CROWDSTRIKE
Investor Relations

CrowdStrike Delivers AI Security and Safety for the Enterprise

November 3, 2026

Falcon Guardian introduces new AI Kill Switch and unifies agent-level hooks, endpoint network inspection, and the endpoint to stop unauthorized agent activity at runtime; planned acquisition of Fiddler increases AI safety through agent observability

AUSTIN, Texas & BARCELONA, Spain--(BUSINESS WIRE)--Nov. 3, 2026-- **Fal.Con Europe 2026 --** CrowdStrike (NASDAQ: CRWD) today announced a new AI Kill Switch in Falcon Guardian and innovations to secure AI agents at every control point. Coupled with its intended acquisition of Fiddler AI, a leader in AI agent observability, CrowdStrike will deliver the industry's broadest set of AI agent security and safety capabilities through the Falcon platform.

AI agents are automating work end-to-end. Securing them requires protection at every control point. Falcon Guardian secures AI agents where they execute, on the endpoint at runtime. New innovations add the agent and the network: agent-level hooks enforce what agents are told to do, and endpoint network inspection sees when they communicate with models and tools. Only CrowdStrike brings the agent, the network, and the endpoint together, so organizations can move fast with AI without losing control.

"Every organization is racing to get more out of AI, and every week we see agents chain steps together, hit an obstacle, and take actions they were never authorized to take," said Michael Sentonas, president of CrowdStrike. "One control point isn't enough to stop that. It takes the agent, the network, and the endpoint, together. This is how we make security the enabler for AI adoption, not the obstacle."

CrowdStrike's Architectural Advantage: One Sensor at Every AI Control Point

Agent-level hooks see the prompt, but miss the model's response and can't catch every action an agent takes. Network-only approaches watch traffic but can't stop the action, because the agent executes on the endpoint, not the network. And the moment an agent runs a local or open-weight model that never touches the network, network-only tools go blind.

Guardian unifies agent-level controls, endpoint network inspection, and the endpoint on a single Falcon sensor, connecting what an agent is told to do, what it communicates, and what it executes. That architectural advantage provides the full context to know when an agent has turned into a threat, and to stop it. Generally available since September 2026, Guardian has shipped new innovations since launch, with more on the way.

Available Today

- **AI Kill Switch:** Terminates unauthorized agents in real time first at the Gateway, and soon on the endpoint, and blocks them from running again across the organization.
- **AI Gateway:** Now generally available and included with Guardian, the AI Gateway routes AI traffic through a centralized gateway to inspect prompts and responses, monitor usage, and enforce policy across managed and unmanaged devices.
- **Agent-Level Hooks:** Enforces policy inside the most widely used AI agents, including Claude Code, OpenAI Codex, GitHub Copilot, Microsoft 365 Copilot, OpenCode, and Cursor, using hooks to inspect prompts and block malicious activity at the source.
- **SafeMind-Powered Detection:** Applies CrowdStrike SafeMind models and adversary intelligence to detect attacks targeting AI systems, including prompt injection, malicious instructions, and personally identifiable information.
- **AI Supply Chain Protection:** Discovers malicious AI skills and MCP servers to stop threats before they enter the AI environment.
- **Anthropic Integration:** Run the Falcon sensor inside the Claude Cowork virtual machine, delivered in partnership with Anthropic, to gain visibility inside the Cowork environment and connect it to activity across the enterprise.

New Innovations

- **Endpoint Network Inspection:** Inspects all AI traffic as it enters and leaves the endpoint, pairing what an agent sends over the network with what it does on the endpoint. Network-only approaches see the traffic but never the endpoint, so they cannot connect a prompt to the action it triggers. Generally available for Windows, with Mac in early access.
- **Agentic Identity:** Identity-aware controls will authorize what agents can access.
- **Cloud Expansion:** Extends Guardian to secure AI agents across cloud workloads, SaaS, virtualized agents including Claude Cowork, and cloud agent frameworks including AWS AgentCore.

The Enabler for AI Adoption

Guardian stops unauthorized agent activity at runtime. CrowdStrike's planned acquisition of Fiddler will add agent observability to evaluate agents before they deploy and explain why they act. The more enterprises rely on agents, the more they need to prove those agents behave as intended, and that trust is what lets them go faster with AI.

To learn more about Falcon Guardian, visit here.

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.

Forward-Looking Statements

This press release contains forward-looking statements that involve risks and uncertainties, including statements regarding the benefits and capabilities of our current and future products and services, the expected timing of product and feature availability, the benefits of the planned acquisition of Fiddler to CrowdStrike and its customers and CrowdStrike's plans to integrate Fiddler's technology and operations. You should not place undue reliance on these forward-looking statements, as actual outcomes and results may differ materially from those contemplated as a result of risks and uncertainties. There are a number of factors that could cause actual results to differ materially from statements made in this press release, including the satisfaction of conditions to closing the acquisition, CrowdStrike's ability to integrate Fiddler's technology and operations, and other risks described in the filings CrowdStrike makes with the Securities and Exchange Commission from time to time, including CrowdStrike's most recently filed Annual Report on Form 10-K, most recently filed Quarterly Report on Form 10-Q, and subsequent filings. All forward-looking statements in this press release are based on information available to CrowdStrike as of the date hereof, and CrowdStrike does not assume any obligation to update any of these forward-looking statements to reflect events that occur or circumstances that exist after the date on which they were made.

View source version on businesswire.com: https://www.businesswire.com/news/home/20261103352360/en/

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

Source: CrowdStrike