CrowdStrike Brings Agentic AI Security Workflow Integrations and GenAI Protection to AWS Marketplace

July 16, 2025

falcon-mcp and AI Red Team Services now available in new AI Agents and Tools category of AWS Marketplace

AUSTIN, Texas--(BUSINESS WIRE)--**AWS Summit NYC –** CrowdStrike (NASDAQ: CRWD) today announced an expanded collaboration with Amazon Web Services (AWS) to accelerate AI adoption in cybersecurity and secure AI use. With the availability of *falcon-mcp*, an MCP server for the CrowdStrike Falcon® platform, and CrowdStrike AI Red Team Services in the new AI Agents and Tools category of AWS Marketplace, AWS customers can securely operationalize agentic AI workflow integrations, and test, validate, and protect GenAI systems – all within their existing AWS environment.

AI adoption is accelerating, yet most enterprises still lack secure, scalable ways to connect models to real-time security operations. Without trusted frameworks for integration and testing, agentic innovation can introduce new risks. With *falcon-mcp* and AI Red Team Services now available in the AI Agents and Tools category in AWS Marketplace, organizations can power security operations with AI – and protect the AI systems those operations rely on.

“Agentic AI is fundamentally changing business of all sizes across every industry – but only secure AI can safely scale to deliver long-term results,” said Daniel Bernard, chief business officer, CrowdStrike. “With these offerings now available in AWS Marketplace, CrowdStrike is giving customers the power to safely build, test, and run AI-driven security workflows using the same cybersecurity platform trusted to protect the world’s most critical environments.”

“As AI becomes embedded across enterprise workflows, the security risks tied to LLMs and agentic platforms are quickly moving from theoretical to practical,” said Jay McBain, chief analyst, Canalys. “CrowdStrike’s work with AWS – bringing both real-time security integration and proactive AI system validation to the Marketplace – sets a new bar for how the ecosystem can operationalize AI securely at scale.”

Build Agentic Workflows Securely with *falcon-mcp*

With the launch of *falcon-mcp*, an MCP server for Falcon platform, CrowdStrike is delivering a standardized, open protocol that securely connects AI agents and LLM-powered applications to Falcon telemetry – including detections, incidents, threat intelligence, and behavioral data. Now available in preview via Amazon Bedrock AgentCore, *falcon-mcp* simplifies deployment and accelerates adoption of agentic workflows by providing plug-and-play access to Falcon data, enabling seamless integration of AI capabilities into existing security operations – streamlining adoption of secure, agentic workflows.

Test and Harden GenAI Systems with AI Red Team Services

CrowdStrike AI Red Team Services provide organizations with comprehensive security assessments for AI systems, including LLMs and their integrations, to identify vulnerabilities and misconfigurations that could lead to data breaches, unauthorized code execution, or application manipulation. These assessments align with frameworks like the OWASP Top 10 for LLMs, delivering clear, actionable guidance to harden both AI models and the infrastructure they rely on.

Secure End-to-End AI Innovation with CrowdStrike and AWS

CrowdStrike and AWS enable joint customers to protect AI applications, services, and LLMs in the cloud. With native integrations across AWS services – including Amazon SageMaker and Amazon Bedrock – customers can deploy and scale AI workloads securely across the entire lifecycle. CrowdStrike delivers purpose-built security for AI through innovations like AI Security Posture Management (AI-SPM), Falcon Data Protection, and AI Red Team Services. Just as AWS relies on the Falcon® platform to protect its own infrastructure – from code to cloud, and device to data – organizations trust CrowdStrike to secure the infrastructure powering the next wave of AI innovation on AWS.

To learn more about the CrowdStrike-AWS partnership, visit CrowdStrike at AWS Summit NYC Booth #842.

Disclaimer:

This press release contains information about developing products and services, including products in public preview and under active development. These offerings including the release timing and features are subject to change at CrowdStrike’s sole discretion at any time.

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 | 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/20250716921254/en/

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

Source: CrowdStrike