CROWDSTRIKE

CrowdStrike Products

Data Sheet

# Falcon Next-Gen SIEM

Respond faster to stop breaches with a unified SOC platform

## Legacy SIEMs can't keep pace with adversaries

Legacy SIEMs are slowing you down. Complex and costly, they were designed for an age that's long since passed, when data volumes and adversary speed were a fraction of today's. 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.

## Powering SOC transformation

CrowdStrike Falcon® Next-Gen SIEM reimagines security operations by delivering a cloud-native, petabyte-scale solution that gives you unprecedented visibility across all of your users and data. The lightweight CrowdStrike Falcon® agent simplifies data collection for endpoints and cloud workloads, while an expanding set of data connectors harnesses the potential of all of your security tools and data. Get full visibility, high-speed search, and AI-led investigations to stop breaches fast, while cutting costs.

## Key benefits

- **Seamless data onboarding** with your Falcon data already in the CrowdStrike Falcon platform
- **Rapid migration and deployment** up to 3x faster than other solutions, further accelerated by expert services[1]
- **AI-led investigations** including AI-based report summarization, real-time collaboration, and incident visualization
- **Blazing-fast search and** petabyte scalability up to 150x faster than legacy SIEMs[1]
- **24/7 expert protection** and full-cycle remediation with CrowdStrike Falcon® Complete Next-Gen MDR
- **Up to 80% cost savings** compared to siloed solutions[2]

[1] Results are from a customer. Individual results may vary.

[2] This number reflects the median inputs provided by customers during pre- and post-sale motions that compare the value of CrowdStrike with incumbent solutions and are not guaranteed. They are intended to demonstrate potential value compared to incumbent solutions and do not represent promised outcomes. Actual value realized will depend on individual customer module deployment and environment.

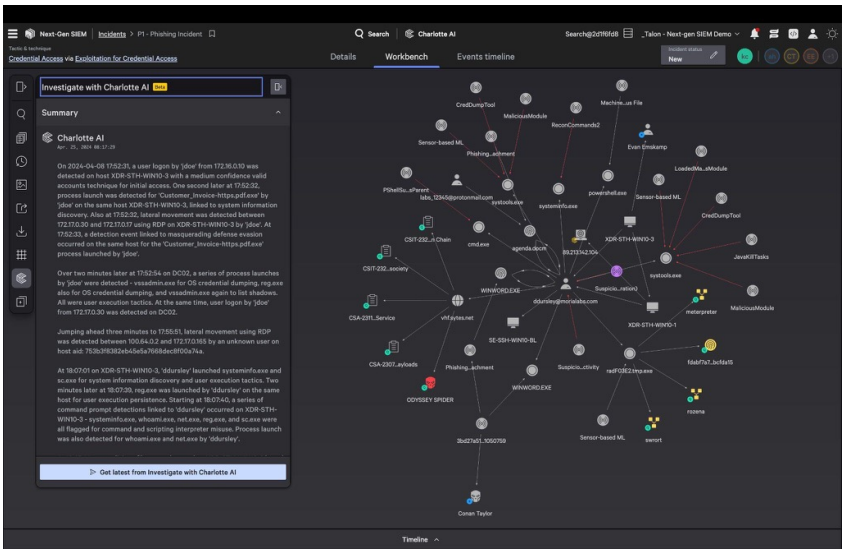


*Figure 1. Swiftly analyze threats in the Falcon Next-Gen SIEM Workbench*

# Key capabilities

## Detect in Real Time with Unified Data

- **Easily extend visibility with integrations:** Leverage a growing set of data connectors 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. Seamlessly discover additional integration content in-console with the unified content library, and extend visibility to more third-party tools.
- **The key data you need — built in:** Get immediate visibility with all critical data and threat intelligence already in the Falcon platform. Consolidate all threat detection, investigation, and response in one place, and avoid the time and cost of transferring data to a siloed, legacy SIEM.
- **Adversary-driven detections, extended to all data sources:** Find the most sophisticated adversaries across all data sources with detections powered by the same advanced AI and behavior analysis as CrowdStrike's industry-leading endpoint detection and response (EDR). CrowdStrike Signal uses self-learning AI to build models for every host that pinpoint subtle, early-stage threat activities and generate a single high-confidence lead. Context-rich UEBA with risk scores, entity resolution, and timelines empower teams to focus on the threats that matter most.

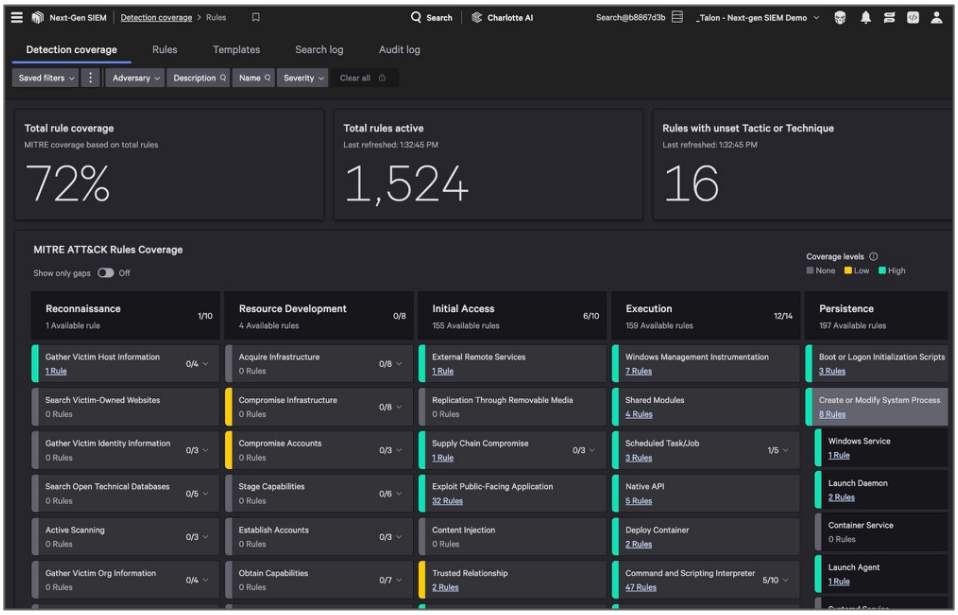


*Figure 2. Identify every attack with comprehensive detection content*

## 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.
- **Faster search and real-time collaboration:** Dramatically speed up investigations with search performance that's up to 150x faster than legacy SIEMs. Centralized case management seamlessly integrates with automated workflows, enhances collaboration, and tracks SLAs.
- **Uplevel analysts with AI:** With AI-powered investigations, analysts can quickly derive insights from searches, automate triage, prioritize and enrich alerts, and get incident summaries in plain language.

## Stop the Breach with Workflow Automation

- **Automated response with intuitive built-in workflows and actions:** Coordinate response across your security and IT stack with native workflow automation powered by CrowdStrike Falcon® Fusion SOAR. Build automation workflows effortlessly using CrowdStrike no-code visual builder or by describing them to CrowdStrike® Charlotte AI. More than 2,500 workflow actions in third-party tools let you fully eradicate threats and free up your team to focus on higher-order operations.
- **Smarter decisions and swifter resolution with adversary intelligence:** Speed up incident response with world-class threat intelligence and automation on your side. Get direct context on adversaries and their tradecraft from CrowdStrike's industry-leading threat intelligence.
- **Tight integration with the Falcon agent to drive any endpoint action:** Contain fast-moving attacks, limit lateral movement, and stop breaches through native integration with the Falcon agent for rapid response and optional recovery.

## 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.
- **Industry-leading managed security:** Falcon Complete Next-Gen MDR provides 24/7 expert support and full remediation while giving coverage across third-party data sources.
- **Simplified procurement:** CrowdStrike Falcon® Flex gives the most 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

## 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.**