CROWDSTRIKE
Investor Relations

CrowdStrike Extends Its Endpoint Advantage to Secure the Software Supply Chain

September 2, 2026

As AI rewrites how software gets built, CrowdStrike stops malicious open-source packages at the endpoint before they execute

AUSTIN, Texas & LAS VEGAS--(BUSINESS WIRE)--Sep. 2, 2026--

Fal.Con 2026-- CrowdStrike (NASDAQ: CRWD) today introduced Real-Time Supply Chain Attack Protection, a new Falcon platform innovation that blocks malicious open-source packages at the endpoint before their embedded code can run.

AI has changed how software gets built. Coding agents now assemble applications from open-source packages pulled off public registries at machine speed, faster than anyone can review what comes in. A poisoned package runs its code on the endpoint the moment it installs. The endpoint is the point of execution, and where the Falcon sensor already operates. CrowdStrike blocks malicious packages in real time, before that code can run.

“Attackers know that compromising one trusted package can give them a path into thousands of organizations. That makes the software supply chain one of the most powerful attack surfaces in the AI era,” said Michael Sentonas, president of CrowdStrike. “The endpoint is where malicious code executes, and only CrowdStrike turns it into the control point that stops the attack.”

Software Supply Chain Risk Converges on the Endpoint

Adversaries have industrialized poisoning the packages enterprises trust. CrowdStrike's 2026 Threat Hunting Report found DPRK-nexus adversary STARDUST CHOLLIMA poisoned 131 trusted AI framework packages, while eCrime actor ALTERED SPIDER compromised more than 300 software dependencies in a single day. The risk no longer stops at engineering. As AI agents spread across the business, any endpoint can pull a package to finish a task, and the attack surface widens to the whole enterprise.

A poisoned package does not look like malware. It arrives as an ordinary file and runs its code the moment it installs. Legacy endpoint tools were built to catch executables, not to govern the packages that assemble AI software. Standalone scanners, proxies, and browser-based tools flag compromises days after poisoned packages have already landed. If not stopped at the endpoint before embedded scripts execute, a poisoned package moves downstream, giving adversaries a foothold.

Stopping Malicious Packages Before They Run

CrowdStrike Real-Time Supply Chain Attack Protection stops malicious packages the moment they reach the endpoint, intercepting at the command line, before any embedded script runs. Because CrowdStrike already enforces at that checkpoint through the same sensor, adversary intelligence, and response orchestration securing the endpoint, protection carries forward into whatever the package tries to do next: execution, credential access, lateral movement. No new agent, and no coverage gaps.

- **Block Malicious Packages at Download:** The Falcon sensor intercepts open-source package manager transactions – npm install, pip install – across npm and PyPI on Windows, macOS, and Linux, before any embedded script runs. Protection extends to every endpoint where agentic applications run, not just developer workstations.
- **Stop the Attack Before it Starts:** Security teams can set granular controls to govern what code reaches their endpoints – including minimum package age requirements – so the most common vector of supply chain compromise never gets a foothold.
- **Automated Investigation and Response:** The moment a package is flagged, CrowdStrike automatically runs a lookback across every endpoint and triggers remediation through Charlotte Agentic SOAR.
- **Global Package Inventory:** Delivers complete visibility into every software package installed across every endpoint, so when a package is compromised, security teams know exactly where it lives and can act immediately.

Securing the Software Enterprises Build on AI

Software will only be built faster and with more automation. CrowdStrike makes the endpoint the control point for the software supply chain, so enterprises can build on AI without leaving the door open to the adversary. To learn more, read our blog and 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

Forward-Looking Statements

This release includes 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.

View source version on businesswire.com: https://www.businesswire.com/news/home/20260902312863/en/

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

Source: CrowdStrike