



CrowdStrike and NVIDIA Expand AI Agent Security from Software to Silicon

October 21, 2026

Falcon Guardian integration with NVIDIA OpenShell and NVIDIA Sentry will extend AIDR from agent runtimes to hardware-based enforcement

AUSTIN, Texas & BERLIN--(BUSINESS WIRE)--Oct. 21, 2026-- NVIDIA GTC 2026--[CrowdStrike](#) (NASDAQ: CRWD) today announced an expanded collaboration with [NVIDIA](#) to extend AI-native security from software to silicon.

Building on the [NVIDIA OpenShell Reference Architecture](#) announced today, CrowdStrike is integrating [Falcon Guardian](#), its AI Detection and Response (AIDR) solution, with [NVIDIA OpenShell](#) secure runtime software, and plans to integrate with [NVIDIA Sentry](#) for in-silicon enforcement. Together, these capabilities will extend AI agent security from software to silicon, helping enterprises secure autonomous AI across software and infrastructure.

"AI agents have already created a new attack surface, and guardrails alone won't stop an adversary," said Daniel Bernard, chief business officer at CrowdStrike. "CrowdStrike pioneered AI-native cybersecurity. Together with NVIDIA, we're setting the standard for securing autonomous AI, from detecting threats in software to stopping them at the silicon level."

The collaboration will extend Falcon Guardian's AIDR capabilities across NVIDIA's OpenShell Reference Architecture to:

- **Secure Autonomous AI at Scale:** Integration with NVIDIA OpenShell will connect agent prompts, model interactions, and runtime activity with broader Falcon platform security context, helping enterprises detect malicious behavior across AI agent workflows.
- **Contain Threats at Machine Speed:** Planned integration with NVIDIA Sentry on BlueField-4 DPUs will bring AIDR together with out-of-band monitoring and in-silicon policy enforcement to help enterprises detect and contain unsafe agent behavior beyond the software runtime.

"Autodesk customers design and make the buildings, products, and infrastructure people depend on, and in that world there is little room for error. We hold AI agents to the same standard," said Sebastian Goodwin, chief trust officer, Autodesk. "CrowdStrike Falcon Guardian gives us visibility into what our agents are doing, what they can access, and when to intervene. Extending that control deeper into the infrastructure helps customers of every size, from large enterprises to small businesses, trust the AI behind their work."

"Securing agents in production requires protection from the runtime to the underlying infrastructure," said Justin Boitano, vice president of enterprise at NVIDIA. "The NVIDIA OpenShell Reference Architecture provides the foundation for runtime security and hardware-based enforcement. Together with CrowdStrike's AI Detection and Response capabilities, we're working to bring comprehensive security to AI agents at scale."

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 may include discussion of unreleased services or features. Any references to unreleased features reflect our current plans only and do not constitute a promise or commitment to deliver such features. These items may change or may not

be made available in all regions. Customers should make purchase decisions based on features currently available.

View source version on businesswire.com: <https://www.businesswire.com/news/home/20261020113617/en/>

Media Contact

Jake Schuster

CrowdStrike Corporate Communications

press@crowdstrike.com

Source: CrowdStrike