment results in the carrying value of the reporting unit exceeding its fair value, net of related income tax effect, in which case an impairment charge is recorded to goodwill to the extent the carrying value exceeds the fair value, limited to the amount of goodwill. We did not recognize any impairment of goodwill during fiscal 2023 and 2022.

Business Combinations

We account for our acquisitions using the acquisition method of accounting. We allocate the fair value of purchase consideration to the tangible and intangible assets acquired, and liabilities assumed, based on their estimated fair values. The excess of the fair value of purchase consideration over the values of these identifiable assets and liabilities is recorded as goodwill. When determining the fair value of assets acquired and liabilities assumed, management makes significant estimates and assumptions, especially with respect to intangible assets. Significant estimates in valuing certain identifiable assets include, but are not limited to, the selection of valuation methodologies, forecasted revenue, discount rates, and useful lives. Management's estimates of fair value are based upon assumptions believed to be reasonable, but which are inherently uncertain and unpredictable and, as a result, actual results may differ from estimates. Acquisition costs, such as legal and consulting fees, are expensed as incurred and are included in general and administrative expenses in the consolidated statements of operations. During the measurement period, which is up to one year from the acquisition date, we may record adjustments to the assets acquired and liabilities assumed, with the corresponding offset to goodwill. Upon the conclusion of the measurement period, any subsequent adjustments are recorded in the consolidated statements of operations. See Note 15 for additional information regarding our acquisitions.

Leases

In accordance with ASC 842, we determine if an arrangement is or contains a lease at inception by evaluating various factors, including if the contract conveys the right to control the use of an identified asset for a period of time in exchange for consideration and other facts and circumstances. Operating lease right-of-use (ROU) assets and operating lease liabilities are recognized on the consolidated balance sheets at the lease commencement date based on the present value of lease payments over the lease term, which is the non-cancelable period stated in the contract adjusted for any options to extend or terminate the lease when it is reasonably certain that we will exercise that option.

Lease payments consist of the fixed payments under the arrangement, less any lease incentives, such as tenant improvement allowances. Variable costs, such as maintenance and utilities based on actual usage, are not included in the measurement of operating lease ROU assets and operating lease liabilities and are expensed when the event determining the amount of variable consideration to be paid occurs. When the implicit rate of the leases is not determinable, we use an IBR based on the information available at the lease commencement date in determining the present value of lease payments. Lease cost for lease payments is recognized on a straight-line basis over the lease term.

We account for lease components and non-lease components as a single lease component. In addition, we do not recognize operating lease ROU assets and operating lease liabilities for leases with lease terms of 12 months or less.

In addition, we sublease certain of our unoccupied facilities to third parties. We recognize sublease income on a straight-line basis over the sublease term.

We did not have any material finance leases during fiscal 2023, 2022 and 2021.

Recently Adopted Accounting Pronouncements

In October 2021, the Financial Accounting Standards Board (FASB) issued Accounting Standards Update (ASU) No. 2021-08, Business Combinations (Topic 805): Accounting for Contract Assets and Contract Liabilities from Contracts with Customers. The new guidance requires contract assets and contract liabilities (i.e., deferred revenue) acquired in a business combination to be recognized in accordance with Accounting Standards Codification Topic 606 as if the acquirer had originated the contracts. Previously, contract assets and contract liabilities were measured at fair value. The standard is effective for fiscal years beginning after December 15, 2022, including interim periods within those fiscal years, and early adoption is permitted. We early adopted this guidance on February 1, 2022, which did not have a material impact at the time of adoption on our consolidated financial statements.

3. REVENUE AND CONTRACT BALANCES

Disaggregation of Revenue

The following table summarizes revenue by geography based on the shipping address of end customers who have contracted to use our platform for the periods presented (in thousands, except percentages):

	Year Ended January 31,					
	2023		2022		2021	
	Amount	% of Revenue	Amount	% of Revenue	Amount	% of Revenue
United States	$ 276,443	65 %	$ 140,034	68 %	$ 65,497	70 %
International	145,736	35	64,765	32	27,559	30
Total	$ 422,179	100 %	$ 204,799	100 %	$ 93,056	100 %

No single country other than the United States represented 10% or more of our revenue during fiscal 2023, 2022 and 2021.

The following table summarizes revenue from contracts by type of customer for the periods presented (in thousands, except percentages):

	Year Ended January 31,					
	2023		2022		2021	
	Amount	% of Revenue	Amount	% of Revenue	Amount	% of Revenue
Channel partners	$ 380,857	90 %	$ 187,541	92 %	$ 88,954	96 %
Direct customers	41,322	10	17,258	8	4,102	4
Total	$ 422,179	100 %	$ 204,799	100 %	$ 93,056	100 %

Contract Balances

Contract assets consist of unbilled accounts receivable, which arise when a right to consideration for our performance under the customer contract occurs before invoicing the customer. The amount of unbilled accounts receivable included within accounts receivable, net on the consolidated balance sheets was $1.5 million as of both January 31, 2023 and 2022.

Contract liabilities consist of deferred revenue, which represents invoices billed in advance of performance under a contract. Deferred revenue is recognized as revenue over the contractual period. The deferred revenue balance was $406.3 million and $262.0 million as of January 31, 2023 and 2022, respectively. We recognized revenue of $195.9 million, $95.5 million and $53.8 million for fiscal 2023, 2022 and 2021, respectively, that was included in the corresponding contract liability balance at the beginning of the period.

Remaining Performance Obligations

Our contracts with customers typically range from one to three years. Revenue allocated to remaining performance obligations represents non-cancelable contract revenue that has not yet been recognized, which includes deferred revenue and amounts that will be invoiced in future periods.

As of January 31, 2023, our remaining performance obligations were $609.4 million, of which we expect to recognize 85% as revenue over the next 24 months, with the remainder to be recognized thereafter.

Capitalized contract costs were $93.4 million and $68.6 million as of January 31, 2023 and 2022, respectively. Amortization expense of contract costs was $36.4 million, $21.7 million, and $11.5 million for fiscal 2023, 2022 and 2021 respectively. We periodically review deferred contract acquisition costs to determine whether events or changes in circumstances have occurred that could impact the period of benefit. We did not recognize any impairment of deferred contract acquisition costs during fiscal 2023, 2022 and 2021.

4. FAIR VALUE MEASUREMENTS

We measure fair value based on a three-level hierarchy, maximizing the use of observable inputs, where available, and minimizing the use of unobservable inputs, as follows:

Level 1: Assets and liabilities whose values are based on observable inputs such as quoted (unadjusted) prices in active markets for identical assets or liabilities.

Level 2: Assets and liabilities whose values are based on inputs from quoted prices for similar assets and liabilities in active markets or inputs that are observable for the asset or liability, either directly or indirectly through market corroboration, for substantially the full term of the asset or liability.

Level 3: Assets and liabilities whose values are based on unobservable inputs that are supported by little or no market activity and that are significant to the overall fair value measurement.

The following table summarizes information about our cash, cash equivalents, and investments by investment category (in thousands):

	As of January 31, 2023				
	Fair Value Level	Amortized Cost	Gross Unrealized Gains	Gross Unrealized Losses	Estimated Fair Value
Assets					
Cash and cash equivalents:					
Cash		$ 35,055	$ —	$ —	$ 35,055
Money market funds	Level 1	102,886	—	—	102,886
Total cash and cash equivalents		$ 137,941	$ —	$ —	$ 137,941
Short-term investments:					
U.S. Treasury securities	Level 1	$ 144,392	$ 1	$ (501)	$ 143,892
Commercial paper	Level 2	230,305	30	(667)	229,668
Corporate notes and bonds	Level 2	38,443	15	(148)	38,310
U.S. agency securities	Level 2	74,060	3	(349)	73,714
Total short-term investments		$ 487,200	$ 49	$ (1,665)	$ 485,584
Long-term investments:					
U.S. Treasury securities	Level 1	$ 192,337	$ —	$ (2,460)	$ 189,877
Corporate notes and bonds	Level 2	233,946	178	(2,029)	232,095
U.S. agency securities	Level 2	101,844	27	(921)	100,950
Total long-term investments		$ 528,127	$ 205	$ (5,410)	$ 522,922
Total assets measured at fair value		$ 1,153,268	$ 254	$ (7,075)	$ 1,146,447

The table above does not include the Company's strategic investments in non-marketable debt and equity securities, which are classified as level 3 investments and were $12.5 million as of January 31, 2023.

The following table summarizes the respective fair value and the classification by level within the fair value hierarchy (in thousands):

	As of January 31, 2022			
	Level 1	Level 2	Level 3	Total
Assets				
Cash equivalents:				
Money market funds	$ 1,641,642	$ —	$ —	$ 1,641,642
Short-term investments:				
Certificates of deposit	—	374	—	374
Total assets measured and recorded at fair value	$ 1,641,642	$ 374	$ —	$ 1,642,016

We invest in highly rated securities with a weighted average maturity of 18 months or less. As of January 31, 2023, all of our investments will mature within 2 years.

There were no transfers between the levels of the fair value hierarchy during fiscal 2023, 2022 and 2021.

As of January 31, 2023, we determined that the declines in the market value of our investment portfolio were not driven by credit related factors. During the years ended January 31, 2023 and 2022, we did not recognize any

losses on our investments due to credit related factors. As of January 31, 2023, no unrealized losses were in a continuous unrealized loss position for more than twelve months.

5. PROPERTY AND EQUIPMENT, NET

Property and equipment, net consisted of the following (in thousands):

	As of January 31,	
	2023	2022
Office furniture and fixtures	$ 2,110	$ 1,318
Computers, software, and equipment	4,603	4,895
Capitalized internal-use software	34,753	17,917
Leasehold improvements	13,188	7,490
Construction in progress	3	3,108
Total property and equipment	54,657	34,728
Less: Accumulated depreciation and amortization	(15,916)	(9,810)
Total property and equipment, net	$ 38,741	$ 24,918

We capitalized internal-use software costs of $17.5 million, $10.6 million and $2.8 million during fiscal 2023, 2022 and 2021, respectively.

Depreciation and amortization expense related to property and equipment was $6.7 million, $4.6 million and $2.8 million for fiscal 2023, 2022 and 2021, respectively, including amortization expense related to capitalized internal-use software of $4.1 million, $2.1 million and $1.3 million for fiscal 2023, 2022 and 2021, respectively.

6. INTANGIBLE ASSETS

Intangible assets, net as of January 31, 2023 consisted of the following (in thousands):

	As of January 31,	
	2023	2022
Developed technology	78,700	15,500
Customer relationship	79,100	1,500
Backlog	11,100	—
Non-compete agreements	650	650
Trademarks	150	150
Patents	1,501	1,094
Total finite-lived intangible assets	171,201	18,894
Less: accumulated amortization	(26,363)	(3,342)
Total finite-lived intangible assets, net	144,838	15,552
Indefinite-lived intangible assets - domain names	255	255
Total intangible assets, net	145,093	15,807

Amortization expense of intangible assets was $23.0 million and $3.3 million for fiscal 2023 and 2022, respectively. Amortization expense of intangible assets was not material for fiscal 2021.

As of January 31, 2023, estimated future amortization expense is as follows (in thousands):

Fiscal Year Ending January 31,	
2024	28,605
2025	24,206
2026	22,773
2027	22,773
2028	13,215
Thereafter	33,266
Total	$ 144,838

7. LEASES

We have entered into non-cancelable real estate operating lease agreements with various expiration dates through fiscal 2029. Our operating lease arrangements do not contain any restrictive covenants or residual value guarantees.

Supplemental cash flow information related to our operating leases for fiscal 2023 and 2022 as well as the weighted-average remaining lease term and weighted-average discount rate as of January 31, 2023 and 2022 were as follows:

	Year Ended January 31,		
	2023	2022	2021
Supplemental Cash Flow Information			
Cash paid for amount included in the measurement of operating lease liabilities	$ 5,266	$ 4,596	$ 3,999
Operating lease ROU assets obtained in exchange for operating lease liabilities	$ 3,224	$ 8,558	$ 6,579

	As of January 31,	
	2023	2022
Lease Term and Discount Rate		
Weighted-average remaining lease term (years)	5.55	6.56
Weighted-average discount rate	4.2 %	4.3 %

The components of lease costs, net of sublease income, consisted of the following (in thousands):

	Year Ended January 31,		
	2023	2022	2021
Operating lease costs	$ 4,905	$ 4,027	$ 3,844
Short-term lease costs	771	2,248	509
Variable lease costs	1,186	1,124	702
Total lease costs	$ 6,862	$ 7,399	$ 5,055

Sublease income was $0.7 million, $0.6 million and $0.9 million for fiscal 2023, 2022 and 2021, respectively, and was recorded as a reduction of lease costs.

The maturities of our non-cancelable operating lease liabilities as of January 31, 2023 were as follows (in thousands):

Fiscal Year Ending January 31,	Amount
2024	$ 4,805
2025	5,733
2026	5,580
2027	5,640
2028	5,702
Thereafter	2,916
Total operating lease payments	$ 30,376
Less: Imputed interest	(3,402)
Present value of operating lease liabilities	$ 26,974

8. COMMON STOCK

We have two classes of common stock: Class A common stock and Class B common stock. In connection with the IPO, we amended and restated our certificate of incorporation and authorized 1,500,000,000 shares of Class A common stock and 300,000,000 shares of Class B common stock. The shares of Class A common stock and Class B common stock are identical, except with respect to voting rights. Each share of Class A common stock is entitled to one vote. Each share of Class B common stock is entitled to twenty votes. Class A and Class B common stock each have a par value of $0.0001 per share, and are referred to collectively as our common stock throughout the notes to the consolidated financial statements, unless otherwise noted. Holders of common stock are entitled to receive any dividends as may be declared from time to time by the board of directors.

Shares of Class B common stock may be converted to Class A common stock at any time at the option of the stockholder. Shares of Class B common stock automatically convert to Class A common stock at the earlier of: (i) the date specified by a vote of the holders of 66 2/3% of the then outstanding shares of Class B common stock, (ii) seven years from the date of our Final Prospectus, or June 29, 2028, (iii) the first date following the completion of our IPO on which the number of shares of outstanding Class B common stock (such calculations shall include shares of Class B common stock subject to outstanding stock options) held by Tomer Weingarten, including certain permitted entities that Mr. Weingarten controls, is less than 25% of the number of shares of outstanding Class B common stock (such calculation shall include shares of Class B common stock subject to outstanding stock options) that Mr. Weingarten originally held as of the date of our Final Prospectus, (iv) the date fixed by our board of directors, following the first date following the completion of our IPO when Mr. Weingarten is no longer providing services to us as an officer, employee, consultant or member of our board of directors, (v) the date fixed by our board of directors following the date on which, if applicable, Mr. Weingarten is terminated for cause, as defined in our restated certificate of incorporation, and (vi) the date that is 12 months after the death or disability, as defined in our restated certificate of incorporation, of Mr. Weingarten.

Our common stock reserved for future issuance on an as-converted basis as of January 31, 2023 and 2022 were as follows:

	As of January 31,	
	2023	2022
Stock options outstanding	32,446,814	42,422,473
RSUs and PSUs outstanding	14,409,166	1,770,304
ESPP reserved for future issuance	8,043,936	6,674,603
2021 Plan available for future grants	40,175,515	38,055,572
Total shares of common stock reserved	95,075,431	88,922,952

9. STOCK-BASED COMPENSATION

2021 Equity Incentive Plan

In May 2021, our board of directors and in June 2021, our stockholders approved our 2021 Equity Incentive Plan (2021 Plan) as a successor to our 2013 Equity Incentive Plan (2013 Plan) and 2011 Stock Incentive Plan (2011 Plan) with the purpose of granting stock-based awards to employees, directors, officers and consultants, including stock options, restricted stock awards, restricted stock units (RSUs), and performance-based restricted stock units (PSUs). A total of 35,281,596 shares of Class A common stock were initially available for issuance under the 2021 Plan. Our compensation committee administers the 2021 Plan. The number of shares of our Class A common stock available for issuance under the 2021 Plan is subject to an annual increase on the first day of each fiscal year beginning on February 1, 2022, equal to the lesser of: (i) five percent (5%) of the aggregate number of outstanding shares of all classes of our common stock as of the last day of the immediately preceding fiscal year or (ii) such other amount as our board of directors may determine.

The 2013 Plan and 2011 Plan (together, the Prior Plans) were terminated in June 2021, in connection with the adoption of our 2021 Plan, and stock-based awards are no longer granted under the Prior Plans. However, the Prior Plans will continue to govern the terms and conditions of the outstanding awards previously granted thereunder. Any shares underlying stock options that are expired, canceled, forfeited or repurchased under the Prior Plans will be automatically transferred to the 2021 Plan and be available for issuance as Class A common stock.

Restricted Stock Units

A summary of our RSU activity is as follows:

	Number of Shares	Weighted-Average Grant Date Fair Value
Outstanding as of January 31, 2022	1,770,304	$ 52.51
Granted	14,992,931	26.28
Released	(1,303,854)	41.96
Forfeited	(1,050,215)	36.19
Outstanding as of January 31, 2023	14,409,166	$ 27.37

As of January 31, 2023, we had unrecognized stock-based compensation expense related to unvested RSUs of $353.3 million that is expected to be recognized on a straight-line basis over a weighted-average period of 3.37 years.

Stock Option Information

A summary of our stock option activity is as follows:

	Number of Options	Weighted-Average Exercise Price	Weighted-Average Remaining Contractual Term (in years)	Aggregate Intrinsic Value (in thousands)
Outstanding as of January 31, 2022	42,422,473	$ 4.30	6.50	$ 1,714,821
Granted	—	—		
Exercised	(7,650,525)	2.26		
Forfeited	(2,703,962)	4.68		
Assumed options from Attivo acquisition	378,828	1.31		
Outstanding as of January 31, 2023	32,446,814	$ 4.71	6.52	$ 337,214
Expected to vest as of January 31, 2023	32,446,814	$ 4.71	6.52	$ 337,214
Vested and exercisable as of January 31, 2023	19,645,571	$ 3.54	5.97	$ 227,200

The weighted-average grant-date fair value of options granted during fiscal 2022 and 2021 were $13.14 and $1.63 per share, respectively. There were no options granted during fiscal 2023.

The aggregate grant-date fair value of options vested during fiscal 2023, 2022 and 2021 was $61.4 million, $32.0 million and $5.1 million, respectively.

The aggregate intrinsic value is the difference between the exercise price and the estimated fair value of the underlying common stock. The aggregate intrinsic value of options exercised during fiscal 2023, 2022 and 2021 was $173.0 million, $333.7 million and $27.0 million, respectively.

As of January 31, 2023, we had unrecognized stock-based compensation expense related to unvested options of $104.3 million that is expected to be recognized on a straight-line basis over a weighted-average period of 2.14 years.

Milestone Options

In March 2021, we granted 1,404,605 options to purchase shares of common stock subject to service-based, performance-based, and market-based vesting conditions to our Chief Executive Officer and Chief Financial Officer under the 2013 Plan. These stock options will vest 100% upon the occurrence of our IPO (the performance-based vesting condition), which was completed in June 2021, and the achievement of certain share price targets (the market-based vesting conditions), subject to the executive's continued service to us from the grant date through the milestone events. As of January 31, 2023, the share price targets have not yet been achieved, and therefore, these milestone options remain unvested. For these options, we used a Monte Carlo simulation to determine the fair value at the grant date and the implied service period.

We recorded stock-based compensation expense related to these milestone options of $3.6 million and $3.1 million during fiscal 2023 and 2022, respectively. As of January 31, 2023, we had unrecognized stock-based compensation expense related to unvested milestone options of $12.7 million, that is expected to be recognized over the remaining implied service period of 3.6 years.

Performance Share Units

In connection with the acquisition of Attivo, we granted 71,003 shares of performance share units subject to service-based and performance-based vesting conditions. These PSUs will vest 100% upon the achievement of certain financial performance and integration milestone events, subject to the employees' continued service to us from the grant date through the milestone events or target dates.

We recorded stock-based compensation expense related to these PSUs of $0.5 million during fiscal 2023. As of January 31, 2023, we had unrecognized stock-based compensation expense related to these PSUs of $0.5 million that is expected to be recognized over the remaining vesting period of 2.3 years.

Restricted Common Stock

In connection with the Attivo acquisition, restricted common stock was issued to Attivo employees. See Note 15, *Acquisitions*, for more information regarding these restricted common stock. We recorded stock-based compensation expense related to restricted common stock in connection with our acquisition of Attivo of $1.0 million during fiscal 2023. As of January 31, 2023, we had unrecognized stock-based compensation expense related to this unvested restricted common stock of $1.0 million.

In connection with the Scalyr acquisition, we granted 1,315,099 shares of restricted common stock with a fair value of $14.59 per share at the time of grant, that vest over a period of two years. We recorded stock-based compensation expense related to restricted common stock in connection with our acquisition of Scalyr of $8.5 million and $10.9 million during fiscal 2023 and 2022, respectively. As of January 31, 2023, we had unrecognized stock-based compensation expense related to this unvested restricted common stock of $0.2 million that is expected to be recognized by the end of February 2023.

Employee Stock Purchase Plan (ESPP)

In May 2021, our board of directors, and in June 2021, our stockholders approved our ESPP, which became effective on the date of effectiveness of our Final Prospectus, or June 29, 2021. The ESPP initially reserved and authorized the issuance of up to a total of 7,056,319 shares of common stock to eligible employees. The number of shares reserved for issuance and sale under the ESPP will automatically increase on the first day of each fiscal year, starting on February 1, 2022 for the first ten calendar years after the first offering date, in an amount equal to (i) 1% of the aggregate number of outstanding shares of all class our common stock on the last day of the immediately preceding fiscal year, or (ii) such other amount as the administrator of the ESPP may determine. The ESPP generally provides for six-month offering periods beginning January 6 and July 6 of each year, with each offering period consisting of single six-month purchase periods, except for the initial offering period which began on July 1, 2021, and will end on July 5, 2023 and the second offering period will begin on January 6, 2022. On each purchase date, eligible employees will purchase the shares at a price per share equal to 85% of the lesser of (1) the fair market value of our common stock as of the beginning of the offering period or (2) the fair market value of our common stock on the purchase date, as defined in the ESPP except for the initial offering period that has a 24-months look back to the IPO price of $35.

The following table summarizes assumptions used in estimating the fair value of employee stock purchase rights for the initial and subsequent offering periods under the 2021 ESPP using the Black-Scholes option pricing model:

	Year Ended January 31,	
	2023	2022
Expected term (in years)	0.5 - 1.0	0.5 - 2.0
Expected volatility	71.5% - 95.8%	52.3% - 70.5%
Risk-free interest rate	2.6% - 4.8%	0.1% - 0.3%
Dividend yield	— %	— %

We recognized stock-based compensation expense related to ESPP of $12.7 million and $5.5 million during fiscal 2023 and 2022, respectively. As of January 31, 2023, $1.5 million amount has been withheld on behalf of employees for a future purchase under the ESPP due to the timing of payroll deductions.

1,335,183 and 381,716 shares were issued under the ESPP for $19.2 million and $11.4 million during fiscal 2023 and 2022, respectively.

During fiscal 2023, we recorded $0.4 million in expense related to modifications of our ESPP as a result of the decrease in our stock price in July 2022 and January 2023 which triggered resets of the ESPP offering periods in accordance with our plan. We expect to record the remaining $0.4 million in expense related to these modifications through the second quarter of 2024.

Attivo Acquisition

In connection with the Acquisition, we granted 539,795 shares of restricted stock units (RSUs) under our 2021 Equity Incentive Plan that will vest over a period of 3 years contingent on continued employment of certain Attivo employees, for which stock-based compensation expense will be recognized ratably over the vesting period.

Attivo Equity Incentive Plan

In connection with the Acquisition, we assumed unvested stock options that were granted under the Attivo 2011 Equity Incentive Plan ("Attivo Plan"). We do not intend to grant any additional shares under the Attivo Plan and the Attivo Plan will continue to govern the terms and conditions of the outstanding awards previously granted thereunder. Any shares underlying stock options that are expired, canceled, forfeited or repurchased under the Attivo Plan will be automatically become available for issuance as Class A common stock pursuant to our 2021 Equity Incentive Plan.

Modification

During the third quarter of fiscal 2023, certain members of our management team converted to non-employee consultants. The transition has been accounted for as a modification, under which, the exercise period of certain vested awards has been extended and a certain number of unvested awards will vest through the end of the consulting agreements.

During fiscal 2023, we recognized an incremental charge of $4.5 million related to the transition of these employees to non-employee consultants and expect to recognize an aggregate of an additional $6.2 million in expense over the requisite service period through the fourth quarter of 2024.

Stock-Based Compensation Expense

We estimate the fair value of stock options granted using the Black-Scholes option pricing model based on the following assumptions:

Expected term – We determine expected term based on the average period the options are expected to remain outstanding using the simplified method, calculated as the midpoint of the options' vesting term and contractual expiration period, until sufficient historical information to develop reasonable expectations about future exercise patterns and post-vesting employment termination behavior becomes available.

Expected volatility – Since there is little trading history of our common stock, expected volatility is estimated based on the historical volatilities of a group of comparable publicly traded companies.

Risk-free interest rate – The risk-free interest rate is based on U.S. Treasury yields for a period that corresponds with the expected term of the award.

Dividend yield – As we do not currently issue dividends and do not expect to issue dividends on our common stock in the foreseeable future, the expected dividend yield is zero.

Fair value of underlying common stock – Prior to the completion of our IPO, the fair value of our common stock was determined by the board of directors by considering a number of objective and subjective factors including input from management and contemporaneous third-party valuations. After the completion of our IPO, the fair value of our Class A common stock is determined by the closing price of our Class A common stock, which is traded on the New York Stock Exchange.

The following table summarizes assumptions used in estimating the fair value of stock options granted under the Black-Scholes pricing model in fiscal 2022 (no stock options were granted in fiscal 2023):

	Year Ended January 31,
	2022
Expected term (in years)	6.0
Expected volatility	62.3% - 66.0%
Risk-free interest rate	0.8% - 1.1%
Dividend yield	— %

The components of stock-based compensation expense recognized in the consolidated statements of operations consisted of the following (in thousands):

	Year Ended January 31,	
	2023	2022
Cost of revenue	$ 10,093	$ 3,618
Research and development	51,771	35,358
Sales and marketing	40,115	15,460
General and administrative	62,487	33,453
Total	$ 164,466	$ 87,889

10. INCOME TAXES

Our loss before provision for income taxes for fiscal 2023, 2022 and 2021 consisted of the following (in thousands):

	Year Ended January 31,		
	2023	2022	2021
Domestic	$ (432,235)	$ (274,270)	$ (18,159)
Foreign	47,944	4,173	(98,954)
Loss before provision for income taxes	$ (384,291)	$ (270,097)	$ (117,113)

The components of provision for income taxes for fiscal 2023, 2022 and 2021 consisted of the following (in thousands):

	Year Ended January 31,		
	2023	2022	2021
Current:			
State	$ 53	$ 82	$ 62
Foreign	3,661	1,011	398
Total current	3,714	1,093	460
Deferred:			
Federal	(6,754)	—	—
State	(2,913)	—	—
Foreign	340	(89)	—
Total deferred	(9,327)	(89)	—
Total provision for income taxes	$ (5,613)	$ 1,004	$ 460

A reconciliation of the expected provision for (benefit from) income taxes at the statutory federal income tax rate to our recorded provision for income taxes consisted of the following (in thousands):

	Year Ended January 31,		
	2023	2022	2021
Benefit from income taxes at U.S. federal statutory rate	$ (80,701)	$ (56,720)	$ (24,594)
State taxes, net of federal benefit	53	82	49
Foreign tax rate differential	10,140	(1,297)	(1,836)
Stock-based compensation	2,734	(23,442)	1,195
Non-deductible expenses	1,780	322	84
Change in valuation allowance	60,145	81,739	25,564
Other	236	320	(2)
Total provision for (benefit from) income taxes	$ (5,613)	$ 1,004	$ 460

Significant components of our net deferred tax assets and liabilities as of January 31, 2023 and 2022 consisted of the following (in thousands):

	As of January 31,	
	2023	2022
Deferred tax assets:		
Net operating loss carryforwards	$ 228,400	$ 174,646
Research and development expenses	72,432	36,989
Deferred revenue	25,643	14,748
Accruals and reserves	6,215	3,960
Operating lease liabilities	9,139	11,158
Stock-based compensation	17,528	7,936
Other	2,622	2,012
Gross deferred tax assets	361,979	251,449
Valuation allowance	(291,751)	(218,981)
Total deferred tax assets	70,228	32,468
Deferred tax liabilities:		
Acquired intangibles, property and equipment	(37,170)	(6,235)
Deferred contract acquisition costs	(22,868)	(16,722)
Operating lease right-of-use assets	(8,162)	(9,422)
Other	(2,279)	—
Total deferred tax liabilities	(70,479)	(32,379)
Net deferred tax assets (liabilities)	$ (251)	$ 89

Based upon available objective evidence, we believe it is more likely than not that the net U.S. and Israel deferred tax assets will not be fully realizable. Accordingly, we have established a valuation allowance for the U.S. and Israel gross deferred tax assets. As of January 31, 2023 and 2022, we had a valuation allowance of $291.8 million and $219.0 million, respectively, against our deferred tax assets. During fiscal 2023 and 2022, total valuation allowance increased by $72.8 million and $132.9 million, respectively, primarily due to additional net operating losses.

As of January 31, 2023, we had federal net operating loss carryforwards of $651.1 million, which will begin to expire in 2031, and state net operating loss carryforwards of $338.3 million, which will begin to expire in 2024. We also had foreign net operating loss carryforwards of $289.8 million, which do not expire.

In addition, we had federal research and development credit carryforwards of $2.0 million, which will begin to expire in 2037, and state research and development credit carryforwards of $2.0 million, which do not expire.

Federal and state tax laws impose substantial restrictions on the utilization of the net operating loss carryforwards and tax credit carryforwards in the event of an ownership change as defined in Section 382 of the Internal Revenue Code of 1986, as amended. Accordingly, our ability to utilize these carryforwards may be limited as a result of such ownership change. Such a limitation could result in the expiration of carryforwards before they are utilized. The carryforwards are currently subject to a valuation allowance.

Foreign withholding taxes have not been provided for the cumulative undistributed earnings of certain foreign subsidiaries of us as of January 31, 2023 and 2022 due to our intention to permanently reinvest such earnings. Determination of the amount of unrecognized deferred tax liability related to these earnings is not practicable.

We file income tax returns in the U.S. federal jurisdiction and various state and foreign jurisdictions. Our tax years generally remain open and subject to examination by federal, state, or foreign tax authorities. We are currently

under examination by the Israel Tax Authorities for the 2017 through 2021 tax years. We are not currently under audit in any other tax jurisdictions.

The changes in the gross amount of unrecognized tax benefits consisted of the following (in thousands):

	As of January 31,		
	2023	2022	2021
Balance at beginning of year	$ 566	$ 534	$ 358
Gross increases for tax positions of current year	447	32	176
Balance at end of year	$ 1,013	$ 566	$ 534

We recognize interests and penalties related to income tax matters as a component of income tax expense. No accrued interest of penalties have been recorded as of January 31, 2023, 2022, and 2021. We do not anticipate that its total unrecognized tax benefits will significantly change during the next 12 months.

11. NET LOSS PER SHARE ATTRIBUTABLE TO COMMON STOCKHOLDERS

Basic and diluted net loss per share attributable to common stockholders is computed in conformity with the two-class method required for participating securities. Basic net loss per share is computed by dividing net loss attributable to common stockholders by the weighted-average number of shares of common stock outstanding during the period. Diluted net loss per share is computed by giving effect to all potentially dilutive common stock equivalents to the extent they are dilutive. For purposes of this calculation, redeemable convertible preferred stock, stock options, restricted common stocks, RSUs, PSUs, ESPP, early exercised stock options, and common stock warrants are considered to be common stock equivalents but have been excluded from the calculation of diluted net loss per share attributable to common stockholders as their effect is anti-dilutive for all periods presented.

The rights, including the liquidation and dividend rights, of the holders of Class A and Class B common stock are identical, except with respect to voting, conversion, and transfer rights. As the liquidation and dividend rights are identical, the undistributed earnings are allocated on a proportionate basis to each class of common stock and the resulting basic and diluted net loss per share attributable to common stockholders are, therefore, the same for both Class A and Class B common stock on both individual and combined basis.

Basic and diluted net loss per share attributable to common stockholders was as follows (in thousands, except share and per share data):

	Year Ended January 31,		
	2023	2022	2021
Numerator:			
Net loss attributable to Class A and Class B common stockholders	$ (378,678)	$ (271,101)	$ (117,573)
Denominator:			
Weighted-average shares used in computing net loss per share attributable to Class A and Class B common stockholders, basic and diluted	277,802,861	174,051,203	35,482,444
Net loss per share attributable to Class A and Class B common stockholders, basic and diluted	$ (1.36)	$ (1.56)	$ (3.31)

The following potentially dilutive securities were excluded from the computation of diluted net loss per share attributable to common stockholders because their inclusion would have been anti-dilutive:

	As of January 31,		
	2023	2022	2021
Redeemable convertible preferred stock	—	—	168,951,059
Stock options	32,446,814	42,422,473	37,231,191
Common stock warrants	—	—	954,884
Shares subject to repurchase	178,308	20,091	37,500
RSUs and PSUs	14,409,166	1,770,304	—
ESPP	134,469	52,381	—
Restricted common stock	451,444	1,142,496	—
Contingently issuable shares	—	1,317,089	—
Total	47,620,201	46,724,834	207,174,634

12. GEOGRAPHIC INFORMATION

Long-lived assets, consisting of property and equipment, net, and operating lease right-of-use assets, by geography were as follows (in thousands):

	As of January 31,	
	2023	2022
United States	$ 27,990	$ 21,176
Israel	27,625	26,646
Rest of world	6,690	980
Total	$ 62,305	$ 48,802

Revenue by geography is presented in Note 3, *Revenue and Contract Balances*.

13. COMMITMENTS AND CONTINGENCIES

Legal Contingencies

From time to time, we may be a party to various legal proceedings and subject to claims in the ordinary course of business.

BlackBerry Litigation

Starting in October 2019, BlackBerry Corp. and its subsidiary Cylance, Inc. (BlackBerry) filed a total of nine proceedings (seven lawsuits and two arbitrations) against us and certain former BlackBerry employees who joined our company. In these proceedings, BlackBerry alleges that it has viable legal claims as a result of its former employees joining us. Many of these proceedings have now been dismissed. The status of each of the currently pending proceedings is discussed below. We have defended against these claims vigorously and expect to continue to do so.

BlackBerry Corp., et al. v. Coulter, et al. On October 17, 2019, BlackBerry commenced an action captioned BlackBerry Corp., et al. v. Chris Coulter, in the Vermont Superior Court—Chittenden Unit, Case No. 953-10-19 Cncv, against Chris Coulter, a now-former employee who worked in our Vigilance services team (the “Vermont Action”). On October 23, 2019, BlackBerry filed an amended complaint that added the company as a defendant. The amended complaint asserts claims against us for conspiracy, tortious interference with contract, aiding and abetting breach of fiduciary duties, and misappropriation of trade secrets. On April 17, 2020, the court in the Vermont Action issued a preliminary injunction that enjoined Mr. Coulter from working at our company until after February 2021.

As a result of the court's order, Mr. Coulter chose to seek other employment and is no longer employed by us. On January 15, 2021, the court entered an order narrowing the scope of the case and limiting the claims against us to avoid conflict with a similar action that was previously filed in California and was dismissed. The Vermont Action is currently pending. The matter is set to be ready for trial by July 1, 2023; no trial date has been set. On October 25, 2019, BlackBerry commenced a separate action captioned BlackBerry Corp., et al v. Coulter, et al., No. 2019-0854-JTL (Del. Ch.) (the "Delaware Action") against Mr. Coulter and the company in Delaware Chancery Court. The court stayed this case pending resolution of the Vermont Action. On February 7, 2020, BlackBerry voluntarily dismissed without prejudice all claims against Mr. Coulter and us in the Delaware Action. On December 3, 2019, BlackBerry initiated a largely duplicative arbitration solely against Mr. Coulter administered by JAMS, an alternative dispute resolution provider. That arbitration, however, was dismissed on or about March 30, 2021, with JAMS informing us that they had closed their files on this matter on April 30, 2021.

BlackBerry Corp. et al. v. Sentinel Labs, Inc., et al. On January 16, 2020, BlackBerry commenced an action captioned BlackBerry Corp., et al. v. Sentinel Labs, Inc., et al., No. 20CV361950 in the California Superior Court of Santa Clara County, California against us and unnamed "Doe" defendants (who counsel understands are all former BlackBerry employees that we later employed), asserting claims for trade secret misappropriation and unfair business practices (the "California Action"). We filed counterclaims that, in part, seek to invalidate unlawful provisions under California law in BlackBerry's agreements it entered into with its employees. Between December 2020 and August 2021, there were several rounds of motion practice, court hearings, and court orders relating to the sufficiency of BlackBerry's identification of its alleged trade secrets in connection with its misappropriation of trade secrets claim, resulting in a narrowed scope of this claim. We are mid-discovery, and there have been court hearings and orders in connection with various discovery disputes. We continue to vigorously litigate this lawsuit, including our counterclaims against BlackBerry. Fact discovery is currently set to close by August 2023, and a trial has now been set for March 28, 2024.

BlackBerry Corp., et al. v. Quinn, et al. On February 17, 2020, BlackBerry commenced an action captioned BlackBerry Corp., et al. v. Quinn, et al., Case No. D-1-GN-20-00096, in 459th Judicial District of Travis County, Texas, against Sean Quinn, our now-former employee, and the company. On August 8, 2020, we and Mr. Quinn moved to stay or dismiss this case in light of the overlapping issues between this lawsuit and the California Action. On September 21, 2020, the court stayed this case pending resolution of the California Action. This lawsuit remains stayed and is pending in abeyance before the Texas court.

BlackBerry Corp., et al. v. Kaylan Brown Coulter. On April 7, 2022, BlackBerry commenced an action captioned BlackBerry Corp., et al. v. Kaylan Brown Coulter, Case No. 22-cv-01249, in the Superior Court - Chittenden Unit, Vermont, against Kaylan Brown-Coulter, the wife of Chris Coulter (referenced above), alleging breach of non-disclosure and non-solicitation agreements, breach of covenant of good faith and fair dealing, breach of fiduciary duties, and civil conspiracy. While this is part of the same series of lawsuits by BlackBerry, we were not named in this action. On May 6, 2022, Ms. Brown-Coulter removed the case to the United States District Court for the District of Vermont (Case No. 5:22-cv-98). Shortly thereafter, on May 13, 2022, Ms. Brown-Coulter filed a motion to dismiss all claims under Federal Rule of Civil Procedure 12(b)(6). This motion is currently pending before the court, and the matter is currently set to be trial ready for April 2023 unless dispositive motions are filed.

We have not recorded any accruals for loss contingencies associated with these legal proceedings, determined that an unfavorable outcome is probable, or determined that the amount or range of any possible loss is reasonably estimable. We believe that there are no other pending or threatened legal proceedings that are likely to have a material adverse effect on our consolidated financial statements.

Warranties and Indemnification

Our services are generally warranted to deliver and operate in a manner consistent with general industry standards that are reasonably applicable and materially conform with our documentation under normal use and circumstances. Our contracts generally include certain provisions for indemnifying customers against liabilities if our products or services infringe a third party's intellectual property rights.

We also offer a limited warranty to certain customers, subject to certain conditions, to cover certain costs incurred by the customer in case of a cybersecurity breach. We have entered into an insurance policy to cover our potential liability arising from this limited warranty arrangement. We have not incurred any material costs related to such obligations and have not accrued any liabilities related to such obligations in the consolidated financial statements as of January 31, 2023 and 2022.

In addition, we also indemnify certain of our directors and executive officers against certain liabilities that may arise while they are serving in good faith in their company capacities. We maintain director and officer liability insurance coverage that would generally enable us to recover a portion of any future amounts paid.

14. EMPLOYEE BENEFIT PLAN

Our U.S. employees participate in a 401(k) defined contribution plan sponsored by us. Contributions to the plan are discretionary. There was $2.8 million matching contributions by us for fiscal 2023. There were no matching contributions by us for fiscal 2022 and 2021.

Israeli Severance Pay

Israeli labor law generally requires payment of severance pay upon dismissal of an employee or upon termination of employment in certain other circumstances. Pursuant to Section 14 of the Severance Compensation Act, 1963 (Section 14), all of our employees in Israel are entitled to monthly deposits made in their name with insurance companies, at a rate of 8.33% of their monthly salary.

These payments release us from any future severance payment obligation with respect to these employees; as such, any liability for severance pay due to these employees and the deposits under Section 14 are not recorded as an asset on our consolidated balance sheets. For fiscal 2023, 2022, and 2021, we recorded $3.9 million, $3.7 million, and $2.7 million, respectively, in severance expenses related to these employees.

15. ACQUISITIONS

On May 3, 2022, we acquired 100% of the issued and outstanding equity securities (the Acquisition) of Attivo Networks, Inc. (Attivo), an identity security and lateral movement protection company. Attivo expands our coverage of critical attack surfaces. Identity is an adjacent security solution that complements our core endpoint solution. The Acquisition closed on May 3, 2022 and has been accounted for as a business combination in accordance with ASC Topic 805, Business Combinations.

We had post-combination expense with a fair value of $32.9 million that was not included in the total purchase consideration, which is comprised of 307,396 of restricted common stock with an aggregate fair value of $10.0 million, and 378,828 assumed options with an aggregate fair value of $11.5 million. Restricted common stock and assumed options will be recognized as stock-based compensation expense. In addition, in connection with the acquisition, certain employees who were promised compensation related to their previous employment agreements will be paid $11.4 million in cash based on continued employment which will be recognized on a straight-line basis as acquisition-related compensation costs. All post-combination expense is expected to be recognized through May 2026. Post-combination compensation expense is subject to adjustment based on continuing service obligations to the Company of certain stockholders of Attivo.

In connection with the Acquisition, we also granted restricted stock units (RSUs) and performance share units (PSUs) under our 2021 Equity Incentive Plan. For further details refer to Note 9, *Stock-Based Compensation*.

SENTINELONE, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS

The following table presents the preliminary allocation of purchase consideration recorded on our consolidated balance sheet as of the acquisition date (in thousands):

	Amount
Consideration:	
Cash	$ 348,917
Common Stock (6,032,231 shares)[(1)]	185,885
Fair value of total consideration transferred	$ 534,802
Cash and cash equivalents	$ 8,836
Accounts receivable	4,867
Prepaid expense and other current assets	3,880
Operating lease right-of-use assets	260
Intangible assets	151,900
Accrued liabilities	(4,270)
Accrued payroll and benefits	(1,113)
Operating lease liabilities	(259)
Deferred revenue	(51,746)
Other liabilities	(2,357)
Deferred tax liability	(7,310)
Total identifiable net assets	102,688
Goodwill	432,114
Total purchase consideration	$ 534,802

[(1)] Consideration calculated using the fair value of our common stock

The estimates and assumptions regarding the fair value of certain tangible assets acquired and liabilities assumed, the valuation of intangible assets acquired, income taxes, and goodwill are subject to change as we obtain additional information during the measurement period, which usually lasts for up to one year from the acquisition date.

The excess of the purchase price over the fair value of net tangible and intangible assets acquired has been assigned to goodwill. Goodwill represents the future benefits resulting from the acquisition that will enhance the value of our product for both new and existing customers and strengthen our competitive position. Goodwill is not deductible for tax purposes.

The following table sets forth the preliminary amounts allocated to the intangible assets identified and their estimated useful lives as of the date of acquisition:

	Fair Value (in thousands)	Useful Life (in years)
Customer relationships	$ 77,600	10
Developed technology	63,200	5
Backlog	11,100	2
Total intangible assets acquired	$ 151,900	

The preliminary fair value assigned to customer relationships was determined using the multi-period excess earnings method of the income approach. The fair value assigned to developed technology was determined using the relief from royalty method under the income approach. The fair value assigned to backlog was determined using the multi-period excess earnings method of the income approach. The intangible assets acquired are expected to be amortized over their useful lives on a straight-line basis.

Aside from $61.0 million, net, within restricted cash on the consolidated balance sheet, held in an indemnity escrow expected to be paid out within 15 months of the Acquisition, there are no other contingent consideration or cash consideration expected to be paid out subsequent to the Acquisition. The indemnity escrow was measured at fair value within other liabilities in our consolidated balance sheet at Acquisition and will be accreted to face value until paid out. The results of operations of Attivo have been included in our consolidated financial statements from the date of the Acquisition.

We have incurred $5.5 million of transaction expenses in connection with the Acquisition during the year ended January 31, 2023. $3.2 million of these costs were recorded as general and administrative expenses in our consolidated statements of operations during the year ended January 31, 2023, with the remainder allocated to purchase price consideration.

Our consolidated statements of operations from the date of the Acquisition to the period ended January 31, 2023 includes revenue and net loss of Attivo of $30.2 million and $36.4 million, respectively.

The following unaudited supplemental pro forma financial information is provided for informational purposes only and summarizes our combined results of operations as if the Acquisition occurred on February 1, 2021 (in thousands):

	Year Ended January 31,	
	2023	2022
Revenue	$ 429,683	$ 235,321
Net loss	$ (393,773)	$ (326,829)

The unaudited supplemental pro forma results reflect certain adjustments for the amortization of acquired intangible assets, recognition of stock-based compensation, acquisition-related transaction expenses, and acquisition-related compensation costs. Such pro forma amounts are not necessarily indicative of the results that actually would have occurred had the Acquisition been completed on the date indicated, nor is it indicative of our future operating results.

16. RECLASSIFICATION OF PRIOR YEAR PRESENTATION

Certain prior year amounts have been reclassified for consistency with the current year presentation. These reclassifications had no effect on the reported results of operations. An adjustment has been made to the consolidated balance sheets for fiscal year ended January 31, 2022, to reclassify $6.0 million in other assets to long-term investments.

17. SUBSEQUENT EVENTS

In February 2023, the Company entered into a non-cancellable agreement with a cloud infrastructure vendor, under which the Company committed to spend an aggregate of at least $860.0 million between March 2023 and February 2029.

ITEM 9. CHANGES IN AND DISAGREEMENTS WITH ACCOUNTANTS ON ACCOUNTING AND FINANCIAL DISCLOSURES

None.

ITEM 9A. CONTROLS AND PROCEDURES

Evaluation of Disclosure Controls and Procedures

Our management, with the participation of our Chief Executive Officer and Chief Financial Officer, has evaluated the effectiveness of our disclosure controls and procedures as of January 31, 2023. The term "disclosure controls and procedures," as defined in Rules 13a-15(e) and 15d-15(e) under the Exchange Act, means controls and other procedures of a company that are designed to ensure that information required to be disclosed by a company in the reports that it files or submits under the Exchange Act is recorded, processed, summarized, and reported within the time periods specified in the SEC's rules and forms. Disclosure controls and procedures include, without limitation, controls and procedures designed to ensure that information required to be disclosed by a company in the reports that it files or submits under the Exchange Act is accumulated and communicated to the company's management, including its principal executive and principal financial officers, or persons performing similar functions, as appropriate to allow timely decisions regarding required disclosure. In designing and evaluating our disclosure controls and procedures, our management recognizes that disclosure controls and procedures, no matter how well conceived and operated, can provide only reasonable assurance that the objectives of the disclosure controls and procedures are met. Based on such evaluation, our Chief Executive Officer and Chief Financial Officer concluded that, as of January 31, 2023, our disclosure controls and procedures were effective at the reasonable assurance level.

Changes in Internal Control Over Financial Reporting

There were no changes in our internal control over financial reporting (as defined in Rules 13a-15(f) and 15d-15(f) under the Exchange Act) that occurred during the period covered by this Annual Report on Form 10-K that has materially affected, or is reasonably likely to materially affect, our internal control over financial reporting.

Inherent Limitations on Effectiveness of Controls

Our management, including our Chief Executive Officer and Chief Financial Officer, believes that our disclosure controls and procedures and internal control over financial reporting are designed to provide reasonable assurance of achieving their objectives and are effective at the reasonable assurance level. However, management does not expect that our disclosure controls and procedures or our internal control over financial reporting will prevent or detect all errors and all fraud. A control system, no matter how well conceived and operated, can provide only reasonable, not absolute, assurance that the objectives of the control system are met. Because of the inherent limitations in all control systems, no evaluation of controls can provide absolute assurance that all control issues and instances of fraud, if any, within the company have been detected. The design of any system of controls also is based in part upon certain assumptions about the likelihood of future events, and there can be no assurance that any design will succeed in achieving its stated goals under all potential future conditions. Over time, controls may become inadequate because of changes in conditions, or the degree of compliance with the policies or procedures may deteriorate. Because of the inherent limitations in a cost-effective control system, misstatements due to error or fraud may occur and not be detected.

Management's Report on Internal Control over Financial Reporting

Our management is responsible for establishing and maintaining adequate internal control over financial reporting, as such term is defined in Exchange Act Rules 13a-15(f) and 15d-15(f). Our management conducted an evaluation of the effectiveness of our internal control over financial reporting as of January 31, 2023, based on the criteria established in Internal Control - Integrated Framework (2013) issued by the Committee of Sponsoring Organizations of the Treadway Commission. We have excluded Attivo from our evaluation of internal control over financial reporting, which financial statements are included in the January 31, 2023 consolidated financial statements and constituted approximately 0.5% of total assets as of January 31, 2023, and approximately 7% of total revenue during the year ended January 31, 2023. Based on the results of its evaluation, management concluded that our internal control over financial reporting was effective as of January 31, 2023. The effectiveness of our internal control over financial reporting as of January 31, 2023, has been audited by Deloitte and Touche LLP, an independent registered public accounting firm, as stated in its report which is included in Part II, Item 8 of this Annual Report.

ITEM 9B. OTHER INFORMATION

None.

ITEM 9C. DISCLOSURE REGARDING FOREIGN JURISDICTIONS THAT PREVENT INSPECTIONS

Not applicable.

PART III.

ITEM 10. DIRECTORS, EXECUTIVE OFFICERS AND CORPORATE GOVERNANCE

The information required by this Item (other than the information set forth in the next paragraph) will be included in our definitive Proxy Statement for our 2023 annual meeting of stockholders, which will be filed with the SEC within 120 days after the end of our fiscal year ended January 31, 2023, and is incorporated herein by reference.

We maintain a Code of Business Conduct and Ethics (Code of Ethics), applicable to all employees, including all directors and executive officers. Our Code of Ethics is published on our Investor Relations website at investors.sentinelone.com under “Governance.” We intend to satisfy the disclosure requirement under Item 5.05 of Form 8-K regarding amendments to, or waiver from, a provision of the Code of Ethics by posting such information on the website address and location specified above.

ITEM 11. EXECUTIVE COMPENSATION

The information required by this Item will be included in our Proxy Statement to be filed with the SEC within 120 days after the end of our fiscal year ended January 31, 2023, and is incorporated herein by reference.

ITEM 12. SECURITY OWNERSHIP OF CERTAIN BENEFICIAL OWNERS AND MANAGEMENT AND RELATED STOCKHOLDER MATTERS

The information required by this Item will be included in our Proxy Statement to be filed with the SEC within 120 days after the end of our fiscal year ended January 31, 2023, and is incorporated herein by reference.

ITEM 13. CERTAIN RELATIONSHIPS AND RELATED PARTY TRANSACTIONS

The information required by this Item will be included in our Proxy Statement to be filed with the SEC, within 120 days after the end of our fiscal year ended January 31, 2023, and is incorporated herein by reference.

ITEM 14. PRINCIPAL ACCOUNTANT FEES AND SERVICES

The information required by this Item will be included in our Proxy Statement to be filed with the SEC, within 120 days after the end of our fiscal year ended January 31, 2023, and is incorporated herein by reference.

PART IV.

ITEM 15. EXHIBITS AND FINANCIAL STATEMENTS SCHEDULES

(a) Financial Statements.

See Index to Consolidated Financial Statements in Item 8 of this Annual Report on Form 10-K.

(b) Financial Statement Schedule.

All financial statement schedules are omitted because the information required to be set forth therein is not applicable or is shown in the consolidated financial statements or the notes thereto.

(c) Exhibits.

The exhibits listed below are filed as part of this Annual Report on Form 10-K or are incorporated herein by reference, in each case as indicated below.

Exhibit Number	Description of Document	Form	File No.	Exhibit	Filing Date
2.1	Agreement and Plan of Merger by and between Registrant, Aardvark Acquisition Sub I, Inc., Aardvark Merger Sub II, LLC, Attivo Networks, Inc., and Fortis Advisors LLC, dated as of March 15, 2022.	10-Q	001-40531	2.1	June 1, 2022
3.1	Restated Certificate of Incorporation of SentinelOne, Inc.	10-K	001-40531	3.1	April 7, 2022
3.2	Amended and Restated Bylaws of SentinelOne, Inc.	8-K	001-40531	3.1	December 13, 2022
4.1	Form of Class A Common Stock certificate of SentinelOne, Inc.	S-1/A	333-256761	4.1	June 21, 2021
4.2	Description of Registrant's securities.	10-K	001-40531	4.2	April 7, 2022
4.3	Amended and Restated Investors' Rights Agreement among SentinelOne, Inc. and certain holders of capital stock, dated October 28, 2020.	S-1	333-256761	4.2	June 3, 2021
10.1	Form of Indemnification Agreement between SentinelOne, Inc. and each of its directors and executive officers.	S-1	333-256761	10.1	June 3, 2021
10.2†	SentinelOne, Inc. 2021 Equity Incentive Plan and related form agreements.	S-1	333-256761	10.4	June 3, 2021
10.3†	SentinelOne, Inc. 2021 Employee Stock Purchase Plan and related form agreements.	S-1/A	333-256761	10.5	June 21, 2021
10.4†	Confirmatory Employment Letter between SentinelOne, Inc. and Tomer Weingarten, dated May 28, 2021.	S-1/A	333-256761	10.7	June 21, 2021
10.5†	Confirmatory Employment Letter between SentinelOne, Inc. and David Bernhardt, dated May 28, 2021.	S-1/A	333-256761	10.8	June 21, 2021
10.6†	Confirmatory Employment Letter between SentinelOne, Inc. and Nicholas Warner, dated June 19, 2021.	S-1/A	333-256761	10.9	June 21, 2021
10.7†	Confirmatory Employment Letter between SentinelOne, Inc. and Ric Smith, dated May 28, 2021.	10-K	001-40531	10.7	April 7, 2022

10.8†	Offer of Employment and Change in Control and Severance Agreement between SentinelOne, Inc. and Keenan Conder, effective June 24, 2021.	10-K	001-40531	10.8	April 7, 2022
10.9†	Change in Control and Severance Agreement by and between SentinelOne, Inc. and Tomer Weingarten, dated May 28, 2021.	S-1/A	333-256761	10.11	June 21, 2021
10.10†	Change in Control and Severance Agreement by and between SentinelOne, Inc. and David Bernhardt, dated May 28, 2021.	S-1/A	333-256761	10.12	June 21, 2021
10.11†	Change in Control and Severance Agreement by and between SentinelOne, Inc. and Nicholas Warner, dated June 19, 2021.	S-1/A	333-256761	10.13	June 21, 2021
10.12†	Change in Control and Severance Agreement by and between SentinelOne, Inc. and Ric Smith.	10-K	001-40531	10.12	April 7, 2022
10.13†	Offer of Employment and Change in Control and Severance Agreement between SentinelOne, Inc. and Narayanan 'Vats' Srivatsan, effective February 26, 2022.				
10.14	Office Lease, by and between SIC-Mountain Bay Plaza, LLC and SentinelOne, Inc. and Silicon Valley Bank dated as of June 9, 2020, as amended.	S-1	333-256761	10.7	June 3, 2021
21.1	List of Subsidiaries of SentinelOne, Inc.				
23.1	Consent of Deloitte & Touche LLP, independent registered public accounting firm.				
24.1	Power of Attorney (included in signature pages hereto).				
31.1*	Certification of Principal Executive Officer Pursuant to Rules 13a-14(a) and 15d-14(a) under the Securities Exchange Act of 1934, as Adopted Pursuant to Section 302 of the Sarbanes-Oxley Act of 2002.				
31.2*	Certification of Principal Financial Officer Pursuant to Rules 13a-14(a) and 15d-14(a) under the Securities Exchange Act of 1934, as Adopted Pursuant to Section 302 of the Sarbanes-Oxley Act of 2002.				
32.1*	Certification of Chief Executive Officer and Chief Financial Officer pursuant to 18 U.S.C. Section 1350, as adopted pursuant to section 906 of the Sarbanes-Oxley Act of 2002.				
101.INS	Inline XBRL Instance Document--the instance document does not appear in the Interactive Data File because XBRL tags are embedded within the Inline XBRL document.				
101.SCH	Inline XBRL Taxonomy Extension Schema Document.				

101.CAL	Inline XBRL Taxonomy Extension Calculation Linkbase Document.
101.DEF	Inline XBRL Taxonomy Extension Definition Linkbase Document.
101.LAB	Inline XBRL Taxonomy Extension Label Linkbase Document.
101.PRE	Inline XBRL Taxonomy Extension Presentation Linkbase Document.
104	Cover Page Interactive Data File (formatted as inline XBRL and contained in Exhibit 101).

_____

* The certifications furnished in Exhibits 32.1 hereto are deemed to accompany this Annual Report on Form 10-K and will not be deemed "filed" for purposes of Section 18 of the Exchange Act, or otherwise subject to the liability of that section, nor shall they be deemed incorporated by reference into any filing under the Securities Act or the Exchange Act.

† Indicates management contract or compensatory plan.

ITEM 16. FORM 10-K SUMMARY

None.

SIGNATURES

Pursuant to the requirements of the Securities Exchange Act of 1934, as amended, the registrant has duly caused this report to be signed on its behalf by the undersigned, thereunto duly authorized, in Mountain View, California on the 29th day of March, 2023.

SENTINELONE, INC.

By: /s/ Tomer Weingarten
Tomer Weingarten
Chairman of the Board of Directors, President and Chief Executive Officer
(*Principal Executive Officer)*

POWER OF ATTORNEY

KNOW ALL THESE PERSONS BY THESE PRESENTS, that each person whose signature appears below constitutes and appoints Tomer Weingarten and David Bernhardt, and each of them, as his or her true and lawful attorney-in-fact and agent, with full power of substitution and resubstitution, for him or her and in his or her name, place and stead, in any and all capacities, to sign any and all amendments to this Annual Report on Form 10-K, and to file the same, with all exhibits thereto, and other documents in connection therewith, with the Securities and Exchange Commission, granting unto said attorneys-in-fact and agents, and each of them, full power and authority to do and perform each and every act and thing requisite and necessary to be done in connection therewith, as fully to all intents and purposes as he or she might or could do in person, hereby ratifying and confirming all that said attorneys-in-fact and agents, or any of them, or their, his or her substitutes, may lawfully do or cause to be done by virtue thereof.

Pursuant to the requirements of the Exchange Act of 1934, as amended, this Annual Report on Form 10-K has been signed by the following persons in the capacities and on the dates indicated.

Signature	Title	Date
/s/ Tomer Weingarten Tomer Weingarten	Chairman of the Board of Directors, President, and Chief Executive Officer (Principal Executive Officer)	March 29, 2023
/s/ David Bernhardt David Bernhardt	Chief Financial Officer (Principal Financial Officer)	March 29, 2023
/s/ Robin Tomasello Robin Tomasello	Chief Accounting Officer (Principal Accounting Officer)	March 29, 2023
/s/ Charlene T. Begley Charlene T. Begley	Director	March 29, 2023
/s/ Aaron Hughes Aaron Hughes	Director	March 29, 2023
/s/ Mark S. Peek Mark S. Peek	Director	March 29, 2023
/s/ Ana Pinczuk Ana Pinczuk	Director	March 29, 2023

/s/ Daniel Scheinman	Director	March 29, 2023
Daniel Scheinman		
/s/ Teddie Wardi	Director	March 29, 2023
Teddie Wardi		
/s/ Jeffery W. Yabuki	Director	March 29, 2023
Jeffery W. Yabuki		

Exhibit 10.13

February 26, 2022

Vats Srivatsan
**

Re: Offer of employment at SentinelOne, Inc.

Dear Vats:

We are very pleased to invite you to join SentinelOne, Inc. (the **"Company,"** or **"SentinelOne").**

1. *Duties and Responsibilities.* You will report to Tomer Weingarten in his capacity as Chief Executive Officer. Your role as Chief Operating Officer, will drive and architect organic and inorganic growth of the company with particular emphasis on go-to-market as we accelerate towards our next phase of growth.
All business solutions will report into this role with DataSet transitioning immediately and we will use our best efforts to transition the Security business within the next six months; provided, however, if the Security business is not transitioned to you within such time-frame, this will be included in the definition of "Good Reason" as set forth in Exhibit B. Under that specific circumstance, the Severance Benefits set forth in Exhibit B, would also include the acceleration of one-half of the RSUs that would otherwise vest on your First Vesting Date (which is 12.5% of the RSU Grant referenced in paragraph 5 below). Moreover, if your role is changed from Chief Operating Officer, this will also be hereby included in the definition of "Good Reason" as set forth in Exhibit B." This Offer Letter ("Offer") is for a full-time position and this position is classified as exempt. This position is designated as a section 16 Executive Officer. You will work remotely and travel to and work from our California offices as needed. The position may also require you to travel to other locations as may be necessary to fulfill your responsibilities.

2. *Salary.* Your initial annual base salary will be $450,000 payable in accordance with the Company's customary payroll practice. Your salary is subject to periodic review and adjustment by the Compensation Committee of the Company's Board of Directors (the **"Compensation Committee"),** and any such adjustment is solely within the discretion of the Compensation Committee.

3. *Variable Compensation.* You may also be eligible to receive variable bonus compensation paid in accordance with the Company's bonus compensation policies and at the sole discretion of the Compensation Committee. Your bonus compensation shall be targeted at $450,000 per year.

4. *Benefits and Vacation.* You will be entitled to participate in the Company's 401(K) plan. Employee Stock Purchase Program and group health insurance plan, subject to and in accordance with applicable eligibility requirements with the terms and conditions as in effect from time to time. You will be eligible for paid Company holidays and to accrue paid vacation under the Company's vacation plan.

5. *RSU Grant.* The Company will recommend that the Board or a committee thereof grant you restricted stock units ("RSUs") with an aggregate value of $15,000,000 (the "Aggregate RSU Value"), pursuant to the terms of the Company's 2021 Equity Incentive Plan (the "Plan"). The number of shares of the Company's Common Stock subject to the RSUs will equal the Aggregate RSU Value divided by the trailing 30-calendar day average of the closing trading price of the Company's Class A Common Stock on the New York Stock Exchange immediately preceding the date of grant, rounding up to the nearest whole share. RSUs are granted at the sole discretion of the Compensation Committee and are typically granted at the next regularly scheduled meeting of the Compensation Committee following commencement of your provision of services to the Company. Following your formal written acceptance of the RSUs and in accordance with your award agreement, for so long as you provide continuous service to the Company, the RSUs will vest as follows: the RSUs will vest over a total of four (4) years with twenty-five percent (25%) of the RSUs vesting on the first Vest Date following the one-year anniversary of your Employment Start Date (the "First Vesting Date"), and thereafter 1/12th of the RSUs vesting on each third Vesting Date following the first Vesting Date. For purposes of this paragraph, a "Vesting Date" is the fifth (5th) day of each month.

6. *Expenses.* Expenses related to your employment at the Company are subject to the Company's Travel & Expenses Policy.

7. *Withholdings.* All forms of compensation paid to you as an employee of the Company shall be less all applicable withholdings.

8. *Confidential Information; Employee Confidential Information and Inventions Agreement* To enable the Company to safeguard its proprietary and confidential information, as a pre-condition to your employment at SentinelOne and by signing this offer letter, You also agree to the terms of the Company's form of At-Will Employment, Confidential Information and Invention Assignment Agreement attached as Exhibit A hereto (the

"Agreement"), and confirm that you have had an opportunity and sufficient time to consider the terms of the Agreement and consult an attorney of your choice. Furthermore, as we understand that you may have signed similar agreements with prior employers, we wish to impress upon you that you are absolutely prohibited from disclosing to the Company, directly or indirectly, any confidential or proprietary information of others, and fully expect that you will comply with your legally binding obligations to prior employers (as further detailed in the Agreement).

9. *At-Will Employment* You should be aware that your employment with the Company is for no specified period and constitutes at-will employment. As a result, you are free to resign at any time, for any reason or for no reason. Similarly, the Company is free to conclude its employment relationship with you at any time, with or without cause, and with or without notice. Participation in any RSUs, benefit, compensation or incentive program does not change the nature of the employment relationship, which remains "at-will." No one other than an executive officer of the Company has the authority to enter into an agreement for employment for any specified period, or to make any promises or commitments contrary to the Company's at-will policy. To be valid and enforceable, any employment agreement for a specified term entered into by the Company must be in writing, expressly described therein as an "employment agreement" and signed by an executive officer of the Company.

10. *Termination Benefits.* You will be eligible to receive change in control and severance payments and benefits under the Change in Control and Severance Agreement (the **"Severance Agreement")** attached hereto as Exhibit B.

11. *No Conflicting Obligations.* You understand and agree that by signing this letter, you represent to the Company that your performance will not breach any other agreement to which you are a party and that you have not, and will not during the term of your employment with the Company, enter into any oral or written agreement in conflict with any of the provisions of this letter or the Company's policies. You are not to bring with you to the Company, or use or disclose to any person associated with the Company, any confidential or proprietary information belonging to any former employer or other person or entity with respect to which you owe an obligation of confidentiality under any agreement or otherwise. The Company does not need and will not use such information and we will assist you in any way possible to preserve and protect the confidentiality of proprietary information belonging to third parties. Also, we expect you to abide by any obligations to refrain from soliciting any person employed by or otherwise associated with any former employer and suggest that you refrain from having any contact with such persons until such time as any non-solicitation obligation expires.

12. *Outside Activities.* While you render services to the Company, you agree that you will not engage in any other employment, consulting or other business activity without the written consent of the Company. In addition, while you render services to the Company, you will not assist any person or entity in competing with the Company, in preparing to compete with the Company or in hiring any employees or consultants of the Company.

13. *Equal Employment Opportunity.* The Company is an equal opportunity employer and conducts its employment practices based on business needs and in a manner that treats employees and applicants on the basis of merit and experience. The Company prohibits unlawful discrimination on the basis of race, color, religion, sex, pregnancy, national origin, citizenship, ancestry, age, physical or mental disability, veteran status, marital status, domestic partner status, sexual orientation, or any other consideration made unlawful by federal, state or local laws.

14. *Authorization to Work.* For purposes of federal immigration law, you will be required to provide to the Company documentary evidence of your identity and eligibility for employment in the United States. Such documentation must be provided to us within three business days of your date of hire, or our employment relationship with you may be terminated. Your work authorization documentation will be validated through the E-Verify program (https://www.e-verify.gov/employees). Your continued employment with SentinelOne is subject to confirmation that you are authorized to work in the United States. If you have any questions, please contact me at peopleops@sentinelone.com.

15. *Indemnification; D&O Insurance Coverage.* Per the Company's Bylaws, as an officer, you will be indemnified (as other officers and members of the Board of Directors) to the fullest extent permitted under the Delaware General Corporation Law and included in the Company's Directors and Officers insurance policy.

16. *Complete Offer and Agreement* This letter, the Agreement and the Severance Agreement set forth the entire agreement and terms of your employment with the Company and supersede any prior representations, discussions or agreements, even if inconsistent, and whether written or oral, among you and the Company. This letter may not be modified or amended except by a written agreement, signed by an executive officer of the Company and by you. It is understood that the Company may, from time to time, in its sole discretion, adjust the salaries, incentive compensation and benefits paid to you and its other employees, as well as job titles, locations, duties, responsibilities, assignments and reporting relationships.

17. *Start Date; Acceptance of Offer.* This Offer is subject to successful completion of relevant background checks (as may be limited by applicable law). Unsatisfactory completion of such background checks will be considered and may lead to withdrawal of this Offer. Subject to the foregoing, we hope that you will accept this offer promptly and begin your full-time employment at the Company by April 4, 2022 your **"Employment Start Date").** If our offer is acceptable to you, please sign the enclosed copy of this letter in the space indicated and return it to me at your earliest convenience.

Vats, our team was impressed by your accomplishments and potential, and we are enthusiastic at the prospect of your joining us. I look forward to your early acceptance of this offer, and to your contributions to the growth and success of SentinelOne.

Sincerely,

Tomer Weingarten
Chief Executive Officer

ACCEPTANCE OF EMPLOYMENT OFFER:

I accept the offer of employment by the Company on the terms described in this letter.

Signature:

Date:

EXHIBIT A
SENTINELONE, INC.
AT-WILL EMPLOYMENT, CONFIDENTIAL INFORMATION AND INVENTION ASSIGNMENT AGREEMENT

As a condition of my employment with SentinelOne, Inc. (the **"Company"),** and in consideration of my employment with the Company, my receipt of the compensation now and hereafter paid to me by Company, the Company's promise to provide and/or continue to provide access to the Company's Confidential Information as defined below, and the Company's promise to provide and/or continue to provide access to the Company's goodwill (none of which I would receive absent signing this Agreement), I agree to the following provisions of this At-Will Employment, Confidential Information and Invention Assignment Agreement (this **"Agreement"):**

1. **At-Will Employment**

I UNDERSTAND AND ACKNOWLEDGE THAT MY EMPLOYMENT WITH THE COMPANY IS FOR NO SPECIFIED TERM AND CONSTITUTES "AT-WILL" EMPLOYMENT. I ALSO UNDERSTAND THAT ANY REPRESENTATION TO THE CONTRARY IS UNAUTHORIZED AND NOT VALID UNLESS IN WRITING AND SIGNED BY THE PRESIDENT OR CEO OF THE COMPANY. ACCORDINGLY, I ACKNOWLEDGE THAT MY EMPLOYMENT RELATIONSHIP MAY BE TERMINATED AT ANY TIME, WITH OR WITHOUT GOOD CAUSE OR FOR ANY OR NO CAUSE, AT MY OPTION OR AT THE OPTION OF THE COMPANY, WITH OR WITHOUT NOTICE. I FURTHER ACKNOWLEDGE THAT THE COMPANY MAY MODIFY JOB TITLES, SALARIES, AND BENEFITS FROM TIME TO TIME AS IT DEEMS NECESSARY.

2. **Duty of Loyalty**

I understand and acknowledge that I owe the Company a fiduciary duty of loyalty. While employed by the Company, I agree at all times to devote my best efforts to the business of the Company, to perform conscientiously all duties and obligations required or assigned, and not to usurp, for personal gain, any opportunities in the Company's line of business or reasonably anticipated research and development. During my employment with the Company, I shall promptly and fully provide the Company with and disclose to the Company all information, ideas, improvements and recommendations relating to the Company's business, line of business, or reasonably anticipated research and development, whether or not protectable by patent, copyright or other proprietary right, and whether or not they are made, conceived or reduced to practice during my employment with the Company, or using the Company's facilities or data, of which I have knowledge, that could reasonably be considered to benefit the Company. I shall not usurp, for personal gain or the benefit of any other third party, any information which could reasonably be considered to benefit the Company that I learned, accessed, obtained or acquired during employment with the Company. Examples of conduct that constitutes a breach of an employee's duty of loyalty if engaged in during employment with the Company include, but are not limited to:

A. Soliciting customers of the Company for the personal benefit of the employee or any other third party, such as by having customers do business with the employee outside the Company's facilities on a cash basis or other methods of direct or indirect payment to the employee;

B. Offering trades of services to other employees of the Company while at the Company without authorization where the Company typically does not provide such services to employees for free;

C. Offering free services to customers while at the Company without authorization where such services are typically provided by the Company for a fee;

D. Performing any work or services outside of the Company that competes or interferes with the employee's work at the Company or results in usurping or interfering with any prospective business opportunity that is within the Company's line of business or reasonably anticipated research and development;

E. Taking a second or third job that results in diminishing, inhibiting, limiting or negatively impacting the employee's ability to effectively and proficiently complete job duties for the Company and to be available during normal business hours during which the employee's services are regularly scheduled or otherwise needed at the Company (the employee remains free to work anywhere else as long as such work does not compete with the Company's business and does not conflict with or inhibit the employee's ability to perform work for the Company);

F. If the employee is an hourly, non-exempt employee, doing or attending to other non- Company-related work or personal business while on the clock at the Company and not on a break;

G. Discussing with any customer whether the customer would follow or continue to work with the employee if/when the employee leaves the Company; and

H. Taking or retaining customer information at any time without the customer's authorization and/or upon termination of employment.

3. **Confidentiality**

A. *Definition of Company Confidential Information.* I understand that **"Company Confidential Information"** means information (including any and all combinations of individual items of information) that the Company has or will develop, acquire, create, compile, discover or own, whether reduced to writing or simply within my head, that has value in or to the Company's business and which the Company wishes and/or makes good faith efforts, to maintain as confidential and/or proprietary. Company Confidential Information includes both information disclosed by the Company to me, and information developed or learned by me during the course of my employment with the Company. Company Confidential Information also includes all information of which the unauthorized disclosure could be detrimental to the interests of the Company, whether or not such information is identified as Company Confidential Information. By example, and without limitation, Company Confidential Information includes any and all non-public information that relates to the actual or anticipated business and/or products, research or development of the Company, or to the Company's technical data, trade secrets, or know-how, including, but not limited to, research, product plans, or other information regarding the Company's products or services and markets therefor, customer lists and customers (including, but not limited to, customers of the Company on which I called or with which I may become acquainted during the term of my employment), software, developments, inventions, discoveries, ideas, processes, formulas, technology, designs, drawings, engineering, hardware configuration information, marketing, finances, and other business information disclosed by the Company either directly or indirectly in writing, orally or by drawings or inspection of premises, parts, equipment, or other Company property. For the avoidance of doubt, Company Confidential Information includes information that constitutes a trade secret—which is defined as information, including a formula, pattern, compilation, program, device, method, technique or process, that: (a) derives independent economic value, actual or potential, from not being generally known to the public or to other persons or entities who can obtain economic value from its disclosure or use and (b) is the subject of efforts that are reasonable under the circumstances to maintain it secrecy—as well as information that is not trade secret, but otherwise meets the definition of Company Confidential Information. Notwithstanding the foregoing, Company Confidential Information shall not include any such information which I can establish
(x) was publicly known or made generally available prior to the time of disclosure by the Company to me;
(y) becomes publicly known or made generally available after disclosure by the Company to me through no wrongful action or omission by me; or (z) is in my rightful possession, without confidentiality obligations, at the time of disclosure by the Company as shown by my then-contemporaneous written records; provided that any combination of individual items of information shall not be deemed to be within any of the foregoing exceptions merely because one or more of the individual items are within such exception, unless the combination as a whole is within such exception. Company Confidential Information does not include an employee's knowledge or experience acquired through experience in a field or industry. I understand that nothing in this Agreement is intended to limit employees' rights to discuss the terms, wages, and working conditions of their employment, as protected by applicable law.

B. *Nonuse and Nondisclosure.* I agree that during and after my employment with the Company, I will hold in the strictest confidence and take all reasonable precautions to prevent any unauthorized use or disclosure of Company Confidential Information. I will not (i) use Company Confidential Information for any purpose whatsoever other than for the benefit of the Company in the course of my employment, or (ii) disclose Company Confidential Information to any third party without the prior written authorization of the President, CEO, or the Board of Directors of the Company. Prior to disclosure, when compelled by applicable law, I shall provide prior written notice to the President, CEO, and General Counsel of the Company (as applicable). I agree that I obtain no title to any Company Confidential Information, and that as between Company and myself, the Company retains all Confidential Information as the sole property of the Company. I understand that my unauthorized use or disclosure of Company Confidential Information during my employment may lead to disciplinary action, up to and including, immediate termination and legal action by the Company. I understand that my obligations under this **Section 3.B** shall continue after termination of my employment and also that nothing in this Agreement prevents me from engaging in Protected Activity, as described below.

The prohibitions on use and disclosure in this Section 3.B. include, but are not limited to, using Company Confidential Information to (a) identify existing customers of the Company for my own personal benefit or the benefit of any other firm or entity; (b) facilitate the solicitation, for my personal benefit or the benefit of any other firm or entity, of any existing or prospective customers of the Company, that I serviced or solicited or about whom I otherwise gained Company Confidential Information during my employment with the Company; (c) facilitate the solicitation, for my personal benefit or the benefit of any other firm or entity, of any existing employees of the Company with whom I worked during my employment with the Company; and/or (d) otherwise unfairly compete with the Company. I will not reverse engineer, decompile or disassemble any products, software or other materials containing any company Confidential Information.

C. *Former Employer Confidential Information.* I agree that during my employment with the Company, I will not improperly use, disclose, or induce the Company to use any proprietary information or trade secrets of any former employer or other person or entity with which I have an obligation to keep such proprietary information or trade secrets in confidence. I further agree that I will not bring onto the Company's premises or transfer onto the Company's technology systems any unpublished document, proprietary information, or trade secrets belonging to any such third party unless disclosure to, and use by, the Company has been consented to, in writing, by such third party and the Company.

D. *Third Party Information.* I recognize that the Company has received, and in the future may receive, from third parties (for example, customers, suppliers, licensors, licensees, partners, and collaborators) as well as its subsidiaries and affiliates **("Associated Third Parties"),** information which the Company is required to maintain and treat as confidential or proprietary information of such Associated Third Parties **("Associated Third Party Confidential Information"),** and I agree to use such Associated Third Party Confidential Information only as directed by the Company and to not use or disclose such Associated Third Party Confidential Information in a manner that would violate the Company's obligations to such Associated Third Parties. By way of example, Associated Third Party Confidential Information may include the habits or practices of Associated Third Parties, the technology of Associated Third Parties, requirements of Associated Third Parties, and information related to the business conducted between the Company and such Associated Third Parties. I agree at all times during my employment with the Company and thereafter, that I owe the Company and its Associated Third Parties a duty to hold all such Associated Third Party Confidential Information in the strictest confidence, and not to use it or to disclose it to any person, firm, corporation, or other third party except as necessary in carrying out my work for the Company consistent with the Company's agreement with such Associated Third Parties. I further agree to comply with any and all Company policies and guidelines that may be adopted from time to time regarding Associated Third Parties and Associated Third Party Confidential Information. I understand that my unauthorized use or disclosure of Associated Third Party Confidential Information or violation of any Company policies during my employment may lead to disciplinary action, up to and including, immediate termination and legal action by the Company.

4. Ownership

A. *Assignment of Inventions.* As between the Company and myself, I agree that all right, title, and interest in and to any and all copyrightable material, notes, records, drawings, designs, logos, inventions, improvements, developments, discoveries, ideas and trade secrets conceived, discovered, authored, invented, developed or reduced to practice by me, solely or in collaboration with others, during the period of time I am in the employ of the Company (including during my off-duty hours), or with the use of Company's equipment, supplies, facilities, or Company Confidential Information, and any copyrights, patents, trade secrets, mask work rights or other intellectual property rights relating to the foregoing, except as provided in Section 4.G below (collectively, "Inventions"), are the sole property of the Company. I also agree to promptly make full written disclosure to the Company of any Inventions, and to deliver and assign and hereby irrevocably assign fully to the Company all of my right, title and interest in and to Inventions. I agree that this assignment includes a present conveyance to the Company of ownership of Inventions that are not yet in existence. I further acknowledge that all original works of authorship that are made by me (solely or jointly with others) within the scope of and during the period of my employment with the Company and that are protectable by copyright are "works made for hire," as that term is defined in the United States Copyright Act. I understand and agree that the decision whether or not to commercialize or market any Inventions is within the Company's sole discretion and for the Company's sole benefit, and that no royalty or other consideration will be due to me as a result of the Company's efforts to commercialize or market any such Inventions.

B. *Pre-Existing Materials.* I will inform the Company, in writing, before incorporating any inventions, discoveries, ideas, original works of authorship, developments, improvements, trade secrets and other proprietary information or intellectual property rights owned by me or in which I have an interest prior to, or separate from, my employment with the Company, including, without limitation, any such inventions that are subject to California Labor Code Section 2870 or other similar state laws ("Prior Inventions") into any Invention or otherwise utilizing any Prior Invention in the course of my employment with the Company; and the Company is hereby granted a nonexclusive, royalty-free, perpetual, irrevocable, transferable worldwide license (with the right to grant and authorize sublicenses) to make, have made, use, import, offer for sale, sell, reproduce, distribute, modify, adapt, prepare derivative works of, display, perform, and otherwise exploit such incorporated or utilized Prior Inventions, without restriction, including, without limitation, as part of, or in connection with, such Invention, and to practice any method related thereto. I will not incorporate any inventions, discoveries, ideas, original works of authorship, developments, improvements, trade secrets and other proprietary information or intellectual property rights owned by any third party into any Invention without the Company's prior written permission. I have attached hereto as Appendix A, a list describing all Prior Inventions that relate to the Company's proposed business, products, or research and development or, if no such list is attached, I represent and warrant that there are no such

Prior Inventions. Furthermore, I represent and warrant that if any Prior Inventions are included on Appendix A. they will not materially affect my ability to perform all obligations under this Agreement.

C. *Moral Rights.* Any assignment to the Company of Inventions includes all rights of attribution, paternity, integrity, modification, disclosure and withdrawal, and any other rights throughout the world that may be known as or referred to as "moral rights," "artist's rights," "droit moral," or the like (collectively, **"Moral Rights").** To the extent that Moral Rights cannot be assigned under applicable law, **I** hereby waive and agree not to enforce any and all Moral Rights, including, without limitation, any limitation on subsequent modification, to the extent permitted under applicable law.

D. *Maintenance of Records.* I agree to keep and maintain adequate, current, accurate, and authentic written records of all Inventions made by me (solely or jointly with others) during the term of my employment with the Company. The records will be in the form of notes, sketches, drawings, electronic files, reports, or any other format that may be specified by the Company. As between the Company and myself, the records are and will be available to and remain the sole property of the Company at all times.

E. *Further Assurances.* I agree to assist the Company, or its designee, at the Company's expense, in every proper way to secure the Company's rights in the Inventions in any and all countries, including the disclosure to the Company of all pertinent information and data with respect thereto, the execution of all applications, specifications, oaths, assignments, and all other instruments that the Company shall deem proper or necessary in order to apply for, register, obtain, maintain, defend, and enforce such rights, and in order to deliver, assign and convey to the Company, its successors, assigns, and nominees the sole and exclusive rights, title, and interest in and to all Inventions, and testifying in a suit or other proceeding relating to such Inventions. **I** further agree that my obligations under this **Section 4.E** shall continue after the termination of this Agreement.

F. *Attorney-in-Fact.* I agree that, if the Company is unable because of my unavailability, mental or physical incapacity, or for any other reason to secure my signature with respect to any Inventions, including, without limitation, for the purpose of applying for or pursuing any application for any United States or foreign patents or mask work or copyright registrations covering the Inventions assigned to the Company in **Section 4.A,** then **I** hereby irrevocably designate and appoint the Company and its duly authorized officers and agents as my agent and attorney-in-fact, to act for and on my behalf to execute and file any papers and oaths, and to do all other lawfully permitted acts with respect to such Inventions to further the prosecution and issuance of patents, copyright and mask work registrations with the same legal force and effect as if executed by me. This power of attorney shall be deemed coupled with an interest, and shall be irrevocable.

G. *Exception to Assignments.* PURSUANT TO CALIFORNIA LABOR CODE SECTIONS 2870-2872 AND OTHER SIMILAR STATE LAWS, I UNDERSTAND AND ACKNOWLEDGE THAT MY OBLIGATION TO ASSIGN INVENTIONS TO THE COMPANY DOES NOT APPLY TO ANY INVENTION FOR WHICH THERE WAS NO EQUIPMENT, SUPPLIES, FACILITY, OR TRADE SECRET INFORMATION OF THE COMPANY USED AND WHICH WAS DEVELOPED ENTIRELY ON MY OWN TIME, AND WHICH (1) DOES NOT RELATE DIRECTLY TO THE BUSINESS OF THE COMPANY OR THE COMPANY'S ACTUAL OR DEMONSTRABLY ANTICIPATED RESEARCH OR DEVELOPMENT, OR (2) DOES NOT RESULT FROM ANY WORK PERFORMED BY ME FOR THE COMPANY. FOR THE AVOIDANCE OF DOUBT, ANY DERIVATIVE OF THE COMPANY TECHNOLOGY OR OTHER INTELLECTUAL PROPERTY RIGHTS SHALL REMAIN OWNED BY THE COMPANY. I WILL ADVISE THE COMPANY PROMPTLY IN WRITING OF ANY INVENTIONS THAT I BELIEVE MEET THE ABOVE CRITERIA AND ARE NOT OTHERWISE DISCLOSED ON APPENDIX A TO PERMIT A DETERMINATION OF OWNERSHIP BY THE COMPANY. ANY SUCH DISCLOSURE WILL BE RECEIVED IN CONFIDENCE.

5. Conflicting Obligations

A. *Current Obligations.* I agree that during the term of my employment with the Company, I will not engage in or undertake any other employment, occupation, consulting relationship, or commitment that is directly related to the business in which the Company is now involved or becomes involved or has plans to become involved, nor will I engage in any other activities that conflict with my obligations to the Company.

B. *Prior Relationships.* Without limiting **Section 5.A, I** represent and warrant that **I** have no other agreements, relationships, or commitments to any other person or entity that conflict with the provisions of this Agreement, my obligations to the Company under this Agreement, or my ability to become employed and perform the services for which I am being hired by the Company. I further agree that if I have signed a

confidentiality agreement or similar type of agreement with any former employer or other entity, I will comply with the terms of any such agreement to the extent that its terms are lawful under applicable law. I represent and warrant that after undertaking a careful search (including searches of my computers, cell phones, electronic devices, and documents), **I** have returned all property and confidential information belonging to all prior employers (and/or other third parties **I** have performed services for in accordance with the terms of my applicable agreement). Moreover, **I** agree to fully indemnify the Company, its directors, officers, agents, employees, investors, shareholders, administrators, affiliates, divisions, subsidiaries, predecessor and successor corporations, and assigns for all verdicts, judgments, settlements, and other losses incurred by any of them resulting from my breach of my obligations under any agreement with a third party to which I am a party or obligation to which I am bound, as well as any reasonable attorneys' fees and costs if the plaintiff is the prevailing party in such an action, except as prohibited by law.

6. **Return of Company Materials**

A. *Definition of Electronic Media Equipment and Electronic Media Systems. I* understand that **"Electronic Media Equipment"** includes, but is not limited to, computers, external storage devices, thumb drives, mobile devices (including, but not limited to, smart phones, tablets, and e-readers), telephone equipment, and other electronic media devices. **I** understand that **"Electronic Media Systems"** includes, but is not limited to, computer servers, messaging and email systems or accounts, applications for computers or mobile devices, and web-based services (including cloud-based information storage accounts).

B. *Return of Company Property.* I understand that anything that I created or worked on for the Company while working for the Company belongs solely to the Company and that I cannot remove, retain, or use such information without the Company's express written permission. Accordingly, upon separation from employment with the Company or upon the Company's request at any other time, I will immediately deliver to the Company, and will not keep in my possession, recreate, or deliver to anyone else, any and all Company property, including, but not limited to, Company Confidential Information, Associated Third Party Confidential Information, all Company equipment including all Company Electronic Media Equipment, all tangible embodiments of the Inventions, all electronically stored information and passwords to access such property, Company credit cards, records, data, notes, notebooks, reports, files, proposals, lists, correspondence, specifications, drawings, blueprints, sketches, materials, photographs, charts, any other documents and property, and reproductions of any of the foregoing items including, without limitation, those records maintained pursuant to **Section 4.D.** Notwithstanding the foregoing, I understand that I am allowed to keep a copy of the Employee Handbook and personnel records relating to my employment.

C. *Return of Company Information on Company Electronic Media Equipment.* In connection with my obligation to return information to the Company, I agree that I will not copy, delete, or alter any information, including personal information voluntarily created or stored, contained in Company Electronic Media Equipment before I return the information to the Company.

D. *Return of Company Information on Personal Electronic Media Equipment.* In addition, if I have used any personal Electronic Media Equipment or personal Electronic Media Systems to create, receive, store, review, prepare or transmit any Company information, including, but not limited to, Company Confidential Information, I agree to make a prompt and reasonable search for such information in good faith, including reviewing any personal Electronic Media Equipment or personal Electronic Media Systems to locate such information and, if I locate such information, I agree to notify the Company of that fact and then provide the Company with a computer-useable copy of all such Company information from those equipment and systems. I agree to cooperate reasonably with the Company to verify that the necessary copying is completed (including upon request providing a sworn declaration confirming the return of property and deletion of information), and, upon confirmation of compliance by the Company, I agree to delete and expunge all Company information.

E. *No Expectation of Privacy in Company Property.* I understand that I have no expectation of privacy in Company property, and I agree that any Company property is subject to inspection by Company personnel at any time with or without further notice. As to any personal Electronic Media Equipment or personal Electronic Systems that I have used for Company purposes, I agree that the Company, at its sole discretion, may have reasonable access, as determined by the Company in good faith, to such personal Electronic Media Equipment or personal Electronic Media Systems to review, retrieve, destroy, or ensure the permanent deletion of Company information from such equipment or systems or to take such other actions necessary to protect the Company or Company property, as determined by the Company reasonably and in good faith. I also consent to an exit interview and an audit to confirm my compliance with this **Section 6,** and **I** will certify in writing that **I** have complied with the requirements of this **Section 6.**

7. **Termination Certification**

Upon separation from employment with the Company, I agree to immediately sign and deliver to the Company the "Termination Certification" attached hereto as Appendix B.

8. **Notification to New Employer**

In the event that I leave the employ of the Company, I hereby grant consent to notification by the Company to my new employer or contracting entity about my obligations under this Agreement. I also agree to keep the Company advised of my home and business address for a period of three (3) years after termination of my employment with the Company, so that the Company can contact me regarding my continuing obligations provided by this Agreement.

9. **Non-Competition**

To the fullest extent permitted under applicable law,, I agree that during my employment, and for a period of nine (9) months immediately following the termination of my relationship with the Company for any reason, whether voluntary or involuntary, with or without cause, I will not engage in competition with the Company in the geographical location where I was assigned to perform services for the Company during the last twenty-four months of relationship with the Company, or, if I performed services for the Company during that period which had an impact on the Company's products and/or services across the entire United States, then anywhere in the United States. I acknowledge that the Company does business across the United States. For purposes of this **Section 9,** "engage in competition" means entering into the employ of, or rendering any services to, a competitor of the Company where I am performing or rendering the same or similar services to the services I performed within the last twenty-four (24) months of my relationship with the Company, whether in the capacity of principal, agent, partner, officer, director, employee, consultant, independent contractor, or the like. A "competitor of the Company" is any entity that offers products and/or services which are substantially similar in nature to, such that they actually compete with, the products or services I worked on or about which I learned Confidential Information during the last twenty-four (24) months of my relationship with the Company. I agree that nothing in this
Section 9 shall affect my continuing obligations under this Agreement during and after this nine (9) month period, including, without limitation, my obligations under **Section 3.**

10. **Solicitation of Employees**

To the fullest extent permitted under applicable law, I agree that during my employment, and for a period of twelve (12) months immediately following the termination of my relationship with the Company for any reason, whether voluntary or involuntary, with or without cause, I will not solicit any of the Company's employees who hold a position uniquely essential to the management, organization, or service of the business to leave their employment at the Company. **I** agree that nothing in this **Section 10** shall affect my continuing obligations under this Agreement during and after this twelve (12) month period, including, without limitation, my obligations under **Section 3.**

11. **Solicitation of Customers**

To the fullest extent permitted under applicable law, I agree that during my employment, and for a period of twelve (12) months immediately following the termination of my relationship with the Company for any reason, whether voluntary or involuntary, with or without cause, I will not solicit, contact, call upon, or attempt to solicit or call upon, any customer of the Company for the purpose of selling products or performing services which are substantially similar in nature to, such that they actually compete with, the products or services I sold to or performed for customers on behalf of the Company during the last twenty-four (24) months of my relationship with the Company. This restriction shall apply only to any customer or prospective customer of the Company with whom I had contact during the last twenty-four (24) months of my relationship with the Company, or any customer of the Company about whom I obtained Company Confidential Information. For purposes of this **Section 11,** "contact" means interaction between me and the customer which takes place to further a business relationship with, or perform services for, the customer. The prohibitions in this **Section 11** apply regardless who initiates the contact. I agree that nothing in this **Section 11** shall affect my continuing obligations under this Agreement during and after this twelve (12) month period, including, without limitation, my obligations under **Section 3.**

12. **Remedies**

I acknowledge and agree that any breach of this Agreement by me would cause irreparable harm to the Company and that money damages would not provide an adequate remedy to the Company. I agree that if I commit or threaten to commit any such breach, the Company has the right to have the provisions of this Agreement specifically enforced by any court having jurisdiction, and I agree not to assert in any such enforcement action that the Company has an adequate remedy in damages. I agree that the right to specific enforcement will be in addition to, and not in lieu of, any other rights or remedies available to the Company in law or in equity. In addition, in the

event I violate any of the post-employment restrictive covenants set forth in this Agreement, I agree that the periods of restriction shall extend automatically by the number of days a court determines I violated such restriction. Further, in the event I breach this Agreement, I shall be liable for all damages and costs suffered by the Company.

13. **Conflict of Interest Guidelines. Code of Business Conduct and Ethics, and Anti-Corruption Policies**

I agree to diligently adhere to all policies of the Company, including the Company's insider trading policies, Conflict of Interest Guidelines, Anti-Corruption Policy, and Code of Business Ethics. Current copies of the Company's Conflict of Interest Guidelines, Anti-Corruption Policy, and Code of Business Conduct and Ethics are attached as Appendix C hereto, but I understand that these documents may be revised from time to time during my employment.

14. **Representations**

Without limiting my obligations under **Section 4.E** above, **I** agree to execute any proper oath or verify any proper document required to carry out the terms of this Agreement. I represent and warrant that my performance of all the terms of this Agreement will not breach any agreement to keep in confidence information acquired by me in confidence or in trust prior to my employment by the Company. I hereby represent and warrant that I have not entered into, and I will not enter into, any oral or written agreement in conflict herewith.

15. AUDIT

I acknowledge that I have no reasonable expectation of privacy in any Company Electronic Media Equipment or Company Electronic Media System. All information, data, and messages created, received, sent, or stored in Company Electronic Media Equipment or Company Electronic Media Systems are, at all times, the property of the Company. As such, the Company has the right to audit and search all such items and systems, without further notice to me, to ensure that the Company is licensed to use the software on the Company's devices in compliance with the Company's software licensing policies, to ensure compliance with the Company's policies, and for any other business-related purposes in the Company's sole discretion. I understand that I am not permitted to add any unlicensed, unauthorized, or non-compliant applications to the Company's technology systems, including, without limitation, open source or free software not authorized by the Company, and that I shall refrain from copying unlicensed software onto the Company's technology systems or using non-licensed software or websites. I understand that it is my responsibility to comply with the Company's policies governing use of the Company's documents and the internet, email, telephone, and technology systems to which I will have access in connection with my employment. In addition, as to any personal Electronic Media Equipment or personal Electronic Systems or other personal property that I have used for Company purposes, I agree that the Company may have reasonable access to such personal Electronic Media Equipment or personal Electronic Media Systems or other personal property to review, retrieve, destroy, or ensure the permanent deletion of Company information from such equipment or systems or property or take such other actions that are needed to protect the Company or Company property, as determined by the Company reasonably and in good faith.

I am aware that the Company has or may acquire software and systems that are capable of monitoring and recording all Company network traffic to and from any Company Electronic Media Equipment or Company Electronic Media Systems. The Company reserves the right to access, review, copy, and delete any of the information, data, or messages accessed through Company Electronic Media Equipment or Electronic Media Systems, with or without notice to me and/or in my absence. This includes, but is not limited to, all e-mail messages sent or received, all website visits, all chat sessions, all news group activity (including groups visited, messages read, and postings by me), and all file transfers into and out of the Company's internal networks. The Company further reserves the right to retrieve previously deleted messages from e-mail or voicemail and monitor usage of the Internet, including websites visited and any information I have downloaded. In addition, the Company may review Internet and technology systems activity and analyze usage patterns, and may choose to publicize this data to assure that technology systems are devoted to legitimate business purposes.

16. **Governing Law: Equitable Relief**

A. *Governing Law.* This Agreement will be governed by the laws of the state in which I am to be employed by the Company at the time I execute this Agreement as those laws apply to contracts entered into and wholly to be performed within such state.

B. *Administrative Relief.* I UNDERSTAND THAT THIS AGREEMENT DOES NOT PROHIBIT ME FROM PURSUING AN ADMINISTRATIVE CLAIM WITH A LOCAL, STATE, OR FEDERAL ADMINISTRATIVE BODY OR GOVERNMENT AGENCY THAT IS AUTHORIZED TO ENFORCE OR ADMINISTER LAWS RELATED TO EMPLOYMENT OR WORKERS' COMPENSATION, INCLUDING, BUT NOT LIMITED TO, THE EQUAL EMPLOYMENT OPPORTUNITY COMMISSION, THE NATIONAL LABOR RELATIONS BOARD, OR SIMILAR STATE AGENCIES. THIS AGREEMENT DOES, HOWEVER, PRECLUDE ME FROM PURSUING A COURT ACTION REGARDING ANY SUCH CLAIM, EXCEPT AS PERMITTED BY LAW.

C. *Voluntary Nature of Agreement.* I ACKNOWLEDGE AND AGREE THAT I AM EXECUTING THIS AGREEMENT VOLUNTARILY AND WITHOUT ANY DURESS OR UNDUE

INFLUENCE BY THE COMPANY OR ANYONE ELSE. I FURTHER ACKNOWLEDGE AND AGREE THAT I HAVE CAREFULLY READ THIS AGREEMENT AND THAT I HAVE ASKED ANY QUESTIONS NEEDED FOR ME TO UNDERSTAND THE TERMS, CONSEQUENCES, AND BINDING EFFECT OF THIS AGREEMENT AND FULLY UNDERSTAND IT, INCLUDING THAT *I AM WAIVING MY RIGHT TO A JURY TRIAL*. FINALLY, I AGREE THAT I HAVE BEEN PROVIDED AN OPPORTUNITY TO SEEK THE ADVICE OF AN ATTORNEY OF MY CHOICE BEFORE SIGNING THIS AGREEMENT.

17. **Miscellaneous**

A. *Assignability.* This Agreement will be binding upon my heirs, executors, assigns, administrators, and other legal representatives, and will be for the benefit of the Company, its successors, and its assigns. The Associated Third Parties are intended third-party beneficiaries to this Agreement with respect to my obligations in **Section 3.D.** Notwithstanding anything to the contrary herein, the Company may assign this Agreement and its rights and obligations under this Agreement to any successor to all, or substantially all, of the Company's relevant assets, whether by merger, consolidation, reorganization, reincorporation, sale of assets or stock, or otherwise.

B. *Entire Agreement.* This Agreement, together with the Appendices herein and any executed written offer letter between me and the Company, to the extent such materials are not in conflict with this Agreement, sets forth the entire agreement and understanding between the Company and me with respect to the subject matter herein and supersedes all prior written and oral agreements, discussions, or representations between us, including, but not limited to, any representations made during my interview(s) or relocation negotiations. I represent and warrant that I am not relying on any statement or representation not contained in this Agreement. Any subsequent change or changes in my duties, salary, compensation, conditions or any other terms of my employment will not affect the validity or scope of this Agreement.

C. *Headings.* Headings are used in this Agreement for reference only and shall not be considered when interpreting this Agreement.

D. *Reformation; Severability.* If a court or other body of competent jurisdiction finds, or the Parties mutually believe, any provision of this Agreement, or portion thereof, to be invalid or unenforceable, such provision will be enforced to the maximum extent permissible so as to effect the intent of the Parties, and the remainder of this Agreement will continue in full force and effect.

E. *Modification, Waiver.* No modification of or amendment to this Agreement, nor any waiver of any rights under this Agreement, will be effective unless in a writing signed by the President or CEO of the Company and me. Waiver by the Company of a breach of any provision of this Agreement will not operate as a waiver of any other or subsequent breach.

F. *Survivorship.* The rights and obligations of the Parties to this Agreement will survive termination of my employment with the Company.

G. *Applicability to Past Activities.* To the extent I have been engaged by the Company to provide services for a period of time prior to the date of this Agreement (the **"Prior Engagement Period"),** I agree that if and to the extent that, during the Prior Engagement Period: (i) I received access to any information from or on behalf of Company that would have been Company Confidential Information if I received access to such information during the period of my employment with the Company under this Agreement; or (ii) I conceived, created, authored, invented, developed or reduced to practice any item, including any intellectual property rights with respect thereto, that would have been an Invention if conceived, created, authored, invented, developed or reduced to practice during the period of my employment with the Company under this Agreement; then any such information shall be deemed Company Confidential Information hereunder and any such item shall be deemed an Invention hereunder, and this Agreement shall apply to such information or item as if conceived, created, authored, invented, developed or reduced to practice under this Agreement.

18. PROTECTED ACTIVITY NOT PROHIBITED

I understand that nothing in this Agreement shall in any way limit or prohibit me from engaging in any Protected Activity. For purposes of this Agreement, **"Protected Activity"** means disclosing Company Confidential Information if permitted by applicable state or federal laws, and filing a charge or complaint with, or otherwise communicating or cooperating with or participating in any investigation or proceeding that may be conducted by any federal, state or local government agency or commission, including the Securities and Exchange Commission, the Equal Employment Opportunity Commission, the Occupational Safety and Health Administration, and the National Labor Relations Board **("Government Agencies"). I** understand that in connection with such Protected Activity, I

am permitted to disclose documents or other information as permitted by law, and without giving notice to, or receiving authorization from, the Company. Notwithstanding, in making any such disclosures or communications, I agree to take all reasonable precautions to prevent any unauthorized use or disclosure of any information that may constitute Company Confidential Information to any parties other than the Government Agencies. I further understand that **"Protected Activity"** does not include the disclosure of any Company attorney-client privileged communications. In addition, I understand that under the U.S. Defend Trade Secrets Act of 2016,1 will not be held criminally or civilly liable under any U.S. federal or state trade secret law for the disclosure of a trade secret that is made in confidence to government officials, either directly or indirectly, or to an attorney, in each case solely for the purpose of reporting or investigating a suspected violation of law, or in a complaint or other document filed in a lawsuit or other proceeding, provided such filing is made under seal..

Date:

Signature

Name of Employee (typed or printed)

EXHIBIT A

LIST OF PRIOR INVENTIONS
AND ORIGINAL WORKS OF AUTHORSHIP

Title Identifying Number or Brief Date Description

No inventions or improvements Additional Sheets Attached

Date:

Signature

Name of Employee (typed or printed)

Exhibit 10.13

EXHIBIT B

SENTINELONE, INC. TERMINATION CERTIFICATION

This is to certify that I do not have in my possession, nor have I failed to return, any devices, records, data, notes, reports, proposals, lists, correspondence, specifications, drawings, blueprints, sketches, materials, equipment, any other documents or property, or reproductions of any and all aforementioned items belonging to SentinelOne, Inc. (the **"Company").** Notwithstanding the foregoing, **I** understand that I may keep a copy of the Employee Handbook and personnel records relating to me.

I further certify that I have complied with all the terms of the Company's At-Will Employment, Confidential Information, Invention Assignment, and Arbitration Agreement (the **"Agreement")** signed by me, including the reporting of any inventions and original works of authorship (as defined therein) conceived or made by me (solely or jointly with others), as covered by that Agreement.

I understand that pursuant to the Agreement, and subject to its Protected Activity exclusion, I am obligated to preserve, as confidential, all Company Confidential Information and Associated Third Party Confidential Information, including trade secrets, confidential knowledge, data, or other proprietary information relating to products, processes, know-how, designs, formulas, developmental or experimental work, computer programs, databases, other original works of authorship, customer lists, business plans, financial information, or other subject matter pertaining to any business of the Company or any of its employees, clients, consultants, or licensees.

I also acknowledge that under the Agreement, I am subject to certain restrictions for a period of time on my future employment, which restrictions are described in the Agreement at Section . I understand that nothing in this paragraph affects my continuing obligations under the Agreement during and after this restriction period, including, without limitation, my obligations under **Section 3** (Confidentiality) thereof.

After leaving the Company's employment, I will be employed by in the position of

Date:

Signature

Name of Employee (typed or printed)

Address for Notifications:

EXHIBIT C

CONFLICT OF INTEREST GUIDELINES

It is the policy of SentinelOne, Inc. to conduct its affairs in strict compliance with the letter and spirit of the law and to adhere to the highest principles of business ethics. Accordingly, all officers, employees, and independent contractors must avoid activities that are in conflict, or give the appearance of being in conflict, with these principles and with the interests of the Company. The following are potentially compromising situations that must be avoided:

1. Revealing confidential information to outsiders or misusing confidential information. Unauthorized divulging of information is a violation of this policy whether or not for personal gain and whether or not harm to the Company is intended. (The At-Will Employment, Confidential Information, Invention Assignment, and Arbitration Agreement elaborates on this principle and is a binding agreement.)

2. Accepting or offering substantial gifts, excessive entertainment, favors, or payments that may be deemed to constitute undue influence or otherwise be improper or embarrassing to the Company.

3. Participating in civic or professional organizations that might involve divulging confidential information of the Company.

4. Initiating or approving personnel actions affecting reward or punishment of employees or applicants where there is a family relationship or is, or appears to be, a personal or social involvement.

5. Initiating or approving any form of personal or social harassment of employees.

6. Investing or holding outside directorship in suppliers, customers, or competing companies, including financial speculations, where such investment or directorship might influence in any manner a decision or course of action of the Company.

7. Borrowing from or lending to employees, customers, or suppliers.

8. Acquiring real estate of interest to the Company.

9. Improperly using or disclosing to the Company any proprietary information or trade secrets of any other employer or other person or entity with whom obligations of confidentiality exist.

10. Unlawfully discussing prices, costs, customers, sales, or markets with competing companies or their employees.

11. Making any unlawful agreement with distributors with respect to prices.

12. Improperly using or authorizing the use of any inventions that are the subject of patent claims of any other person or entity.

13. Engaging in any conduct that is not in the best interest of the Company.

Each officer, employee, and independent contractor must take every necessary action to ensure compliance with these guidelines and to bring problem areas to the attention of higher management for review. Violations of this conflict of interest policy may result in discharge without warning.

Nothing in these guidelines is intended to limit employees' rights to discuss the terms, wages, and working conditions of their employment, as protected by applicable law. Also, nothing in these guidelines is intended to limit or prohibit employees from engaging in any Protected Activity. **"Protected Activity"** means filing a charge or complaint or complaint with, or otherwise communicating or cooperating with or participating in any investigation or proceeding that may be conducted by any federal, state or local government agency or commission, including the Securities and Exchange Commission, the Equal Employment Opportunity Commission, the Occupational Safety and Health Administration, and the National Labor Relations Board **("Government Agencies").** In connection with such Protected Activity, employees are permitted to disclose documents or other information as permitted by law, and without giving notice to, or receiving authorization from, the Company. Notwithstanding, in making any such disclosures or communications, employees must take all reasonable precautions to prevent any unauthorized use or disclosure of any information that may constitute

Company Confidential Information to any parties other than the Government Agencies. **"Protected Activity"** does not include the disclosure of any Company attorney-client privileged communications.

SENTINELONE, INC.
ANTI-CORRUPTION POLICY

PURPOSE

SentinelOne, Inc., including any of its subsidiaries or affiliates ("*SentinelOne*" or the "*Company")* is committed to promoting the highest standards of ethical business conduct and to compliance with all applicable laws, rules, and regulations. As part of this commitment, all SentinelOne employees, including individuals employed by or acting on behalf of SentinelOne, its officers and member of its board of directors, consultants, agents, other representatives and channel partners ("*Company Personnel and Partners*") are required to comply with the Foreign Corrupt Practices Act *("FCPA")*, the UK Bribery Act, other anti-bribery laws, and local laws designed to prevent improper bribes (collectively, all of these laws are referred to as the "*Anti-Corruption Laws").* The policies set forth in this document are referred to as the Company's "*Anti-Corruption Policy*." In addition to compliance with the Anti-Corruption Laws, all Company Personnel and Partners are required to comply with the Anti-Corruption Policy and any procedures adopted by the Company to implement this Policy.

PROHIBITED CONDUCT

SentinelOne and Company Personnel and Partners are prohibited from authorizing, making, offering, promising, requesting, receiving or accepting bribes or accepting kickbacks in any form. This prohibition applies to all forms of bribery, including commercial bribery as well as bribery of government employees or officials. The Anti-Corruption Laws prohibiting bribery are very broad, so that many kinds of gifts or entertainment provided to government employees or officials might be considered improper. For that reason, you may not give anything of value to any government employee or official in order to wrongfully influence the government employee or official, obtain or retain business or receive any improper advantage. This prohibition applies regardless of whether the payment or offer of payment is made directly to the government employee or official or indirectly through a third party. As discussed in more detail below, *it is critical to understand that, for purposes of the Anti-Corruption Laws, the terms "government official" generally includes any employee of a company that is owned or controlled by a government or governmental agency.* By way of example, this means that someone working for a telecom, energy company, internet company or hospital in another country that is owned or controlled by that country's government is a "government official." In other words, for purposes of the Anti- Corruption Laws, this term is much broader than how we think about "government officials" in the United States.

Examples of prohibited conduct include:

1. payments made directly to a government employee or official for an improper purpose;
2. payments or gifts to third parties where you know or have reason to know that at least a portion of the payments or gifts is likely to be offered by the third party to a government employee or official for an improper purpose;
3. acts "in furtherance of' an improper payment, such as arranging for funds to be available for the improper payment; and
4. payments to retain assets, such as an "under the table" payment to a tax official to settle a tax claim.

It is important to avoid even the appearance of impropriety. If you have any questions about whether a payment may be improper or violate this Policy, consult the Company's Compliance Officer before any payment or offer is made. *For purposes of the Anti-Corruption Policy, the Company's Chief Legal Officer serves as the Compliance Officer.*

IMPORTANT CONCEPTS

Who is a "government official"?

"Government official" includes:

1. any official or employee of a government, including any political party, administrative agency, or government-owned business; any person acting in an official capacity on behalf of a government entity;
2. employees or agents of a business which is owned or controlled by a government;
3. any person or firm employed by or acting for or on behalf of any government;
4. any political party official, employee or agent of a political party, or candidate for political office (or political party position); and
5. any family member or other representative of any of the above.

Any doubts about whether a particular person is a government official should be resolved by assuming that the individual involved is a government official for purposes of the FCPA or the Anti-Corruption Laws.

What does "*anything of value*" mean?

"Anything of value" includes money and monetary equivalents (such as gambling chips and gift cards), entertainment, accommodations, and any other benefit. There is no "minimum" required under the FCPA - any amount can be sufficient to trigger a violation.

What is an "improper advantage"?

An "improper advantage" includes payments intended to wrongfully:

1. influence a decision by a government official, including a failure to perform his or her official functions;
2. induce a government official to use his or her influence to affect a decision by

someone else in his or her government; and
3. induce a government official to use his or her influence to affect or influence any act or decision.

In addition to obtaining or retaining business, "improper advantage" includes reducing taxes, or duties, "looking the other way" at minor code or rule violations, and any form of preferential treatment.

GIFTS, ENTERTAINMENT, TRAVEL & PROMOTIONAL EXPENDITURES Gifts in the business context can be an appropriate way for business people to display respect for each other. SentinelOne expects the use of good judgment and moderation when giving or receiving entertainment or gifts. No gift or entertainment should ever be offered, given, provided or accepted by you unless it:

1. is reasonable and not extravagant;
2. is appropriate under the circumstances and serves a valid business purpose;
3. is customary and appropriate under U.S. and local customs;
4. is not being offered for any improper purpose, and could not be construed as a bribe, kickback or payoff;
5. does not violate any Company policy;
6. does not violate any U.S., local or international laws or regulations; and
7. is accurately described in your expense or other reports and Company's books and records.

It is essential that you accurately report expenditures for gifts or entertainment so that the purpose, amount, and recipient of the gift are obvious *{i.e.,* transparent) to personnel in the Company's Finance Department and other personnel who have responsibility for ensuring that our financial books and records are accurate and reviewing these books and records. Expense reports should accurately state the purpose of the expenditures and the identities of the individuals receiving the gifts or entertainment and state whether the gift or entertainment was given to a government employee or official.

Significant legal restrictions apply with regard to providing gifts, entertainment, travel and promotional expenditures related to government officials. You must make sure you fully understand all such restrictions and associated policies and procedures. In each instance:

1. all gifts, entertainment, or promotional expenses which are intended to induce a government employee or official to misuse his or her position or to obtain an improper advantage are prohibited, regardless of their value;
2. expenses must have a valid business purpose and be reasonable and necessary under the circumstances;
3. gifts must be of token value (such as shirts or tote bags that reflect Company's business name and/or logo), legal and customary, and openly given; and
4. expenses and gifts must be fully and accurately reflected in the Company's books and records and backed by receipts.

You should avoid even the appearance of impropriety. Any gift or expense that is lavish or might otherwise prove embarrassing for the Company is prohibited. If you have any question regarding the appropriateness of any gift or expense, you should consult the Compliance Officer prior to giving the gift or incurring the expense.

FACILITATING PAYMENTS The FCPA and other anti-bribery laws may provide limited exceptions for certain minor payments for the purpose of facilitating or expediting routine, lawful services or nondiscretionary administrative actions, such as telephone installation. However, other anticorruption laws prohibit such payments. Any and all facilitating payments require prior written approval from the Compliance Officer.

REPRESENTATIVES, PARTNERS, CONSULTANTS, DISTRIBUTORS, AGENTS AND OTHER THIRD PARTIES

Before initiating a relationship with a representative, partner, consultant, distributor, agent, or other third party, you must conduct appropriate due diligence to assure yourself that the representative will not engage in any improper conduct. *This is for several important reasons**,** including that the Company can be held responsible for a third party's conduct in certain circumstances under the Anti- Corruption Laws.* Due diligence typically will include considering such factors as:

1. the third party's qualifications for the position or task at issue;
2. whether the third party has personal or professional ties to the government or any government official;
3. the number and reputation of the third party's clientele and the representative's reputation with the United States Embassy or Consulate, local bankers, clients, and other business associates; and
4. the reasonableness of the compensation.

Consult the Compliance Officer regarding the appropriate due diligence procedure for your situation.

The Company must terminate contracts with any third party who is unwilling or unable to represent the Company in a manner consistent with this Anti-Corruption Policy.

RED FLAGS RELATED TO THIRD PARTIES While conducting due diligence and throughout any

subsequent relationship with third parties, you must monitor for any "red flags." A "red flag" is a fact or circumstance that requires additional consideration and extra caution. Red flags must be considered in context rather than in isolation. Red flags may appear in many forms and can include:

1. payments in a country with a history or reputation for corruption;
2. refusal to provide a certification of compliance with the FCPA or other anti-bribery laws;
3. unusual payment patterns or requests, including payments to third parties, in cash, and payments made to bank accounts outside the country;
4. representations or boasting about influence or connections;
5. use of a shell or holding company that obscures ownership without credible explanation;
6. accusations of improper business practices (credible rumors or media reports, etc.);
7. family or business relationship with the government or a government official;
8. requests for payments "up front" or statements that a particular amount of money is needed to "get the business," "make the necessary arrangements," or similar expressions;
9. unusually high commissions, agents' fees, or payments for goods or services;
10. apparent lack of qualifications or resources;
11. whether the representative or joint venture partner has been recommended by an official of the potential government customer;
12. requests to be able to make agreements without the Company's approval; and
13. requests that agreements or communications be kept secret (other than a customary nondisclosure or confidentiality agreement).

You are responsible for monitoring your email and other communications and documents for red flags. Any red flags should be brought promptly to the attention of your supervisor or the Compliance Officer. Failure to do so is considered a violation of this Anti-Corruption Policy.

POLITICAL CONTRIBUTIONS

The Company reserves the right to communicate its position on important issues to elected representatives and other government officials. It is, however, always the Company's policy to comply fully with all applicable laws regarding political contributions. Donations to political campaigns or causes could violate campaign finance laws and Anti-Corruption Laws, especially if contributions are made to a campaign at the request or suggestion of a government official.

To mitigate the risk of an improper payment or the appearance of an improper payment, no Company funds, facilities, or services of any kind may be provided to any government official, including any candidate or prospective candidate for public office, to any political party, or to any political initiative, referendum, or other form of political campaign unless pre-approved in writing by the Compliance Officer.

CHARITABLE CONTRIBUTIONS

The Company is committed to improving and promoting the interests of the communities where it operates. Donations to charitable organizations, however, can, like political contributions, present a risk under the Anti-Corruption Laws, particularly if they are made at the request or suggestion of a government official. Therefore, you must obtain prior written approval from the Compliance Officer before making any charitable donation on behalf of the Company or using Company funds, directly or indirectly.

BOOKS AND RECORDS

All employees must maintain accurate records of all transactions and assist in ensuring that the Company's books and records accurately and fairly reflect, with appropriate detail, all transactions, expenses, or other dispositions of assets. To that end, every employee is prohibited from falsifying any business or accounting record and must truthfully report and record all dispositions of assets. Undisclosed or unrecorded funds or assets—for any purpose—are prohibited.

Any questions on how to record transactions should be referred to the Compliance Officer.

In addition to the guidelines set forth above, all employees must comply with the Company's Code of Business Conduct and Ethics.

REPORTING BREACHES OF THIS ANTICORRUPTION POLICY

Compliance with this Anti-Corruption Policy is, first and foremost, the individual responsibility of each and every employee. All Company Personnel and Partners must report, in person or in writing, any known or suspected violations of this Policy to the Compliance Officer or in a manner consistent with the Company's Whistleblower Policy. Per the Company's Whistleblower Policy, concerns regarding improper or illegal conduct can be reported in several ways, including by: (i) reporting the known or suspected violation to your manager and/or

supervisor; (ii) reporting your concerns to the Compliance Officer at ethicshelp@sentinelone.com: (iii) calling the Company's Whistleblower Reporting Hotline at (650)-537-2443 and/or by letter addressed to the Company's Audit Committee or Legal Department, sent c/o SentinelOne, Inc., 444 Castro Street, Suite 400, Mountain View, California 94041; Attention: Audit Committee or Chief Legal Officer.

You can also submit any questions you may have regarding the Anti-Corruption Policy to the Company's Whistleblower Reporting Hotline number or email address. Any questions or reports of concerns regarding improper or illegal conduct will be addressed promptly, and can be made anonymously.

SentinelOne will not allow any retaliation against any Company employee who acts in good faith in reporting any violation of this Policy. The Company encourages and highly values reporting of conduct that may violate the Anti-Corruption Laws. Per the Company's Whistleblower Policy, the Company will investigate reported violations and will determine an appropriate response, including corrective action and preventative measures as appropriate. For further information regarding the manner in which the Company handles reports related to concerns of improper or illegal conduct, please review the Company's Whistleblower Policy.

PERIODIC REVIEW

The Compliance Officer or a designee will conduct a periodic review to confirm the adequacy and effective implementation of this Anti-Corruption Policy.

CERTIFICATION AND ENFORCEMENT

From time to time, SentinelOne personnel may be required to complete training regarding the FCPA and, more broadly, the Anti-Corruption Laws and sign a certification acknowledging commitment to, full understanding of, and compliance with this Anti-Corruption Policy. The acknowledgment statement shall be included in the personnel file of each such employee. Any Company Personnel or Partners who violate this Policy or who fail to make or falsify any certification required under this Policy may be subject to disciplinary action, up to and including termination of employment or of the business relationship.

Exhibit 10.13

SENTINELONE, INC.

EMPLOYEE CERTIFICATION REGARDING COMPLIANCE WITH
ANTI-CORRUPTION POLICY

I have read and understand the Anti-Corruption Policy (the "*Anti-Corruption Policy*") of SentinelOne, Inc. ("*SentinelOne*" or "*Company").* I undertake to comply with the provisions of the Policy. I hereby represent that:

1. Except as disclosed below, I have not participated in, and am not aware of, any violation of the Foreign Corrupt Practices Act ("*FCPA*") or the Anti-Corruption Policy by myself or any other employee, agent, individual, or entity acting on behalf of or as a representative, channel partner, vendor, consultant, or business partner of SentinelOne. I hereby represent that:

o I have not paid, offered, promised to pay (or authorized any payment or offer of) money or anything of value, directly or indirectly, to any government employee or official in order to wrongfully influence the government official, obtain or retain business, direct business to any person, induce a government official to use his or her influence to affect or influence any act or decision, or receive any improper advantage.

o I am not aware of, and have no reason to believe that, any employee, agent, individual, or entity acting on behalf of or as a representative, channel partner, vendor, consultant, or business partner of SentinelOne has paid, offered, promised to pay (or authorized any payment or offer of) money or anything of value, directly or indirectly, to any government employee or official in order to wrongfully influence the government employee or official, obtain or retain business, direct business to any person, induce a government employee or official to use his or her influence to affect or influence any act or decision, or receive any improper advantage.

1 I shall not pay, offer, promise to pay (or authorize any payment or offer of) money or anything of value, directly or indirectly, to any government employee or official in order to wrongfully influence the government official, obtain or retain business, direct business to any person, induce a government official to use his or her influence to affect or influence any act or decision, or receive an improper advantage.

2. Should I ever obtain information giving me reason to believe that any employee, agent, individual, or entity acting on behalf of SentinelOne may have engaged in conduct that violates the FCPA or the Anti-Corruption Policy, I undertake to report that information promptly to the Compliance Officer of the Company.

2 have engaged in or observed the following incidents of potential non-compliance:

I understand that a false, misleading or incomplete statement in this certification of compliance or other violation of the Anti-Corruption Policy may be grounds for termination of employment or of the business relationship.

Date: Signature: Name printed:
Title:

Office:

SENTINELONE, INC.
CODE OF BUSINESS CONDUCT AND ETHICS

PURPOSE

Our integrity and professionalism have been the cornerstone of our business. In all that we do SentinelOne, Inc. (the *"Company"* including any of its subsidiaries) supports and upholds a set of core values and principles. The success of our business depends on each of us understanding these values and principles and continuously demonstrating the uncompromising integrity that is the foundation of our company.

Each of us has a responsibility to act with integrity - both in terms of how we treat each other, and in terms of how we run our business. This Code of Business Conduct and Ethics *("Code")* is intended to serve as a guide to help you answer potential legal and ethical questions that may arise. However, no policy can address or anticipate every situation you might face. If you have a question about any course of conduct, consult your supervisor or our Chief Legal and Trust Officer before proceeding.

As our Code establishes our policy framework, all our employees, directors and officers are required to read and comply with our Code. Please note that the Company has additional policies that cover other specific topics that you should also read and familiarize yourself with. These additional policies include:

- Anti-Corruption Policy;
- Corporate Communications Policy;
- Insider Trading Policy;
- Related Party Transactions Policy;
- Social Media Guidelines; and
- Whistleblower Policy.

OUR CULTURAL VALUES

- *Trust.* Be dependable. Conduct yourself with the highest integrity at all times.
- *Accountability.* Be reliable in all your actions and words. Put customers first. Be the owner!
- *OneSentinel.* Be passionate about driving team success and collaboration across our company.
- *Relentlessness.* Act with unwavering purpose and determination in everything you do.
- *Ingenuity.* Encourage innovative approaches to problem-solving and market leadership. Embrace diverse perspectives. Hustle!
- *Community.* Be kind to one another. Think about how your actions will affect others. Together with your team you can achieve more.

PERSONS COVERED BY THIS POLICY

This Code applies to our employees, contractors, consultants, agents, representatives, officers and members of our Board of Directors *("Board").*

MAKING THE RIGHT DECISION

In evaluating your conduct, it is useful to ask the following questions:

- Purpose.
  - o Why am I doing this?
  - o Is it legal? Even if it is legal, is it the right thing to do?
- Process.
  - o Did I follow the right steps? o Did I consult the right experts or stakeholders?
- Perception.
  - o How would this look to our customers, regulators, employees or the media?
  - o How would this look in three to four years in the future?

If you ever are in an uncomfortable situation or have any doubt about whether a situation is consistent with our ethical standards or complies with the law, please seek help from your manager or our Chief Legal and Trust Officer. If you would like to remain anonymous, please refer to our Whistleblower Policy for instructions on how to report a situation or seek help anonymously.

DOING OUR JOBS WITH INTEGRITY

The Company expects each of you to strive for excellence and work with integrity in all you do. It is unacceptable to cut ethical or legal comers for any reason.

Exhibit 10.13

HONEST AND ETHICAL CONDUCT

Conflicts of Interest

You must act within guidelines that prohibit real and potential conflicts of interest with your role at the Company. Generally, conflicts of interest are situations that divide your loyalty between the Company, on the one hand, and your own personal interests, on the other. Determining whether a conflict of interest exists is not always easy to do. Even the appearance of a conflict of interest could create a problem. Before engaging in any activity, transaction or relationship that might give rise to a conflict of interest, you must first notify your manager or our Chief Legal and Trust Officer or, if you are a Board member, to the Chair of the Audit Committee of the Board *(*"*Audit Committee*"), and then receive written approval to engage in the activity, transaction and/or relationship.

The following are examples of types of situations that could present potential conflicts of interest and should be disclosed:

- **Conflicting Employment:** You or a family member is working or consulting for a competitor or potential competitor.
- **Hiring Related Parties:** Hiring or supervising family members or others with whom you have a close, personal relationship.
- **Business Transactions with Related Parties:** Awarding Company business to a company owned or controlled by an employee of the Company or a member of his or her family.
- **Board or Advisory Service:** Serving as a board member or advisor for an outside company or organization.
- **Investments:** Owning or having a substantial interest in a competitor, supplier or contractor.
- **Gifts:** Accepting gifts, discounts, favors or services from a customer/potential customer, vendor or supplier, unless equally available to all Company employees.
- **Interested Party Transactions:** Taking personal advantage of the Company's business opportunities.
- **Company Loans:** Receiving a loan or guarantee from the Company benefitting you or your family member.

You must always get approval from our Chief Legal and Trust Officer before participating in any transaction that could result in a potential conflict of interest. Conflicts of interest are fact-specific. For example, you may accept an approved gift from a vendor, but if you then decide to do business with that vendor without evaluating others, there could be a potential conflict of interest. When in doubt about any potential conflict of interest, contact our Chief Legal and Trust Officer.

Outside Employment

You may not engage in any outside employment that would interfere with your job performance or responsibilities. You must inform your manager, as well as our Chief Legal and Trust Officer, before you take on any outside employment that might cause a potential conflict.

Personal Relationships

Being in a personal relationship (e.g., dating, living together, etc.) with another employee (regular or temporary/contingent), applicant or contractor can possibly create a conflict of interest if that relationship might affect your judgment or appear to impact your judgment. If you have questions, our Chief Legal and Trust Officer can help. A personal relationship between a supervisor and an employee who is a direct report to the supervisor, or over whom the supervisor has the ability to influence the terms and conditions of employment, must in all circumstances be disclosed immediately to the Chief Legal and Trust Officer.

Business with Related Parties

You should avoid conducting any Company business with a relative or significant other, or with a business with which you, a relative or significant other is significantly associated. A potential conflict of interest can arise if you direct business from the Company to these types of related parties. To prevent a conflict of interest, employees directing business to or from the Company should discuss the situation with their manager and remove themselves from the decision-making process.
Even if a related-party transaction appears to be in the Company's best interests, you must first fully disclose the transaction to our Chief Legal and Trust Officer, and receive approval from our Audit Committee, before engaging in that transaction. If you discover after the fact that we have done business with a related party, you must promptly report it to our Chief Legal and Trust Officer, who will refer the matter for approval from our Audit Committee. Please also refer to our Related Party Transactions Policy for more information.

Outside Advisory or Board Service

You must obtain approval from our Chief Legal and Trust Officer for certain outside activities that could present an actual or potential conflict of interest with your professional responsibilities at the Company. For example, serving on advisory boards or boards of directors, or being appointed to industry groups may present actual or potential conflicts. Board members must notify our Nominating and Corporate Governance Committee in advance of accepting a new board membership or a change in their principal occupation in accordance with our Governance Guidelines and shall avoid accepting board memberships or positions that would present a conflict of interest. Employees must disclose to their manager, in advance, outside activities that may or will impact the employee's ability to perform the essential functions of their position at the expected level.

Investments and Business Interests

If you, a relative or a member of your household (including a roommate) are considering investing in one of our suppliers, vendors, customers or competitors, take great care to make sure that the investment does not compromise your obligations as our employee.

Things to consider in determining whether there is a real or seeming conflict:

- The size and nature of your investment;
- Your ability to influence the Company's decision;
- Your access to our confidential information; and
- The nature of the relationship between us and the other company.

Meals, Gifts, and Entertainment
We highly encourage the building of strong relationships and socializing with customers, vendors, distributors and suppliers is an integral part of building important business relationships. However, good judgment should be exercised in providing business meals and entertainment or inexpensive gifts, so that all such conduct is consistent with customary and prudent business practices. Please do not solicit or request any gift and do not give or accept any gift that would affect or influence, or give the appearance of affecting or influencing, the business relationship at hand or your judgment in carrying out your duties and responsibilities for the Company. You may never use personal funds or resources to do something that cannot be done with Company resources, and you also are not allowed to lower the value of a gift by absorbing a portion of the cost yourself.

In addition, you should avoid any actions that create a perception that the Company sought or received favorable treatment from other entities or people in exchange for business courtesies such as gifts, gratuities, meals, refreshments, entertainment or other benefits. On occasion, you may be offered a gift, travel, or other compensation by someone in connection with the work you do here at the Company. A good rule of thumb to use in considering whether to accept the gift is whether you would be comfortable telling your manager about the gift or having your acceptance of it known by the public.

Corporate Opportunities

You may not take advantage of or direct a third party to take advantage of any opportunities discovered through your job with the Company for personal gain, or for the personal gain of a roommate, close friend, relative or significant other, unless the opportunity is disclosed to and pre-approved by our Chief Legal and Trust Officer. These opportunities include, among others, the Company's sales and other business development opportunities, inventing products or services and writing books.

You are further prohibited from competing with the Company directly or indirectly during your employment with the Company and as otherwise provided in any written agreement with the Company.

Loans

Under U.S. Securities and Exchange Commission ("*Commission*") rules, we are not allowed to provide loans (or guarantee loans) to our executive officers and directors or their family members. The Compensation Committee of the Board must approve any Company loan to any other service provider.

COMPLYING WITH THE LAW

Everyone at the Company is expected to comply with the law. Laws can be complex and at times, even counterintuitive. Although it's impossible to know all aspects of every law, you should understand the major laws, rules and regulations that apply to your work. You should consult with our Chief Legal and Trust Officer if you are unsure or have any questions or concerns related to your work. A few specific areas of legal compliance are discussed in greater detail below.

Insider Trading

Because we believe firmly in transparency and trust across the organization, you may find yourself in possession of inside information. The definition of inside information is any material nonpublic information, positive or negative, about the Company or other organizations with which we work. For a definition of "material non-public information," please see the Company's Insider Trading Policy. Remember that we also may possess confidential information about our customers, partners or other third parties. It is equally important that we treat this information with the same care that we treat our own.

The bottom line is that we never buy or sell securities based on inside information, nor do we tip off others to do so. It doesn't matter how we learned the information—using material nonpublic information to trade securities is never acceptable. Doing so violates the law and the trust we have built with our fellow employees, and with our customers, partners and investors, and others.

To learn more, please review our Insider Trading Policy, which explains how you lawfully can trade in our stock, as well as our trading windows, blackout periods and trading plans.

No Bribery or Corruption

All forms of bribery and corruption are prohibited. We will not tolerate bribery or corruption in any form or for any purpose. There is no potential benefit that can justify damaging our integrity and reputation or the trust others place in us.
All persons subject to this Code must comply fully with the Foreign Corrupt Practices Act (FCPA) and other applicable laws that prohibit bribery and corruption. Many of these laws are very broad and apply to both government and private or commercial bribery and corruption.

You are responsible for ensuring that you understand the applicable laws and our Anti-Corruption Policy. If you have a question regarding any gift, entertainment or other expense, consult with our Chief Legal and Trust Officer before you incur or authorize the expense.

Unlawfully Obtaining Business Intelligence

Gathering information about our competitors, often called competitive intelligence, is a legitimate business practice. It helps us stay competitive. However, we must always obtain business intelligence appropriately from legitimate sources. You must not steal or unlawfully use the information, material, products, intellectual property or proprietary or confidential information of others, including that of business partners and customers. These rules also apply to consultants, vendors and other partners we retain.

Fair Sales and Marketing Practices

We compete vigorously for business based solely on the merits of our products and services. We do not participate in any activities that unfairly harm competition. We want to win, but win fairly.

We will accurately represent the Company and our products and services in our marketing, advertising and sales materials. We can promote our products and services and make comparisons between us and our competitors.

Deliberately misleading messages, leaving out important facts or false claims about our products and services or competitors are inconsistent with our policies.

Antitrust laws govern relationships between a company and its competitors. Collusion among competitors is illegal and the consequences of a violation are severe. You must not enter into an agreement or understanding of any kind with competitors concerning prices, discounts or other terms or conditions of sale; profits or profit margins; costs; allocation of products, services, customers, markets or territories; boycotts of customers or suppliers; or bids or the intent to bid or even discuss or exchange information on these subjects.

Selecting Suppliers

We rely on our supplier relationships for our success. To achieve our mission, we need suppliers that are as committed as we are to building trust with our customers, that will do great work, and that will follow the law. We select the best suppliers for the job, by carefully considering their proven track record, reputation for integrity, and other merits—not based on favoritism. We work to eliminate child labor, human trafficking, and other labor abuses in our supply chain.

RESPECTING HUMAN RIGHTS

We are committed to respecting human rights to ensure that our business plays a positive role in the communities in which we operate. We respect human rights by seeking to avoid infringing on the rights of others and working to address adverse human rights impacts with which we are involved. We expect employees, partners, suppliers, customers and governments to share this commitment.

FINANCIAL MATTERS AND BUSINESS PRACTICES

You are expected to act responsibly and exercise sound judgment with respect to our finances and financial reporting. Investors rely on accurate and fair financial and business information to understand our financial results and make informed decisions. You may execute financial transactions only with authorization and in compliance with our policies. You also are expected to record and report all financial transactions and business information honestly and accurately, to comply with our system of internal controls and to follow applicable laws, regulations and accounting practices.

We regularly file reports and other documents with regulatory authorities, including the Commission. In addition, we may make other public communications, such as press releases, from time to time.

Depending upon your position with the Company, you may be called upon to provide information to help ensure that our public reports and communications are complete, fair, accurate and understandable. You are expected to use all reasonable efforts to provide complete, accurate, objective, relevant, timely and understandable answers to inquiries related to our public disclosures. Employees involved in preparing public reports and communications must use all reasonable efforts to comply with our disclosure controls and procedures.

If you believe that any disclosure is materially misleading or if you become aware of any material information that you believe should be disclosed to the public, it is your responsibility to bring this information to the attention of our Chief Legal and Trust Officer. If you believe that questionable accounting or auditing conduct or practices have occurred or are occurring, you should follow the procedures set forth in our Whistleblower Policy.

Commission Reporting and Financial Statement Preparation

Our periodic reports and other documents filed with the Commission, including all financial statements and other financial information, must comply with applicable federal securities laws, and Commission rules. If you contribute in any way to the preparation or verification of our financial statements and other financial information, you must ensure that our books, records and accounts are accurately maintained. You must also cooperate fully with our finance department, as well as our independent public accountants and counsel. If you are involved in the preparation of our Commission reports or financial statements, you must:

- Be familiar with and comply with our disclosure controls and procedures and our internal control over financial reporting.
- Take all necessary steps to ensure that all filings with the Commission and all other public communications about our financial and business condition provide full, fair, accurate, timely and understandable disclosure.

Quarterly Compliance Certifications

Depending on your position here at the Company, we may ask you to certify your knowledge of various facts each quarter. We rely on certifications to record transactions, make legal and accounting determinations and comply with laws. If you do not provide a certification or complete a certification completely, honestly and accurately, you may be in violation of this Code. This will result in disciplinary action up to and including termination of your service with the Company.

Business Expenses

You are expected to incur business expenses wisely. When you submit an expense for reimbursement or spend money on our behalf, you must make sure that the cost is reasonable, directly related to our business.
supported by appropriate documentation and in compliance with our policies. Always submit expense reports in a timely manner, record the business purpose and relevant details and comply with all submission requirements. If you are uncertain about whether you should spend money or submit an expense for reimbursement, check with your manager. Managers are responsible for all money spent and expenses incurred by their direct reports and should carefully review such expenses and supporting receipts before approving.

Money-laundering and Third-party Payments

We are committed to complying fully with all anti money-laundering and antiterrorism laws throughout the world. Money laundering occurs when individuals or organizations attempt to conceal illicit funds or make such funds look legitimate. If you are requesting payments to vendors or potential vendors, or are monitoring payments we receive, you must flag suspicious activity. The following examples may be indications of potential money laundering:

- Attempts to make large cash payments.
- Payments by or to someone who is not a party to the relevant contract.
- Requests to pay more than provided for in the relevant contract.
- Payments made in currencies other than those specified in the relevant contract.
- Payments from an unusual, non-business account.

USING AND PROTECTING OUR ASSETS, SYSTEMS AND FACILITIES *Access to Our Offices*
Each Company office has policies to ensure the security and confidentiality of our communications, protect our assets from theft, misuse or destruction and keep you and any guests safe. All employees are responsible for complying with these policies and with all related systems.

Computers and Other Equipment

You must care for any equipment provided by the Company (such as your laptop computer) and use it responsibly for business purposes. You may make limited personal use of our equipment, provided such use does not interfere with our business or violate any law or Company policy. If you use any Company equipment at a location outside of our offices, you need to take precautions to protect the equipment from loss, theft or damage. All Company equipment must be fully accessible to us and remains our property, even while in your possession. You have no right to privacy in our personal equipment (including laptop computers provided to you) or to any personal information stored on that equipment. You may not use your own equipment for Company work without advance permission from your manager and only in compliance with all policies relating to the use of such equipment.

Software and Content

All software you use in your work for the Company must be appropriately licensed and approved. Any non- licensed software should be removed. It is against our policy to make, use or share illegal or unauthorized copies of software or other copyrighted material.

Retaining Records

Our records and information are important assets that comprise our corporate memory and contain information critical to the continuity of our business. These documents or records include not only transaction records, but other electronic records, such as e-mail, voicemail, messaging apps and computer drives. You must manage business records and dispose of them only in the manner and timeframe established by our document retention policies. Please be especially cautious with records and information that are subject to a "legal hold," which may be imposed under certain circumstances such as litigation or government investigations. When there is a "legal hold" in place, you may not alter, destroy or discard documents relevant to the lawsuit, legal proceeding or investigation.

Protecting Information and Intellectual Property (IP)

The innovations you create every day are vital to our success. We expect you to understand the value of these innovations and to take appropriate steps to protect them. This means disclosing to the Company all inventions and other IP created or improved as part of your work for us, assisting with the preparation and prosecution of patent applications, protecting confidential information and avoiding the improper use of third-party confidential information or IP.

Disclosing Confidential Information About the Company and Others

We sometimes must disclose our confidential information in the course of performing our jobs. If you need to disclose confidential information belonging to the Company, you first must ask our legal department to work with the other party to sign an approved non-disclosure agreement *("NDA").* In addition, you should not discuss sensitive matters or confidential information in public places.

If a third party has disclosed confidential information to you or the Company under an NDA, we must comply with the terms of the NDA and limit our use of the confidential information to the specific purpose for which it was intended.

You should never attempt to obtain a competitor's confidential information improperly. This includes asking another employee to disclose confidential information they received while working at another company.

If you obtain another company's confidential information accidentally or from an unknown source, it may be unethical or even illegal to use the information. You should immediately contact our Chief Legal and Trust Officer to determine how to proceed.

Data Privacy

Trust is the foundation of our relationship with our customers. We value the confidence our customers have in us and take the responsibility of protecting their information seriously. To be worthy of their trust, we built, and will continue to grow, the Company with an emphasis on security, compliance and privacy.

Requests by Regulatory Authorities

Stewardship of the data we receive from other parties, including customers, suppliers and vendors, is a responsibility we embrace. All government requests for our information, documents or interviews of our employees should be referred to our legal department immediately. This does not prevent you from providing information to a government or law enforcement agency if you reasonably believe that the information discloses a legal violation by us or our agents.

COMMUNICATING WITH OTHERS

We are committed to providing accurate, timely and clear disclosure in our public communications. Because any external communications can affect our business, you must be thoughtful and conscientious about what you say and write in public on the Company's behalf. In general, only people who have been specifically authorized may speak on behalf of the Company without prior approval. If you are approached by anyone such as a member of the press,

analyst, or current or potential investor of the Company, please refer the individual to our public relations team. For additional information, please refer to our Corporate Communications Policy.

A PLACE WHERE YOU CAN DO YOUR BEST WORK

We are committed to fostering an environment where ALL people are welcome and supported. We respect and value different experiences and viewpoints. We always act respectfully toward one another and embrace diversity of people and ideas. Having a diverse workforce made up of team members who bring a wide variety of skills, abilities, experiences and perspectives is essential to our success. Creativity and innovation flourish in an environment of openness, inclusion and mutual respect.

Authenticity and Inclusion

We are more productive, more creative and happier when each of us can be our authentic self. We act as a team that embraces different perspectives, seeks innovation from everywhere, and enables our colleagues, our customers and our communities to change the world. We value groundbreaking thinking and new ways of approaching problems—and we know that to solve the most complex problems, we need to attract the most creative, innovative and committed people from across the globe.

Fair Employment Practices

We are committed to providing equal employment opportunities for all applicants and employees. We do not unlawfully discriminate in employment opportunities (such as hiring or promotions) or practices (such as discipline, compensation or benefits) on the basis of any protected characteristic, including race, color, religion, sex, gender identity or expression, transgender status, genetics, marital or veteran status, age, national origin, ancestry, physical disability (including HIV/AIDS), mental disability, medical condition, pregnancy or childbirth (including breast-feeding), sexual orientation or any other characteristic protected by law. Additionally, every Company employee has a right to a work environment free from unlawful harassment. Harassment can include any behavior (verbal, visual or physical) that creates an intimidating, offensive, abusive or hostile work environment.

We will promptly address reports of discrimination or harassment. If you believe you've observed or been subjected to discrimination or harassment in violation of our policies, you should immediately contact your manager, Human Resources, our Chief Legal and Trust Officer, or any manager with whom you feel comfortable. If you conclude that you can only report these violations anonymously, please follow the procedures in our Whistleblower Policy. We will not retaliate against any employee for bringing a complaint in good faith or participating in any investigation in good faith and we will not tolerate retaliation by others. You should report any concerns about retaliation immediately. See "No Retaliation" below.

Safety and Security

We expect you to treat others fairly and with respect and to be professional at all times. We promote and provide a work environment free of violence and we are committed to the safety and security of our employees and property. We will not tolerate threats of violence, acts of aggression, intimidation or hostility. You may not possess firearms, other weapons, explosive devices or dangerous substances or materials in the workplace. Any potentially dangerous situation must be reported immediately to our Chief Legal and Trust Officer.

Cooperating with Investigations

We will conduct investigations of alleged or actual violations of our policies, procedures and laws, rules and regulations. All persons subject to this Code are required to cooperate with any Company investigation. All persons subject to this Code are expected to maintain and safeguard the confidentiality of an investigation to the extent possible, except as otherwise provided herein or by applicable law.

PENALTIES FOR VIOLATIONS OF COMPANY POLICIES

You are expected to be familiar with and comply with all Company policies. If you have a question regarding any course of conduct, consult your supervisor or the Chief Legal and Trust Officer before moving forward. Those who

violate our policies are subject to disciplinary action up to and including termination of employment. Examples of misconduct that may result in disciplinary measures includes:

- Violating any Company policy;
- Failing to report known or suspected violations of any Company policy;
- Failure to cooperate in a Company investigation into possible violations of Company policies; and
- Engaging in retaliation.

Furthermore, violations of some provisions of this Code are illegal and may subject persons subject to this Code to civil and criminal liability.

REPORTING CONCERNS

If you have a concern about any actual or possible violations of this Code or any of our policies, you are required to report it promptly. You may raise any concern orally or in writing through several channels. Use the channel that is most comfortable for you. Your supervisor or manager is often in the best position to resolve a concern quickly. However, you can always report a concern to the Company's Chief Legal and Trust Officer or their designee, the next level of management or anonymously. Consult the process set forth in our Whistleblower Policy for additional ways to report concerns.

NO RETALIATION

We will not tolerate any reprisals or retaliation against any person raising a concern or participating in any investigation in good faith.

CHANGES TO THIS CODE

Our Board reserves the right in its sole discretion to modify or grant waivers to this Code. Any such modification or waiver must be approved in writing. Any amendments or waiver for the principal executive officer, principal financial officer, principal accounting officer, controller, or any other persons performing similar functions in the company will be publicly disclosed if and as required by applicable laws, rules and regulations.

Exhibit 10.13

EXHIBIT B

SENTINELONE, INC.

CHANGE IN CONTROL AND SEVERANCE AGREEMENT

This Change in Control and Severance Agreement (the **"Agreement")** is entered into by and between Vats Srivatsan, (the **"Executive")** and SentinelOne, Inc., a Delaware corporation (the **"Company"),** on [•], 2022, and is effective as of [•] 2022 (the **"Effective Date").**

1. **Term of Agreement.**

Except to the extent renewed as set forth in this Section 1, this Agreement shall terminate upon the earlier of (x) the third (3rd) anniversary of the Effective Date (the **"Expiration Date")** or (y) the date that Executive's employment with the Company terminates for a reason other than Executive's Qualifying Termination or CIC Qualifying Termination; *provided however,* if a definitive agreement relating to a Change in Control has been signed by the Company on or before the Expiration Date, then this Agreement shall remain in effect through the earlier of:

(a) The date that Executive's employment with the Company terminates for a reason other than a Qualifying Termination or CIC Qualifying Termination, or

(b) The date the Company has met all of its obligations under this Agreement following a termination of Executive's employment with the Company due to a Qualifying Termination or CIC Qualifying Termination.

This Agreement shall expire on the initial Expiration Date and each subsequent Expiration Date, unless the Company provides Executive notice of renewal at least three (3) months prior to the date on which this Agreement would otherwise expire, in which case this Agreement shall remain outstanding and effective for an additional three (3) year term. For the avoidance of doubt, and notwithstanding anything to the contrary in Section 2 or 3 below, the Company's non-renewal of this Agreement shall not constitute a Qualifying Termination or CIC Qualifying Termination, as applicable.

2. **Qualifying Termination.** If Executive is subject to a Qualifying Termination, then, subject to Sections 4, 8, and 9 below, Executive will be entitled to the following benefits:

(a) **Severance Benefits.** The Company shall pay Executive an amount equal to six (6) months' worth of his or her monthly base salary (at the rate in effect immediately prior to the actions that resulted in the Qualifying Termination). The Executive will receive his or her severance payment in a cash lumpsum in accordance with the Company's standard payroll procedures, which payment will be made no later than the first regular payroll date occurring after the sixtieth (60^{th}) day following the Separation, *provided that* the Release Conditions have been satisfied.

(b) **Continued Employee Benefits.** If Executive timely elects continued coverage under the Consolidated Omnibus Budget Reconciliation Act **("COBRA"),** the Company shall pay the full amount of Executive's COBRA premiums on behalf of the Executive for the Executive's continued coverage under the Company's health, dental and vision plans, including coverage for the Executive's eligible dependents, for the same period that the Executive is paid severance benefits pursuant to Section 2(a) following the Executive's Separation or, if earlier, until Executive is eligible to be covered under another substantially equivalent medical insurance plan by a subsequent employer. Notwithstanding the foregoing, if the Company, in its sole discretion, determines that it cannot provide the foregoing subsidy of COBRA coverage without potentially violating or causing the Company to incur additional expense as a result of noncompliance with applicable law (including, without limitation. Section 2716 of the Public Health Service Act), the Company instead shall provide to Executive a taxable monthly payment in an amount equal to the monthly COBRA premium that Executive would be required to pay to continue the group health coverage in effect on the date of the Separation (which amount shall be based on the premium for the first month of COBRA coverage), which payments shall be made regardless of whether Executive elects COBRA continuation coverage and shall commence on the later of (i) the first day of the month following the month in which Executive experiences a Separation and (ii) the effective date of the Company's determination of violation of applicable law, and shall end on the earlier of (x) the effective date on which Executive becomes covered by a health, dental or vision insurance plan of a subsequent employer, and (y) the last day of the period that the Executive is paid severance benefits pursuant to Section 2(a) after the Separation, provided that, any taxable payments under Section 2(b) will not be paid before the first business day occurring after the sixtieth (60th) day

following the Separation and, once they commence, will include any unpaid amounts accrued from the date of Executive's Separation (to the extent not otherwise satisfied with continuation coverage). Executive shall have no right to an additional gross-up payment to account for the fact that such COBRA premium amounts are paid on an after-tax basis.

3. **CIC Qualifying Termination.** If Executive is subject to a CIC Qualifying Termination, then, subject to Sections 4, 8, and 9 below, Executive will be entitled to the following benefits:

(a) **Severance Payments.** The Company or its successor shall pay Executive twelve (12) months' worth of his or her monthly base salary and Executive's then-current annual target bonus, in each case at the rate in effect immediately prior to the actions that resulted in the Separation. Such payment shall be paid in a cash lump sum payment in accordance with the Company's standard payroll procedures, which payment will be made no later than the first regular payroll date occurring after the sixtieth (60^{th}) day following the Separation, *provided that* the Release Conditions have been satisfied. For the avoidance of doubt, in the event that a Change in Control occurs within three (3) months following a Qualifying Termination, then, provided that such Qualifying Termination followed a Potential Change in Control, Executive shall receive an additional payment in order to provide the benefits described in this Section 3(a), payable within 60 days following the date of such Change in Control.

(b) **Equity.** Each of Executive's then outstanding Equity Awards, excluding awards that would otherwise vest contingent upon remaining-unsatisfied performance criteria, shall accelerate and become vested and exercisable as to 100% of the then-unvested shares subject to the Equity Award. To the extent only service conditions remain with respect to an Equity Award that would otherwise vest in part upon satisfaction of performance criteria, such service conditions shall accelerate. Subject to Section 4, the accelerated vesting described above shall be effective as of the Separation. For the avoidance of doubt, in order to give effect to the acceleration contemplated by this Section 3(b), each of Executive's outstanding Equity Awards shall remain outstanding and eligible to vest (solely pursuant to the terms of this Section 3(b)) for a period of three (3) months following a Qualifying Termination and will be effective upon the Change of Control.

(c) **Continued Employee Benefits.** The Company or its successor shall provide the Executive with continuation of COBRA benefits or a cash benefit, in both cases on the same terms as set forth in Section 2(b) above for the same period that Executive is paid severance benefits pursuant to Section 3(a) following Executive's Separation or, if earlier, until Executive is eligible to be covered under another substantially equivalent medical insurance plan by a subsequent employer.

4. **General Release.** Any other provision of this Agreement notwithstanding, the benefits under Sections 2 and 3 shall not apply unless Executive (i) has executed a general release of all known and unknown claims that he or she may then have against the Company or persons affiliated with the Company and such release has become effective and (ii) has agreed not to prosecute any legal action or other proceeding based upon any of such claims. The release must be in the form prescribed by the Company, without alterations (this document effecting the foregoing, (the **"Release").** The Company will deliver the form of Release to Executive within thirty (30) days after Executive's Separation or such other time limit as is expressly provided in the Release documents, provided however that in all cases the Release must be executed and have become irrevocable within sixty (60) days following the date of the Executive's Separation.

5. **Accrued Compensation and Benefits.** Notwithstanding anything to the contrary in Sections 2 and 3 above, in connection with any termination of employment (whether or not a Qualifying Termination or CIC Qualifying Termination), the Company shall pay Executive's earned but unpaid base salary and other vested but unpaid cash entitlements for the period through and including the termination of employment, including unreimbursed documented business expenses incurred by Executive through and including the date of termination (collectively **"Accrued Compensation and Expenses"),** as required by law and the applicable Company plan or policy. In addition, Executive shall be entitled to any other vested benefits earned by Executive for the period through and including the termination date of Executive's employment under any other employee benefit plans and arrangements maintained by the Company, in accordance with the terms of such plans and arrangements, except as modified herein.

6. **Definitions.**

(a) **"Board"** means the Company's board of directors.

(b) **"Cause"** shall mean, as reasonably determined by the Board, (a) Executive's unauthorized use or disclosure of the Company's confidential information or trade secrets, which use or disclosure causes material harm to the Company, (b) Executive's material breach of any agreement between Executive and the Company, (c) Executive's commission of an act of personal dishonesty, fraud, deceit, or embezzlement in connection with Executive's employment, (d) Executive's material failure to comply with the Company's policies or rules, including, without limitation, the Company's policies or rules regarding harassment, alcohol or substance abuse, confidentiality, workplace violence, and discrimination, (e) Executive's conviction of, or plea of 'guilty" or 'no contest" to, a felony or a crime of moral turpitude, (f) Executive's failure to perform lawfully assigned duties after receiving written notification of the failure from the Company's Chief Executive Officer or other supervisor or (g) Executive's failure to cooperate in good faith with a governmental or internal investigation of the Company or its directors, officers or employees, if the Company has requested Executive's cooperation in writing, or (h) Executive's engagement in gross misconduct or gross neglect of Executive's duties where such misconduct or neglect is materially injurious to the Company, or (i) Executive's breach of any fiduciary duty owed to the Company by Executive that has or could reasonably be expected to have a detrimental effect on the Company's reputation or business. Notwithstanding, the foregoing, in the case of clauses (b), (d), (f) and (g), the Company will not terminate Executive's employment for Cause without first providing Executive with written notification of the acts or omissions constituting Cause and providing Executive with at least 10 days following such notice to cure such conduct (to the extent capable of cure).

(c) **"Code"** means the Internal Revenue Code of 1986, as amended.

(d) **"Change in Control."** For all purposes under this Agreement, a Change in Control shall mean a "Corporate Transaction," as such term is defined in the Plan, provided that the transaction (including any series of transactions) also qualifies as a change in control event under U.S. Treasury Regulation 1.409A-3(i)(5)(v) and(vii).

(e) **"CIC Qualifying Termination"** means a Separation (A) within twelve (12) months following a Change in Control, or (B) within three (3) months preceding a Change in Control (but as to part (B), only if the Separation occurs after a Potential Change in Control) resulting, in either case (A) or (B), from (i) the Company or its successor terminating Executive's employment for any reason other than Cause, or (ii) Executive voluntarily resigning his or her employment for Good Reason. A termination or resignation due to Executive's death or disability shall not constitute a CIC Qualifying Termination. A **"Potential Change in Control"** means the date of execution of a legally binding and definitive agreement for a corporate transaction which, if consummated, would constitute the applicable Change in Control (which for the avoidance of doubt, would include a merger agreement, but not a term sheet for a merger agreement). In the case of a termination following a Potential Change in Control and before a Change in Control, solely for purposes of benefits under this Agreement, the date of Separation will be deemed the date the Change in Control is consummated

(f) **"Equity Awards"** means all options to purchase shares of Company common stock as well as all other stock-based awards granted to Executive, including but not limited to stock bonus awards, restricted stock, restricted stock units and stock appreciation rights but excluding any equity awards that remain subject, in whole or in part, to any unsatisfied performance-based vesting conditions (it being understood that service-based vesting conditions alone shall not be deemed performance-based for this purpose).

(g) **"Good Reason"** means, without Executive's prior written consent, (i) a material reduction in the Executive's duties, authority, or responsibilities relative to Executive's duties, title, authority or responsibilities as an officer or employee in effect immediately prior to such reduction provided, however that (1) a mere change in Executive's title shall not constitute grounds for a termination by Executive for Good Reason unless in connection with or followed by a reduction in Executive's duties, responsibilities or authority or Executive's removal from such position or responsibilities without Cause and (2) a change in responsibility shall not be deemed to occur (A) solely because Executive is part of a larger organization, or (B) solely because of a change in title, (ii) a reduction by more than 10% in Executive's annual base salary or annual target bonus (other than a reduction generally applicable to executive officers of the Company and in generally the same proportion as for the Executive), (iii) a requirement that Executive relocate Executive's principal place of work to a location more than fifty (50) miles from Executive's then- current work location, or (iv) a material breach of this Agreement by the Company. For Executive to receive any benefits under this Agreement as a result of a resignation for Good Reason, all of the following requirements must be satisfied: (1) Executive must provide notice to the Company of his or her intent to assert Good Reason within sixty (60) days of the initial existence of one or more of the conditions set forth in subclauses (i) through (iv); (2) the Company will have thirty (30) days (the **"Company Cure Period")** from the date of such notice to remedy the condition and, if it does so, Executive may withdraw his or her resignation or may resign with no benefits under this Agreement; and (3) any termination of employment under this provision must occur within ten (10) days of the earlier of expiration of the Company Cure Period or written notice from the Company that it will not undertake to cure the condition set forth in subclauses (i) through (iv). Should the

Company remedy the condition as set forth above and then one or more of the conditions arises again, Executive may assert Good Reason again, subject to all of the conditions set forth herein.

(h) **"Plan"** means the Company's 2021 Equity Incentive Plan, as may be amended from time to time.

(i) **"Release Conditions"** mean the following conditions: (i) Company has received Executive's executed Release and (ii) any rescission period applicable to Executive's executed Release has expired (without Executive having rescinded the executed Release).

(j) **"Qualifying Termination"** means a Separation that is not a CIC Qualifying Termination, but which results from the Company terminating Executive's employment for any reason other than Cause or Executive voluntarily resigning his or her employment for Good Reason. A termination or resignation due to Executive's death or disability shall not constitute a Qualifying Termination.

(k) **"Separation"** means a "separation from service," as defined in the regulations under Section 409A of the Code.

7. **Successors.**

(a) **Company's Successors.** The Company shall require any successor (whether direct or indirect and whether by purchase, lease, merger, consolidation, liquidation or otherwise) to all or substantially all of the Company's business and/or assets, by an agreement in substance and form satisfactory to Executive, to assume this Agreement and to agree expressly to perform this Agreement in the same manner and to the same extent as the Company would be required to perform it in the absence of a succession. For all purposes under this Agreement, the term "Company" shall include any successor to the Company's business and/or assets or which becomes bound by this Agreement by operation of law.

(b) **Executive's Successors.** This Agreement and all rights of Executive hereunder shall inure to the benefit of, and be enforceable by, Executive's personal or legal representatives, executors, administrators, successors, heirs, distributees, devisees and legatees.

8. **Golden Parachute Taxes.**

(a) **Best After-Tax Result.** In the event that any payment or benefit received or to be received by Executive pursuant to this Agreement or otherwise **("Payments")** would (i) constitute a "parachute payment" within the meaning of Section 280G of the Code and (ii) but for this subsection (a), be subject to the excise tax imposed by Section 4999 of the Code, any successor provisions, or any comparable federal, state, local or foreign excise tax **("Excise Tax"),** then, subject to the provisions of Section 8, such Payments shall be either (A) provided in full pursuant to the terms of this Agreement or any other applicable agreement, or (B) provided as to such lesser extent which would result in no portion of such Payments being subject to the Excise Tax **("Reduced Amount"),** whichever of the foregoing amounts, taking into account the applicable federal, state, local and foreign income, employment and other taxes and the Excise Tax (including, without limitation, any interest or penalties on such taxes), results in the receipt by Executive, on an after-tax basis, of the greatest amount of payments and benefits provided for hereunder or otherwise, notwithstanding that all or some portion of such Payments may be subject to the Excise Tax. Unless the Company and Executive otherwise agree in writing, any determination required under this Section shall be made by independent tax counsel designated by the Company and reasonably acceptable to Executive **("Independent Tax Counsel"),** whose determination shall be conclusive and binding upon Executive and the Company for all purposes. For purposes of making the calculations required under this Section, Independent Tax Counsel may make reasonable assumptions and approximations concerning applicable taxes and may rely on reasonable, good faith interpretations concerning the application of Sections 280G and 4999 of the Code; provided that Independent Tax Counsel shall assume that Executive pays all taxes at the highest marginal rate. The Company and Executive shall furnish to Independent Tax Counsel such information and documents as Independent Tax Counsel may reasonably request in order to make a determination under this Section. The Company shall bear all costs that Independent Tax Counsel may reasonably incur in connection with any calculations contemplated by this Section. In the event that Section 8(a)(ii)(B) above applies, then based on the information provided to Executive and the Company by Independent Tax Counsel, Executive may, in Executive's sole discretion and within thirty (30) days of the date on which Executive is provided with the information prepared by Independent Tax Counsel, determine which and how much of the Payments (including the accelerated vesting of

equity compensation awards) to be otherwise received by Executive shall be eliminated or reduced (as long as after such determination the value (as calculated by Independent Tax Counsel in accordance with the provisions of
Sections 280G and 4999 of the Code) of the amounts payable or distributable to Executive equals the Reduced Amount). If the Internal Revenue Service (the **"IRS")** determines that any Payment is subject to the Excise Tax, then Section 8(b) hereof shall apply, and the enforcement of Section 8(b) shall be the exclusive remedy to the Company.

(b) **Adjustments.** If, notwithstanding any reduction described in Section 8(a) hereof (or in the absence of any such reduction), the IRS determines that Executive is liable for the Excise Tax as a result of the receipt of one or more Payments, then Executive shall be obligated to surrender or pay back to the Company, within one-hundred twenty (120) days after a final IRS determination, an amount of such payments or benefits equal to the **"Repayment Amount."** The Repayment Amount with respect to such Payments shall be the smallest such amount, if any, as shall be required to be surrendered or paid to the Company so that Executive's net proceeds with respect to such Payments (after taking into account the payment of the Excise Tax imposed on such Payments) shall be maximized. Notwithstanding the foregoing, the Repayment Amount with respect to such Payments shall be zero (0) if a Repayment Amount of more than zero (0) would not eliminate the Excise Tax imposed on such Payments or if a Repayment Amount of more than zero would not maximize the net amount received by Executive from the Payments. If the Excise Tax is not eliminated pursuant to this Section 8(b), Executive shall pay the Excise Tax.

9. **Miscellaneous Provisions.**

(a) **Section 409A.** To the extent (i) any payments to which Executive becomes entitled under this Agreement, or any agreement or plan referenced herein, in connection with Executive's termination of employment with the Company constitute deferred compensation subject to Section 409A of the Code and (ii) Executive is deemed at the time of such termination of employment to be a "specified" employee under Section 409A of the Code, then such payment or payments shall not be made or commence until the earlier of (i) the expiration of the six (6)-month period measured from the Executive's Separation; or (ii) the date of Executive's death following such Separation; provided, however, that such deferral shall only be effected to the extent required to avoid adverse tax treatment to Executive, including (without limitation) the additional twenty percent (20%) tax for which Executive would otherwise be liable under Section 409A(a)(l)(B) of the Code in the absence of such deferral. Upon the expiration of the applicable deferral period, any payments which would have otherwise been made during that period (whether in a single sum or in installments) in the absence of this paragraph shall be paid to Executive or Executive's beneficiary in one lump sum (without interest). Except as otherwise expressly provided herein, to the extent any expense reimbursement or the provision of any in-kind benefit under this Agreement (or otherwise referenced herein) is determined to be subject to (and not exempt from) Section 409A of the Code, the amount of any such expenses eligible for reimbursement, or the provision of any in-kind benefit, in one calendar year shall not affect the expenses eligible for reimbursement or in kind benefits to be provided in any other calendar year, in no event shall any expenses be reimbursed after the last day of the calendar year following the calendar year in which Executive incurred such expenses, and in no event shall any right to reimbursement or the provision of any in-kind benefit be subject to liquidation or exchange for another benefit. To the extent that any provision of this Agreement is ambiguous as to its exemption or compliance with Section 409A, the provision will be read in such a manner so that all payments hereunder are exempt from Section 409A to the maximum permissible extent, and for any payments where such construction is not tenable, that those payments comply with Section 409A to the maximum permissible extent. To the extent any payment under this Agreement may be classified as a "short-term deferral" within the meaning of Section 409A, such payment shall be deemed a short-term deferral, even if it may also qualify for an exemption from Section 409A under another provision of Section 409A. Payments pursuant to this Agreement (or referenced in this Agreement) are intended to constitute separate payments for purposes of Section 1.409A- 2(b)(2) of the regulations under Section 409A. To the extent any nonqualified deferred compensation subject to Section 409A of the Code payable to Executive hereunder could be paid in one or more taxable years depending upon Executive completing certain employment-related actions (such as resigning after a failure to cure a Good Reason event and/or returning the Release), then any such payments will commence or occur in the later taxable year to the extent required by Section 409A of the Code.

(b) **Other Arrangements.** This Agreement supersedes any and all cash severance arrangements and vesting acceleration arrangements under any agreement governing Equity Awards, severance and salary continuation arrangements, programs and plans which were previously offered by the Company to Executive, including employment agreement or offer letter, and Executive hereby waives Executive's rights to such other benefits. In no event shall any individual receive cash severance benefits under both this Agreement and any other vesting acceleration, severance pay or salary continuation program, plan or other arrangement with the Company. For the avoidance of doubt, in no event shall Executive receive payment under both Section 2 and Section 3 with respect to Executive's Separation.

(c) **Dispute Resolution.** To ensure rapid and economical resolution of any and all disputes that might arise in connection with this Agreement, Executive and the Company agree that any and all disputes, claims, and causes of action, in law or equity, arising from or relating to this Agreement or its enforcement, performance, breach, or interpretation, will be resolved solely and exclusively by final, binding, and confidential arbitration, by a single arbitrator, in Santa Clara County, and conducted by Judicial Arbitration & Mediation Services, Inc. **("JAMS")** under its then-existing employment rules and procedures. Nothing in this section, however, is intended to prevent either party from obtaining injunctive relief in court to prevent irreparable harm pending the conclusion of any such arbitration. Each party to an arbitration or litigation hereunder shall be responsible for the payment of its own attorneys' fees. The Company will pay the arbitration costs.

(d) **Notice.** Notices and all other communications contemplated by this Agreement shall be in writing and shall be deemed to have been duly given when personally delivered or when mailed by U.S. registered or certified mail, return receipt requested and postage prepaid or deposited with Federal Express Corporation, with shipping charges prepaid. In the case of Executive, mailed notices shall be addressed to him or her at the home address which he or she most recently communicated to the Company in writing. In the case of the Company, mailed notices shall be addressed to its corporate headquarters, and all notices shall be directed to the attention of its Secretary.

(e) **Waiver.** No provision of this Agreement shall be modified, waived or discharged unless the modification, waiver or discharge is agreed to in writing and signed by Executive and by an authorized officer of the Company (other than Executive). No waiver by either party of any breach of, or of compliance with, any condition or provision of this Agreement by the other party shall be considered a waiver of any other condition or provision or of the same condition or provision at another time.

(f) **Withholding Taxes.** All payments made under this Agreement shall be subject to reduction to reflect taxes or other charges required to be withheld by law.

(g) **Severability.** The invalidity or unenforceability of any provision or provisions of this Agreement shall not affect the validity or enforceability of any other provision hereof, which shall remain in full force and effect.

(h) **No Retention Rights.** Nothing in this Agreement shall confer upon Executive any right to continue in service for any period of specific duration or interfere with or otherwise restrict in any way the rights of the Company or any subsidiary of the Company or of Executive, which rights are hereby expressly reserved by each, to terminate his or her service at any time and for any reason, with or without Cause.

(i) **Choice of Law.** The validity, interpretation, construction and performance of this Agreement shall be governed by the laws of the State of California (other than its choice-of-law provisions).

[Signature Page Follows]

IN WITNESS WHEREOF, each of the parties has executed this Agreement, in the case of the Company by its duly authorized officer, as of the day and year first above written.

EXECUTIVE SENTINELONE, INC.

Print Name: By:

Title:

Exhibit 21.1

Subsidiaries of SentinelOne, Inc.

Company Name	Country	Relationship	Address
SentinelOne, Inc	US	Ultimate Parent	444 Castro Street, 4th Floor, Mountain View, CA 94041
SentinelOne Ventures LLC	US	Entity	444 Castro Street, 4th Floor, Mountain View, CA 94041
Sentinel Labs Israel Ltd	Israel	Entity	121 Menachem Begin Road, Sarona Tower, 38th Floor, Tel Aviv
Scalyr, LLC (fka Scalyr, Inc.)	US	Entity	444 Castro Street, 4th Floor, Mountain View, CA 94041
Attivo Networks, LLC (fka Attivo Networks, Inc.)	US	Entity	444 Castro Street, 4th Floor, Mountain View, CA 94041
Sentinel Labs Limited	UK	Entity - Limited Company	Fourth Floor, St James House, St James Square, Cheltenham, GL50 3PR
EPP Sentinel Research Labs France SAS	France	Entity - Limited Company	23 Rue Balzac, 75008 Paris, France
SentinelOne Holding B.V.	Netherlands	Entity	Strawinskylaan 4117, 1077ZX Amsterdam, the Netherlands
SentinelOne B.V.	Netherlands	Entity	Strawinskylaan 4117, 1077ZX Amsterdam, the Netherlands
SentinelOne CZ s.r.o	Czech Republic	Entity - Limited Company	Karolinská 707/7, Karlín, 186 00 Praha 8, Czech Republic
SentinelOne Denmark ApS	Denmark	Entity - Limited Company	C/O Crowe Rygårds Allé 104 2900 Hellerup, Denmark
SentinelOne Italy Srl	Italy	Entity - Limited Company	MILANO (MI) VIA CERESIO 7 CAP 20154, Italy
SentinelOne Cybersecurity Ireland Limited	Ireland	Entity - Limited Company	70 Sir John Rogerson's Quay, Dublin 2, Ireland
SentinelOne GmbH	Germany	Entity - Limited Company	Prielmayerstrasse 3, 80335 Munchen
SentinelOne Poland Sp Z o.o.	Poland	Entity – Limited Company	ul. PRZYOKOPOWA, nr 33 WARSZAWA, kod 01-208 Polska
SentinelOne Japan KK	Japan	Entity - Limited Company	2-1-3 Nihonbashi, Chuo-ku, Tokyo
Sentinel Labs Pte Limited	Singapore	Entity	12 Tannery Road #10-01, HB Centre 1, Singapore 347722
Sentinel Labs Australia Pty Ltd	Australia	Entity - Limited Company	c/o McCullough Robertson, Level 32, MLC Centre, 19 Martin Place, Sydney, NSW 2000
SentinelOne India Private Limited	India	Entity - Limited Company	24, 3 Floor, Harbans Singh Street, Darya Ganj, Delhi Central Delhi DL 110002 IN

Attivo Networks Security India Private Limited	India	Entity - Limited Company	1 Right Wing Second Floor IT PA Bangalore, India
Attivo Networks Pte, Ltd (Non-operational)	Singapore	Entity - Limited Company	10 Anson Road, #20-05A, International Plaza Singapore 079903
Attivo Networks Europe, Limited (Non-operational)	UK	Entity - Limited Company	160 Great Queen Street, Covent Garden London, WC2B 5AH, United Kingdom

EXHIBIT 23.1

CONSENT OF INDEPENDENT REGISTERED PUBLIC ACCOUNTING FIRM

We consent to the incorporation by reference in Registration Statement Nos. 333-264823, 333-264185, and 333-257593 on Form S-8 of our reports dated March 29, 2023, relating to the financial statements of SentinelOne, Inc. and the effectiveness of SentinelOne, Inc.'s internal control over financial reporting appearing in this Annual Report on Form 10-K for the year ended January 31, 2023.

/s/ DELOITTE & TOUCHE LLP

San Jose, California

March 29, 2023

Exhibit 31.1

CERTIFICATION OF PRINCIPAL EXECUTIVE OFFICER
PURSUANT TO EXCHANGE ACT RULES 13a-14(a) AND 15d-14(a),
AS ADOPTED PURSUANT TO SECTION 302 OF THE SARBANES-OXLEY ACT OF 2002

I, Tomer Weingarten, certify that:

1. I have reviewed this Annual Report on Form 10-K of SentinelOne, Inc.;

2.Based on my knowledge, this report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this report;

3.Based on my knowledge, the financial statements, and other financial information included in this report, fairly present in all material respects the financial condition, results of operations and cash flows of the registrant as of, and for, the periods presented in this report;

4.The registrant's other certifying officer(s) and I are responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-15(e) and 15d-15(e)) and internal control over financial reporting (as defined in Exchange Act Rules 13a-15(f) and 15d-15(f)) for the registrant and have:

(a) Designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under our supervision, to ensure that material information relating to the registrant, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this report is being prepared;

(b) Designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under our supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;

(c) Evaluated the effectiveness of the registrant's disclosure controls and procedures and presented in this report our conclusions about the effectiveness of the disclosure controls and procedures, as of the end of the period covered by this report based on such evaluation; and

(d) Disclosed in this report any change in the registrant's internal control over financial reporting that occurred during the registrant's most recent fiscal quarter (the registrant's fourth fiscal quarter in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the registrant's internal control over financial reporting; and

5. The registrant's other certifying officer(s) and I have disclosed, based on our most recent evaluation of internal control over financial reporting, to the registrant's auditors and the audit committee of the registrant's board of directors (or persons performing the equivalent functions):

(a) All significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the registrant's ability to record, process, summarize and report financial information; and

(b) Any fraud, whether or not material, that involves management or other employees who have a significant role in the registrant's internal control over financial reporting.

Date: March 29, 2023

By:	/s/ Tomer Weingarten
Name:	Tomer Weingarten
Title:	Chairman of the Board of Directors, President and Chief Executive Officer (Principal Executive Officer)

Exhibit 31.2

CERTIFICATION OF PRINCIPAL FINANCIAL OFFICER
PURSUANT TO EXCHANGE ACT RULES 13a-14(a) AND 15d-14(a),
AS ADOPTED PURSUANT TO SECTION 302 OF THE SARBANES-OXLEY ACT OF 2002

I, David Bernhardt, certify that:

1. I have reviewed this Annual Report on Form 10-K of SentinelOne, Inc.;

2. Based on my knowledge, this report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this report;

3. Based on my knowledge, the financial statements, and other financial information included in this report, fairly present in all material respects the financial condition, results of operations and cash flows of the registrant as of, and for, the periods presented in this report;

4. The registrant's other certifying officer(s) and I are responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-15(e) and 15d-15(e)) and internal control over financial reporting (as defined in Exchange Act Rules 13a-15(f) and 15d-15(f)) for the registrant and have:

    (a) Designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under our supervision, to ensure that material information relating to the registrant, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this report is being prepared;

    (b) Designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under our supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;

    (c) Evaluated the effectiveness of the registrant's disclosure controls and procedures and presented in this report our conclusions about the effectiveness of the disclosure controls and procedures, as of the end of the period covered by this report based on such evaluation; and

    (d) Disclosed in this report any change in the registrant's internal control over financial reporting that occurred during the registrant's most recent fiscal quarter (the registrant's fourth fiscal quarter in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the registrant's internal control over financial reporting; and

5. The registrant's other certifying officer(s) and I have disclosed, based on our most recent evaluation of internal control over financial reporting, to the registrant's auditors and the audit committee of the registrant's board of directors (or persons performing the equivalent functions):

    (a) All significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the registrant's ability to record, process, summarize and report financial information; and

    (b) Any fraud, whether or not material, that involves management or other employees who have a significant role in the registrant's internal control over financial reporting.

Date: March 29, 2023

By: /s/ David Bernhardt
Name: David Bernhardt
Title: Chief Financial Officer
(Principal Financial Officer)

Exhibit 32.1

CERTIFICATIONS OF PRINCIPAL EXECUTIVE OFFICER AND PRINCIPAL FINANCIAL OFFICER PURSUANT TO 18 U.S.C. SECTION 1350, AS ADOPTED PURSUANT TO SECTION 906 OF THE SARBANES-OXLEY ACT OF 2002

I, Tomer Weingarten, certify, pursuant to 18 U.S.C. Section 1350, as adopted pursuant to Section 906 of the Sarbanes-Oxley Act of 2002, that, to the best of my knowledge, the Annual Report on Form 10-K of SentinelOne, Inc. for the fiscal year ended January 31, 2023 fully complies with the requirements of Section 13(a) or 15(d) of the Securities Exchange Act of 1934 and that information contained in such Annual Report on Form 10-K fairly presents, in all material respects, the financial condition and results of operations of SentinelOne, Inc.

Date: March 29, 2023

By: /s/ Tomer Weingarten
Name: Tomer Weingarten
Title: Chairman of the Board of Directors, President and Chief Executive Officer
(Principal Executive Officer)

I, David Bernhardt, certify, pursuant to 18 U.S.C. Section 1350, as adopted pursuant to Section 906 of the Sarbanes-Oxley Act of 2002, that, to the best of my knowledge, the Annual Report on Form 10-K of SentinelOne, Inc. for the fiscal year ended January 31, 2023 fully complies with the requirements of Section 13(a) or 15(d) of the Securities Exchange Act of 1934 and that information contained in such Annual Report on Form 10-K fairly presents, in all material respects, the financial condition and results of operations of SentinelOne, Inc.

Date: March 29, 2023

By: /s/ David Bernhardt
Name: David Bernhardt
Title: Chief Financial Officer
(Principal Financial Officer)