

Falcon Next-Gen SIEM for Third-Party EDR

Stop breaches faster with an open, unified, AI-native
SOC platform built for your ecosystem

Legacy SIEMs can't keep pace with adversaries exploiting siloed data

Legacy security information and event management (SIEM) solutions are slowing you down. In modern environments built on diverse endpoint and cloud platforms, siloed architectures create critical visibility gaps that adversaries exploit. Yet legacy SIEMs were designed for an age that's long since passed, when data volumes were smaller and breakout times were measured in hours, not minutes. Complex and costly, they have become data dumping grounds, forcing analysts to navigate multiple data sources, tools, and consoles to extract meaning from data and conduct investigations.

Legacy SIEMs struggle with slow search speeds and arduous data onboarding processes that delay time-to-value and drive up overall costs. To give security teams the speed they need to stop breaches, the modern SOC requires a platform that converges data, security, and AI while working seamlessly with your existing stack.

Powering the agentic SOC transformation

CrowdStrike Falcon® Next-Gen SIEM for Third-Party EDR reimagines security operations by delivering a cloud-native, petabyte-scale solution that gives you unprecedented visibility across all of your users and data. Leverage native CrowdStrike Falcon® endpoint telemetry already in the platform, or ingest data from your third-party endpoint technology, such as Microsoft Defender, alongside cloud and security tools through real-time CrowdStrike Falcon® Onum pipelines and an expanding ecosystem of connectors. Get full visibility, high-speed search, and AI-led investigations to stop breaches fast, while cutting costs.

Key benefits

- **Seamless data onboarding** with more than 175 data connectors and 260 parsers
- **ROI improvement:** Reduce overhead with Falcon Onum's smart filtering — cut telemetry ingest and storage costs by up to 50%¹
- **Blazing-fast search and petabyte scalability** up to 150x faster than legacy SIEMs²
- **Built for flexibility:** Route to Falcon, Amazon S3, a security orchestration, automation, and response (SOAR) solution, or any destination, with no vendor lock-in

¹ Numbers are projected estimates of average benefit based on the company's own internal analysis and recorded metrics provided by customers during pre-sale motions that compare the value of CrowdStrike with the customer's incumbent solution. Actual realized value will depend on the customer's module deployment and environment.

² Results are from a customer. Individual results may vary.

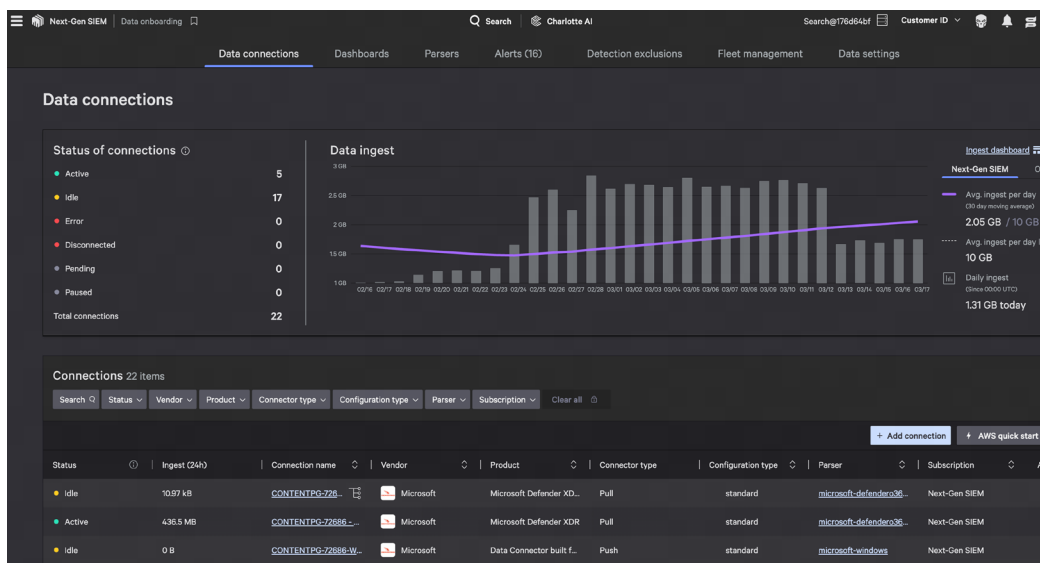


Figure 1. Seamlessly ingest Microsoft Defender data for unified visibility in Falcon Next-Gen SIEM for Third-Party EDR

Key capabilities

Detect in Real Time with Unified Data

- Easily extend visibility with integrations:** Leverage a growing set of data connectors and real-time Falcon Onum pipelines to unlock the power of your security ecosystem. Quickly realize the value of any data source with detection coverage management, and use AI-generated parsers to make onboarding a breeze.
- The key data you need in one platform:** Get immediate visibility with all critical data and threat intelligence already in the Falcon platform — or bring in your existing third-party endpoint, third-party intelligence indicators, and security data. Consolidate all threat detection, investigation, and response in one place, reducing context switching and accelerating analyst workflows.
- Adversary-driven detections, extended to all data sources:** Find sophisticated adversaries across first- and third-party data sources with out-of-the-box detection content designed for both Falcon and supported third-party endpoint platforms. Powered by advanced AI and behavior analysis, correlate signals from endpoint, cloud, identity, and network data to uncover cross-domain threats faster.

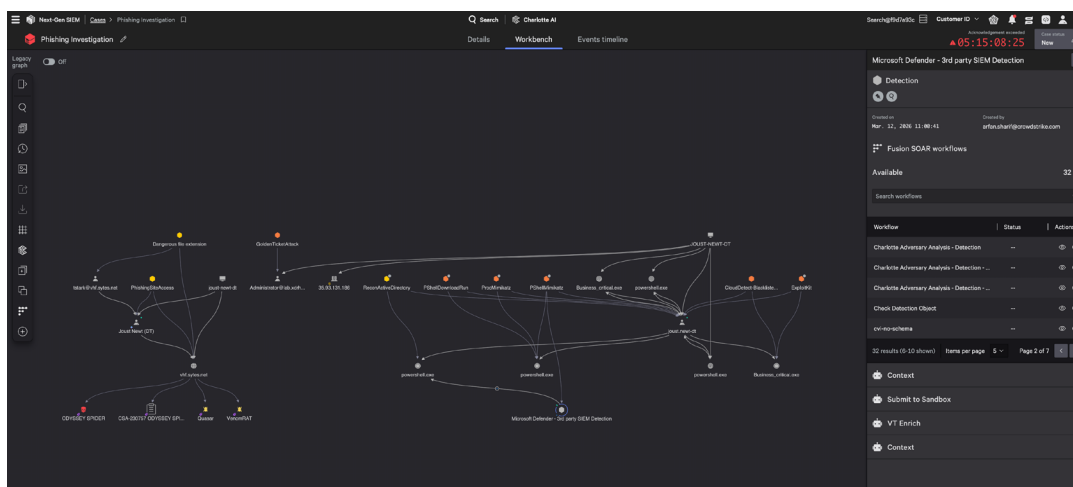


Figure 2. Visualize attacks across first- and third-party data with Workbench in Falcon Next-Gen SIEM.

Investigate in Seconds

- **Incident visualization that reveals the full path of an attack:** Instantly understand the scope of an attack in an elegant visual graph that correlates users, entities, and threat context so you can rapidly orient and respond.
- **Fast search and real-time collaboration:** Dramatically speed up investigations with search performance that's up to 150x faster than legacy SIEMs,² and collaborate instantly to quickly take action.
- **Generative AI, the ultimate force multiplier:** Elevate the skill level of your entire team by harnessing the power of generative AI to prioritize, enrich, and summarize incidents in plain language.

Stop the Breach with Workflow Automation and AI

- **Automated response with intuitive built-in workflows and actions:** Coordinate response across your security and IT stack with native workflow automation powered by CrowdStrike Charlotte Agentic SOAR. Agentic workflows and intelligent agent orchestration drive automated containment, remediation, and escalation, while integrated case management keeps investigations structured and collaborative.
- **Smart decisions and swift resolution with adversary intelligence:** Speed up incident response with world-class threat intelligence embedded directly into investigations and workflows. Ingest, enrich, and manage third-party indicators alongside CrowdStrike intelligence, scoring and deduplicating indicators of compromise (IOCs) to reduce noise and improve prioritization. Gain real-time context on adversaries and their tradecraft to drive faster, more confident resolution.
- **Orchestrate response across your ecosystem:** With more than 8,000 workflow actions and 160+ out-of-the-box playbooks, automate containment and remediation across endpoint, cloud, and security tools. Drive coordinated response across supported third-party endpoints and your entire stack.

Leverage Tailored Services and Flexible Licensing for SIEM Success

- **Migration services:** Leverage operational professional services and resident engineers to get up and running faster. Refine detections and dashboards for your desired use cases to enhance security posture.
- **Simplified procurement:** CrowdStrike Falcon® Flex gives the greatest value for maximum savings with an upfront commitment and flexible licensing for additional offerings and services.

"We're on the precipice of another major leap with Falcon Next-Gen SIEM. It's at least ten times faster than what we had before. The performance improvements have been game-changing, allowing us to instantly ingest Falcon platform data and third-party data for the ultimate visibility and threat hunting."

*– Steve McIntosh,
[Director of Threat Management and Response at Aflac](#)*

Request a Demo →

² Results are from a customer. Individual results may vary.

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/>

Start a free trial today: <https://www.crowdstrike.com/free-trial-guide/>

