

## **SentinelOne Unveils New AI Security Offerings to Give Defenders a Decisive Advantage**

*Agent Security, Agentic Investigations, and Integrated AI Data Pipelines Build On SentinelOne's Battletested AI Security Portfolio*

**SAN FRANCISCO, CA (RSAC 2026) – March 23, 2026 – [SentinelOne®](#)** (NYSE:S), the AI Security leader, has just revealed a new line up of AI security offerings, all designed to give defenders a decisive advantage, today. Covering both security for AI and the use of AI to automate and transform security operations, the new offerings build on SentinelOne's market-leading AI security portfolio. From securing autonomous agents to executing full agentic investigations with a single click of a button, all the new offerings are on display at RSAC 2026 (Booth N-5863).

As organizations race to embrace AI to speed innovation, scale operations and boost productivity, AI itself has become the new attack surface and primary source of risk. Not surprisingly, Gartner has reported that AI cybersecurity – defined as both securing AI and AI-amplified security – will be amongst the most significant and fastest growing markets in all AI spend over the next few years. In a January 2026 forecast, Gartner projected that AI cybersecurity spend will grow at an impressive 73.9% CAGR from 2024-2029, more than double that of AI spend overall.

### **New Prompt AI Agent Security**

Building upon SentinelOne's holistic end-to-end approach to securing AI ([blog link](#)), Prompt AI Agent Security provides a new, real-time discovery and governance control plane for AI agents and agentic workflows. It takes advantage of the same Autonomous Security Intelligence that powers SentinelOne across endpoint, cloud, and identity, extending that proprietary AI and automation into the agentic layer — monitoring, controlling, and enforcing policy on agent interactions in real time, at machine speed. The result is full visibility, risk assessment, and policy enforcement in every MCP server operating across a customer's environment. Also in preview, customers can manage the posture of every AI agent and agentic workflow and automatically remediate agentic behavior before unauthorized actions occur like an OpenClaw agent sending corporate data to an external endpoint without user awareness, or a Claude Cowork agent escalating privileges across enterprise systems through unauthorized action chaining.

### **New Prompt AI Red Teaming**

Prompt AI Red Teaming gives security and product teams first-of-their-kind capabilities to test and fortify homegrown and first-party AI applications. As developers embrace the use of agents to build new tools, applications and workflows in their enterprise environments, traditional security testing is inadequate to address the inherent AI-specific threats. With Prompt AI Red Teaming, organizations can maintain their innovation advantage without exposing their business or customers to critical risks by simulating real AI attacks (prompt injections, jailbreaks, privilege

escalation, data poisoning, etc.), hardening AI apps before they ship, and continuously evaluating risks (detecting model drift, emerging vulnerabilities, new attacks vectors, etc.) as models and threats evolve.

### **New Purple AI Auto Investigation Now GA**

At RSAC 2026, SentinelOne is building on Purple AI's lead with the general availability of new one-click Auto Investigation. Natively integrated into the Singularity™ Platform, this new capability allows analysts to launch complete, agentic investigations with a single click. Moving beyond rigid playbooks, Purple AI autonomously gathers cross-stack evidence, synthesizes threat data, and constructs complete attack timelines in real time. It delivers clear, explainable verdicts that instantly trigger closed-loop remediation via Singularity Hyperautomation—all while maintaining strict, analyst-in-the-loop governance.

Purple AI uses an agentic framework and human-level reasoning to give security teams the advantage of speed, scale, and skills needed to stop sophisticated attacks. It also delivers intuitive human-in-the-loop automation to amplify and free up human defenders to focus on the most strategic work.

First introduced at RSAC 2023 and battle-tested in thousands of real-world SOCs and customer environments, SentinelOne's Purple AI has become the defining agentic AI security analyst offering on the market. It has also become one of the most deployed. In SentinelOne's Q4 FY26 earnings call, the company reported a record attach rate for Purple AI, as it was included in over 50% of all licenses sold during the fourth quarter.

Agentic Auto Investigations now embeds Purple AI reasoning into the most difficult part of security operations, allowing for a complete cross source deep forensic investigation at machine speed, and without additional data routing or extended permissions. All of this is delivered within the bounds of the fully regulated Singularity data platform and AI SIEM.

As a result, Purple AI's new agentic Auto Investigations shrinks security investigations that took hours and days into minutes and seconds - helping defenders level the playing field and equalize the speed of AI-driven, machine speed attack.

Purple AI Auto Investigations is available for all Purple AI Analyst customers, with no further deployment or configuration needed.

### **New AI Data Pipelines in Singularity AI SIEM**

Following the Observo AI acquisition, SentinelOne is integrating AI-native data pipeline capabilities directly into Singularity AI SIEM to offer the only SIEM on the market to provide both pre-ingestion analytics and flexible data collection in a single platform. Bundled as part of Singularity AI SIEM, this integrated AI data pipeline includes intelligent filtering, enrichment, ND normalization — all operating upstream before data reaches the Singularity Platform. This

reduces data noise by up to 80% before ingestion, reducing infrastructure costs, while unlocking AI-detection and response across third party data at enterprise scale.

“From our founding SentinelOne has embraced AI and automation to give those that defend our world a deciding operating advantage,” said Tomer Weingarten, co-founder and CEO of SentinelOne. “Many of the world’s largest and most critical organizations trust SentinelOne’s AI Security portfolio to safeguard AI use and amplify human defenders. With these new innovations, they can now ingest and sanitize security source data on the fly into the Singularity Platform, and have complete human supervised agentic investigations to bring their security operations to machine speed - today. These new innovations build on our proven and production-grade foundation, to ensure customers can confidently harness the full power of AI today, knowing their initiatives are secure, well-governed, and resilient against future threats.”

### **About SentinelOne**

SentinelOne (NYSE: S) is the leader in AI security, setting the standard for using AI and automation to give defenders a decisive operating advantage. Built for those who secure our world, its platform delivers unified coverage across endpoints, identity, cloud, and AI. Powered by Autonomous Security Intelligence, SentinelOne stops attacks at machine speed, reducing risk and delivering clarity and control to stay one step ahead. Headquartered in Mountain View with teams worldwide, SentinelOne protects nearly one-fifth of the Fortune 500 and hundreds of Global 2000 enterprises. From Main Street to Wall Street, the world’s most critical organizations trust SentinelOne with their security.

### **Forward-Looking Statements**

This press release includes forward-looking statements, including, but not limited to, statements concerning the expected timing of product and feature availability, the benefits and capabilities of our current and future products and services, competition and our competitive position, our strategic plans and objectives, and general market trends. Forward-looking statements are subject to risks and uncertainties, including factors beyond our control, that could cause actual performance or results to differ materially from those expressed in or suggested by the forward-looking statements. These and other risk factors are described in the “Risk Factors” section of our most recent Annual Report on Form 10-K, subsequently quarterly reports filed on Form 10-Q, and other filings made with the U.S. Securities and Exchange Commission (SEC), which are available free of charge on our website at <http://investors.SentinelOne.com> and on the SEC’s website at [www.sec.gov](http://www.sec.gov).

You are cautioned not to place undue reliance on these forward-looking statements. Any future products, functionality and services may be abandoned or delayed, and as such, you should make decisions to purchase products and services based on features that are currently available. Any forward-looking statements made in this document are based on our beliefs and assumptions that we believe to be reasonable as of the date hereof. You should not rely upon forward-looking statements as predictions of future events. Except to the extent required by law, we undertake no obligation to update these forward-looking statements to reflect new information or future events.