CrowdStrike Announces the General Availability of Falcon AI Detection and Response to Secure the New AI Attack Surface

With unified AI prompt-layer protection, CrowdStrike secures enterprise AI everywhere it happens – from development through workforce usage

AUSTIN, Texas--(BUSINESS WIRE)--Dec. 15, 2025-- CrowdStrike (NASDAQ: CRWD) today announced the general availability of Falcon® AI Detection and Response (AIDR), extending the Falcon® platform to secure the fastest-growing attack surface in the AI era: the AI prompt and agent interaction layer. With Falcon AIDR, CrowdStrike delivers the industry's first unified platform that secures every layer of enterprise AI – data, models, agents, identities, infrastructure, and interactions – from development through workforce usage.

This press release features multimedia. View the full release here: https://www.businesswire.com/news/home/20251214418582/en/

"Prompt injection is a frontier security problem. Adversaries are injecting hidden instructions into GenAI tools to weaponize the very systems transforming how work gets done," said Michael Sentonas, president of CrowdStrike. "Falcon AIDR secures every prompt, response, and agent action in real time, extending the power of the Falcon platform to the interaction layer and delivering complete protection across our customers' AI infrastructure."

Securing AI Development and Use Across the Enterprise

CrowdStrike pioneered modern endpoint security with EDR and brings the same architectural advantage to AI with AIDR, protecting the interaction layer where AI systems reason, decide, and take action. Adversaries are targeting this layer, using hidden instructions to hijack agents, manipulate outcomes, and access sensitive data. Today, the AI interaction layer is the new attack surface and prompts are the new malware. Falcon AIDR delivers unified, real-time protection across development workflows and workforce AI usage, securing prompts, responses, and agent actions at enterprise scale.

Falcon AIDR delivers unified visibility, governance, and enforcement across enterprise AI development and workforce usage through the following capabilities:

- **See AI Everywhere:** Gain deep visibility into how employees use AI and how agents operate with runtime logs for compliance and investigations.
- **Block Prompt Injection Attacks:** Stop prompt injection, jailbreaks, and unsafe content in real time, powered by intelligence from deep research on adversarial prompt datasets and 180+ known prompt injection techniques.
- **Stop Risky AI Use in Real Time:** Block unsafe interactions, contain malicious agent actions, and enforce policy controls in real time.
- **Protect Sensitive Data:** Automatically detect and block credentials, regulated data, and other sensitive information before it can reach models, agents, or external AI systems.
- **Accelerate Secure AI Innovation:** Build secure applications and agents with built-in safeguards for developers, bringing AI innovation to market faster while reducing risk.

Unified AI Security on the Falcon Platform

With Falcon AIDR as part of the Falcon platform, CrowdStrike delivers a unified security model for AI, protecting everything from the environments where AI runs to the interaction layer where prompts and agents operate. Falcon provides end-to-end security for AI development and workforce use, giving organizations a single, unified approach to protecting AI at enterprise scale.

Additional Resources

- To learn more about Falcon AIDR, read our blog and visit here.
- To learn more about how CrowdStrike secures AI across the enterprise, visit here.
- To register for the virtual AI Summit: Accelerating Secure AI Adoption and Development on January 21, 2026 (AMER), January 22 (APJ), or January 27 (EMEA), 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

View source version on businesswire.com: https://www.businesswire.com/news/home/20251214418582/en/

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

Source: CrowdStrike