CROWDSTRIKE
Investor Relations

CrowdStrike Unveils Falcon Next-Gen SIEM Support for Microsoft Defender for Endpoint, Advancing Open Security Architecture

March 23, 2026

Falcon Next-Gen SIEM ingests Microsoft endpoint telemetry with no Falcon sensor required, as new innovations accelerate legacy SIEM transformation across heterogeneous environments

AUSTIN, Texas & SAN FRANCISCO--(BUSINESS WIRE)--Mar. 23, 2026-- **RSA 2026** -- CrowdStrike (NASDAQ: CRWD) today announced that Falcon® Next-Gen SIEM now ingests and correlates Microsoft Defender for Endpoint telemetry, enabling Microsoft endpoint customers to modernize security operations without deploying additional sensors.

CrowdStrike also unveiled native Falcon® Onum real-time data pipelines, federated search across third-party data stores, third-party intelligence integration, and its Query Translation Agent. Together, these innovations accelerate legacy SIEM transformation by eliminating migration friction, reducing ingestion and storage costs, and delivering real-time threat detection across heterogeneous environments.

“Strategic alignment and disciplined execution between industry leaders is what drives meaningful innovation and stronger security outcomes for customers,” said Daniel Bernard, chief business officer at CrowdStrike. “Our integration with Microsoft accelerates legacy SIEM transformation without the operational burden of deploying additional sensors. By advancing our open, data-agnostic architecture, we are giving organizations the flexibility, performance, and data economics to modernize security operations across any technology stack – meeting customers where they are to unlock the protection outcomes and value from Falcon.”

“It is great to see Microsoft Defender telemetry being leveraged within Falcon Next-Gen SIEM,” said Rob Lefferts, corporate vice president for threat protection at Microsoft. “Defender operates at a global scale, and integrations like this reinforce the importance of an open ecosystem where leading platforms interoperate to help customers improve security outcomes.”

The Operating System of Cybersecurity

Falcon Next-Gen SIEM has proven itself a scaled market disruptor, with performance and cost advantages that set it apart from legacy SIEMs. Growing 75 percent year-over-year,[1] the business is accelerating adoption of the Falcon® platform as the operating system of cybersecurity.

Falcon Next-Gen SIEM for Defender

Falcon Next-Gen SIEM for Defender accelerates SOC modernization for organizations standardized on Microsoft Defender for Endpoint protection. Organizations can ingest and correlate Defender telemetry with Falcon’s log data, threat intelligence, cross-domain context, and AI-driven analytics in real time, augmenting native detections without deploying a new endpoint sensor.

Agentic SOC Transformation

To accelerate the transition to the agentic SOC, CrowdStrike is delivering new innovations that eliminate architectural barriers to modern SIEM adoption, simplifying data onboarding, reducing cost, and increasing operational speed.

- **Native Falcon Onum Integration:** Eliminates onboarding friction and transforms data economics, delivering up to 5X faster streaming, 50 percent lower storage costs, 70 percent faster incident response, and 40 percent less ingestion overhead through intelligent filtering and real-time, in-pipeline detection.
- **Federated Search Across Distributed Data Stores:** Extends fast, flexible access to external data sources, including Falcon LogScale and ExtraHop. Analysts can query data where it lives, eliminating costly duplication and re-ingestion while maintaining unified visibility.
- **Third-Party Indicator Management:** Enables ingestion and operationalization of external indicators of compromise (IOCs), enriching Falcon detections with curated, high-confidence threat correlation across first- and third-party data.
- **Query Translation Agent:** Expanding CrowdStrike’s Agentic Security Workforce, this intelligent agent automatically converts legacy SIEM queries, including Splunk searches, into CrowdStrike Query Language (CQL), accelerating migration, preserving analyst workflows, and eliminating retraining friction.

To learn more about Falcon Next-Gen SIEM:

- Visit booth #N-5845 at RSA
- Read our blog
- Visit our website

Future Products Disclaimer

This press release may include 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.

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

[1] FY26 Earnings

View source version on businesswire.com: https://www.businesswire.com/news/home/20260322055275/en/

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

Source: CrowdStrike