CrowdStrike Delivers Full Lifecycle Protection for LLMs to Enterprise AI Factories with NVIDIA

June 11, 2025

CrowdStrike expands protection for NVIDIA Enterprise AI Factories, integrates Falcon Cloud Security with NVIDIA universal LLM NIM microservices and NeMo Safety for secure cloud deployment

AUSTIN, Texas--(BUSINESS WIRE)--Jun. 11, 2025-- CrowdStrike (NASDAQ: CRWD) today announced the integration of Falcon® Cloud Security with NVIDIA universal LLM NIM microservices and NeMo Safety, delivering full lifecycle protection for AI and over 100,000 large language models (LLMs) in collaboration with NVIDIA.

Expanding CrowdStrike's protection for Enterprise AI Factories with NVIDIA, this new integration enables customers to safely run and scale diverse LLM applications across hybrid and multi-cloud environments from day one. From build, to runtime, to posture management, the CrowdStrike Falcon® platform is securing every stage of AI innovation powered by NVIDIA.

"CrowdStrike pioneered AI-native cybersecurity, and we're defining how AI is secured across the software development lifecycle," said Daniel Bernard, chief business officer at CrowdStrike. "This latest collaboration with NVIDIA brings our leadership to the front lines of cloud-based AI – where LLMs are deployed, run, and scaled. Together, we're giving organizations the confidence to innovate with AI, securely and at speed, from code to cloud."

"As AI becomes fundamental to enterprises, security must evolve to match its scale and speed," said Justin Boitano, vice president, Enterprise AI Software at NVIDIA. "NVIDIA and CrowdStrike are working together to help enterprises protect AI workloads across the entire lifecycle – from the intelligence forged in AI factories to deployment with NIM microservices."

Enterprises can rely on NVIDIA Enterprise AI Factory with CrowdStrike security for the hardware and software to build, deploy, and run AI applications and LLMs with speed and control. NVIDIA universal LLM NIM microservice container streamlines the move from development to production by packaging a broad range of open and specialized LLMs as microservices for fast, scalable deployment for high performance inference across hybrid and multi-cloud environments, including those with AI sovereignty requirements.

As LLMs move into production, AI risk grows, exposing models to risks like data poisoning, tampering, and sensitive data leakage. The Falcon platform integrates with NVIDIA NIM to deliver end-to-end protection, monitoring runtime behavior and powering AI-driven detection and response trained on trillions of daily security events and frontline intelligence. With Falcon Cloud Security, organizations gain pre-deployment protection through capabilities like AI-SPM, AI Model Scanning, and Shadow AI detection, identifying and mitigating risks before models go live. These capabilities also deliver threat intelligence that integrates with NVIDIA's NeMo Safety workflows, helping enterprises assess and strengthen the security of foundation models as they scale new AI applications. Combined with expert services like CrowdStrike AI Red Team and Falcon® Adversary OverWatch, the Falcon platform secures every stage of AI innovation – from code to cloud, across hybrid and multi-cloud environments.

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 | Twitter | LinkedIn | Facebook | Instagram
Start a free trial today: https://www.crowdstrike.com/free-trial-guide/

View source version on businesswire.com: https://www.businesswire.com/news/home/20250611360756/en/

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

Source: CrowdStrike