CROWDSTRIKE
Investor Relations

CrowdStrike Establishes the Endpoint as the Epicenter for AI Security

March 23, 2026

New Falcon platform innovations solidify CrowdStrike as AI's security layer – extending AI agent discovery, governance, and runtime protection across endpoints, SaaS, browser, and cloud

AUSTIN, Texas & SAN FRANCISCO--(BUSINESS WIRE)--Mar. 23, 2026-- RSA 2026--CrowdStrike (NASDAQ: CRWD) today announced new capabilities across the Falcon® platform that establish the endpoint as the epicenter for AI security and CrowdStrike as the market's leading AI security platform. New platform innovations extend AI agent discovery, shadow AI governance, and runtime threat detection directly from the endpoint – the point of AI execution – to every surface where AI agents operate across SaaS, browser, and cloud environments.

As AI agents gain autonomy and system-level privilege, the endpoint has become the target and enforcement point for modern security. AI systems now execute commands, access sensitive data, and trigger downstream workflows directly on the endpoint, often in ways indistinguishable from legitimate user activity. This is where AI actions occur, and where they must be governed in real time. Legacy and network controls were not designed to govern this behavior. With this release, CrowdStrike closes the gap between AI adoption and security enforcement.

"AI agents are fundamentally changing how technology operates and how it must be secured," said Michael Sentonas, president of CrowdStrike. "Security built for static applications can't keep up with autonomous systems. Organizations need real-time visibility and control over AI behavior wherever it runs. CrowdStrike is that new standard."

Securing AI Agents on the Endpoint

The endpoint is emerging as the security epicenter as AI demand surges. CrowdStrike sensors detect more than 1,800 distinct AI applications running on enterprise devices, representing nearly 160 million unique application instances across its customer base.[1] AI agents execute terminal commands, modify files, access sensitive data, and trigger downstream workflows autonomously, with behavior indistinguishable from legitimate user activity. To secure where AI executes, CrowdStrike delivers:

- **EDR AI Runtime Protection:** CrowdStrike delivers runtime visibility of AI behavior at the point of execution. The Falcon sensor captures the commands, scripts, file activity, and network connections of all applications running on the endpoint, including agentic applications. When suspicious behavior is detected, human and agentic security teams can trace activity to the originating process and act immediately, including isolating affected endpoints to contain threats before they spread.
- **Shadow AI Discovery for Endpoint:** Automatically discovers AI applications, agents, LLM runtimes, MCP servers, and development tools running across endpoints, linking them to asset context and privilege exposure to prioritize risk to critical systems. Security teams can assess not just what AI is deployed, but also the potential blast radius of a compromise.
- **AIDR for Endpoint:** Extends prompt-layer protection to desktop AI applications, including ChatGPT, Gemini, Claude, DeepSeek, Microsoft Copilot, O365 Copilot, GitHub Copilot, and Cursor. Delivers real-time prompt inspection and detection of injection attacks and data leaks, and surfaces access and content policy violations.

---

[1] FY26 Earnings

Securing AI Agents Across SaaS, Browser, and Cloud

Agents do not only stay on the endpoint; they also work across SaaS platforms, cloud workloads, and AI pipelines – often with permissions that were not designed for governance at machine speed. CrowdStrike's acquisition of Seraphic extends runtime protection to the browser, securing agentic activity at the point where it increasingly operates. CrowdStrike secures AI systems, data, and agents in SaaS, browser, and cloud environments with:

- **Shadow SaaS and AI Agent Discovery:** Provides visibility into Shadow SaaS usage and AI agent activity, permissions, and data access across leading platforms, including Microsoft Copilot (Power Platform), Salesforce Agentforce, ChatGPT Enterprise, OpenAI Enterprise GPT, and Nexos.ai.
- **AIDR for Copilot Studio Agents:** Extends runtime guardrails to Microsoft Copilot Studio agents, monitoring prompts, data interactions, and agent behavior in real time to detect injection attacks, data leaks, and policy violations.
- **Shadow AI Discovery for Cloud:** Unifies visibility across cloud infrastructure and application layers, enabling identification of shadow AI, ungoverned LLM and MCP connections, and sensitive data exposure, as well as prioritized remediation.
- **AIDR for Cloud:** Secures AI workloads running in containerized environments communicating with the OpenAI API specification, providing runtime inspection for AI services and detection of prompt attacks, data leaks, and policy violations.
- **AI Data Flow Discovery for Cloud:** Delivers real-time visibility into how sensitive data flows into and through AI services. Enables teams to identify AI data exposure as it happens and automate response through unified SOAR workflows.

To learn more about CrowdStrike's latest AI security innovations:

- Visit booth #N-5845 at RSA
- Read our blog
- Visit our website

Future Product Disclaimer

This press release may include discussion of unreleased services or features. Any unreleased services or features referenced here are still in development and subject to change. Customers should make their purchase decisions based upon features that are currently available.

About CrowdStrike

CrowdStrike (NASDAQ: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft, and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting, and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity, and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/
Follow us: Blog | X | LinkedIn | Instagram
Start a free trial today: https://www.crowdstrike.com/trial

© 2026 CrowdStrike, Inc. All rights reserved. CrowdStrike and CrowdStrike Falcon are marks owned by CrowdStrike, Inc. and are registered in the United States and other countries. CrowdStrike owns other trademarks and service marks and may use the brands of third parties to identify their products and services.

View source version on businesswire.com: https://www.businesswire.com/news/home/20260322649008/en/

Media Contact
Jake Schuster
CrowdStrike Corporate Communications
press@crowdstrike.com

Source: CrowdStrike