

CrowdStrike Accelerates Cybersecurity Consolidation with AI-Powered Network Vulnerability Assessment for Falcon Exposure Management

March 24, 2025

New capability extends the Falcon platform's AI-driven risk prioritization to network assets, eliminating the need for standalone scanners, agents or hardware; Falcon Exposure Management customers can assess up to 10% of their assets at no cost

AUSTIN, Texas--(BUSINESS WIRE)--Mar. 24, 2025-- [CrowdStrike](#) (NASDAQ: CRWD) today announced new [CrowdStrike Falcon® Exposure Management](#) innovations, accelerating cybersecurity consolidation by eliminating outdated vulnerability management tools and extending AI-powered risk prioritization to network assets. The general availability of the Network Vulnerability Assessment capability enables security teams to identify and remediate high-risk vulnerabilities in network devices, including routers, switches and firewalls, in real time—without additional scanners, agents or hardware.

The single-agent architecture of the [CrowdStrike Falcon® cybersecurity platform](#) empowers organizations to replace legacy vulnerability management tools with a single click, consolidating security operations on the Falcon platform and modernizing static, CVSS-based risk models with an adversary-driven approach. Falcon Exposure Management customers receive free scanning for up to 10% of assets to immediately experience the benefits of AI-powered, platform-driven exposure management.¹

“Network scanning is a staple in virtually every security stack, and bringing it to the Falcon platform—and replacing legacy solutions—is one of our top customer demands,” said Elia Zaitsev, chief technology officer, CrowdStrike. “For too long, organizations have had to rely on hardware-dependent, difficult-to-deploy solutions with outdated risk models and static CVSS scores, requiring external threat feeds to even attempt prioritization. With the Falcon platform, everything is built in natively—the industry’s richest adversary intelligence, patented AI, and a lightweight agent adapted as a network scanner—allowing teams to extend adversary-based risk mitigation to network devices with a single click, meeting the demand for even greater consolidation on CrowdStrike.”

As adversaries evolve, traditional vulnerability management tools fail to address modern risk, missing how adversaries chain vulnerabilities together in real-world attacks. The [2025 CrowdStrike Global Threat Report](#) reveals that attackers increasingly exploit multiple low/medium vulnerabilities in sequence to escalate privileges and execute remote code, bypassing traditional risk prioritization models. Legacy scanning solutions lack the native threat intelligence and advanced AI capabilities to correlate vulnerabilities with real-world attack techniques. They also require dedicated agents and hardware, creating operational complexity without delivering true risk reduction. As a result, security teams are overwhelmed with static CVSS scores that fail to reflect how an adversary targets their attack surface, leaving critical gaps in exposure management.

Falcon Exposure Management prioritizes vulnerabilities based on adversary activity and real-world attack paths, allowing security teams to identify and mitigate risks before they lead to a breach. By understanding how attackers exploit multiple vulnerabilities in sequence, teams can [reduce critical vulnerabilities by up to 98%](#). With Network Vulnerability Assessment, CrowdStrike extends these capabilities to assets discovered over the network, providing comprehensive risk visibility, prioritization and automated remediation across the entire attack surface, without requiring additional scanners, agents or hardware. This brings another crucial aspect of modern security to the Falcon platform, helping organizations accelerate consolidation and eliminate the costs and complexity of managing numerous disjointed tools.

Key features and benefits include:

- **Real-Time, Continuous Network Assessments:** Eliminates reliance on outdated network scanning tools that create security blind spots. The Falcon platform leverages its existing lightweight agent as a network scanner, enabling instant, continuous assessments with no additional setup—providing real-time visibility into both managed and unmanaged network devices without causing congestion or disruptions.
- **AI-Driven Risk Prioritization:** Falcon Exposure Management’s patented [ExpRT.AI](#) pinpoints the 5% of vulnerabilities driving 95% of risk.² By analyzing adversary behavior, active exploits, and real-world threat intelligence, organizations can focus on the risks that matter most.
- **Cross-Domain Exposure Management:** Provides a single, consolidated view of exposures and attack paths across endpoints, cloud workloads, IT/IoT and network assets leading to business-critical assets and data, enabling teams to predict likely adversary behavior based on real-world activity to harden high-risk areas of exposure.
- **Automated Remediation with Falcon Fusion SOAR:** Traditional scanning tools leave teams burdened with manual remediation. Falcon Exposure Management, combined with [Falcon Fusion SOAR](#), delivers automated, real-time remediation—eliminating risks before they can be exploited.
- **Unified Platform Protection:** The combination of Falcon Exposure Management’s proactive security with the Falcon platform’s industry-leading threat prevention, detection and response across endpoints, cloud, identity and data, along with [Falcon® Next-Gen SIEM](#) and [Falcon® Complete Next-Gen MDR](#), provides organizations with the technology and services they need for full cycle threat protection across every area of enterprise risk.

Availability and Free Scanning

Network Vulnerability Assessment is now generally available as part of Falcon Exposure Management. All customers receive free scanning for up to 10% of their asset count with no additional setup required. For more information:

- Read our [blog](#)
- Visit our [website](#)
- Read our [Intermex customer story](#)

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/>

© 2025 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.

¹ Offer available to existing Falcon Exposure Management (FEM) customers only. Eligible customers will receive free Network Vulnerability Assessment (NVA) coverage for up to 10% of their currently licensed managed assets, capped at a maximum of 10,000 assets. Actual allocation may vary by license tier. Customers may scan additional unmanaged assets by purchasing additional FEM licenses.

² Falcon Spotlight Data

View source version on [businesswire.com](https://www.businesswire.com/news/home/20250323075726/en/): <https://www.businesswire.com/news/home/20250323075726/en/>

Media Contact

Jake Schuster

CrowdStrike Corporate Communications

press@crowdstrike.com

Source: CrowdStrike