

CrowdStrike's Open Gateway Ecosystem Makes Falcon AI's Control Plane

June 16, 2026

With a growing ecosystem of AI gateway partners – including Databricks, Google Cloud, JetStream Security, Kong, LiteLLM, Maxim AI, Microsoft Azure, and TrueFoundry – CrowdStrike extends the Falcon platform to unify visibility, protection, and control across AI

AUSTIN, Texas--(BUSINESS WIRE)--Jun. 16, 2026-- [CrowdStrike](#) (NASDAQ: CRWD) today announced it is extending [CrowdStrike Falcon® AI Detection and Response \(AIDR\)](#) across leading AI gateway partners, including Databricks, Google Cloud, JetStream Security, Kong, LiteLLM, Maxim AI, Microsoft Azure, and TrueFoundry, delivering AI's security control plane.

As enterprises move AI into production, AI traffic spans multiple gateways, APIs, and models, fragmenting visibility and increasing exposure to prompt injection, data leakage, and adversary manipulation. Securing AI requires visibility and control across this interaction layer, where prompts, agents, and models operate in real time.

CrowdStrike addresses this by extending Falcon AIDR through native integrations with its AI gateway partners. The result: correlated telemetry, threat detection, and consistent policy enforcement as AI scales.

"Every enterprise has AI in production across multiple gateways, models, and APIs. That's not a future state, it's today's attack surface," said Daniel Bernard, chief business officer at CrowdStrike. "With Falcon AIDR and our AI gateway ecosystem, CrowdStrike makes the Falcon platform AI's security control plane, so organizations benefit from unified visibility and protection wherever their AI runs."

This open ecosystem approach will expand [CrowdStrike Falcon® platform](#) protection across the AI stack:

- **Protect AI at the gateway:** Integrations with Azure API Management, Databricks, Google Cloud, JetStream Security, Kong, LiteLLM, Maxim AI, and TrueFoundry apply threat detection, data protection, access controls, and policy enforcement directly to AI interactions – without requiring changes to existing architectures.
- **Secure the AI interaction layer:** Falcon AIDR protects prompts, responses, agents, and models – stopping prompt injection, jailbreak attempts, and data exposure in real time.
- **Unify visibility across AI activity:** Capture and correlate telemetry across users, applications, gateways, and models to expose hidden risk.
- **Enforce protection in real time:** Inline controls enable immediate enforcement without disrupting AI workflows.
- **Extending across the Falcon platform:** AIDR feeds [Falcon® Next-Gen SIEM](#), enabling cross-domain detection and response across AI, endpoint, identity, cloud, SaaS, and third-party data sources.

With a growing ecosystem of AI gateway partners, CrowdStrike is extending the Falcon platform to bring AI security together, giving organizations the visibility and control to scale AI with confidence.

Supporting Quotes

Databricks

"As organizations move AI into production, governance must extend beyond access controls to include visibility and protection across AI interactions. By integrating CrowdStrike Falcon AI Detection and Response with Databricks Unity AI Gateway, customers can monitor AI activity, enforce guardrails, and manage risk across models, agents, and tools." – Stephen Orban, SVP, Product Partnerships and Ecosystem, Databricks

Google Cloud

"AI is rapidly becoming embedded across enterprise applications and APIs, which makes consistent governance and visibility critical. Integrating Falcon AIDR with Google Cloud Apigee helps organizations secure AI interactions across distributed environments while maintaining the flexibility developers need to scale AI services." – Vineet Bhan, director of security and identity partnerships, Google Cloud

JetStream Security

"AI isn't a network problem; it's a runtime reality. You can't secure AI with gateways alone that only provide surface-level visibility. CrowdStrike and JetStream operate where AI activity actually happens – across endpoints, browsers, SaaS applications, and the cloud. Together, we're helping organizations bring consistent visibility and control across AI environments as they scale." – Raj Rajamani, co-founder and CEO, JetStream Security

Kong

"Enterprises running AI at scale need security that's both model- and agent-aware, as well as threat-aware. With AI connectivity from Kong and complete AI attack path protection from CrowdStrike, organizations can scale AI without losing control of how those interactions are governed and secured. Together, this gives customers a more complete approach to securing AI in production." – Ken Kim, senior vice president, partners and alliances, Kong

LiteLLM

"Enterprises need to secure AI interactions without disrupting developer workflows. By integrating LiteLLM with Falcon AIDR, organizations can apply real-time protection and policy enforcement across AI traffic as it moves through their environments." – Krrish Dholakia, co-founder and CEO, LiteLLM

Maxim AI

"Organizations need consistent enforcement for AI security policies across growing LLM environments. With Bifrost and Falcon AIDR, customers can inspect prompts before they reach models and automatically block or rewrite risky AI responses in real time. As AI agents become core to enterprise workflows, the gateway and the security layer need to operate as one. Our partnership with CrowdStrike is a strong signal of where the industry is heading, and we're proud to be building it together." – Vaibhavi Gangwar, co-founder and CEO, Maxim AI

Microsoft Azure

"Enterprises are looking for ways to operationalize AI securely across increasingly complex API ecosystems. By extending Falcon AIDR through Microsoft Azure API Management, organizations can apply centralized policy enforcement and gain deeper visibility into AI activity across applications, services, and models." – Balan Subramanian, General Manager, Azure App Platform Services, Microsoft

TrueFoundry

"Customers are building AI applications across multiple frameworks and gateways, and security must follow that architecture. Our integration with Falcon AIDR enables organizations to enforce consistent guardrails across AI workflows as they scale." – Anuraag Gutgutia, co-founder and COO, TrueFoundry

Forward-Looking Statements

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/20260615483269/en/>

Media Contact

Jake Schuster
CrowdStrike Corporate Communications
press@crowdstrike.com

Source: CrowdStrike, Inc.