CROWDSTRIKE

CrowdStrike Products
Data Sheet

Falcon Next-Gen SIEM

Respond faster to stop breaches with the definitive, AI-native SOC platform

Legacy SIEMs can't keep pace with adversaries

Stopping modern attacks requires SecOps teams to match the speed of the adversary. But as attack velocity and stealth increase, the legacy SIEM tools of the past have failed to adapt. Slow, 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 the AI-native SOC

CrowdStrike Falcon® Next-Gen SIEM delivers unprecedented speed and efficiency to stop breaches by unifying Falcon and third-party data, threat intelligence and workflow automation on the definitive AI-native SOC platform. Falcon Next-Gen SIEM delivers more capabilities and up to 150x faster search performance than legacy SIEMs, at up to 80% lower total cost of ownership. Built from the ground up around a modern security analyst experience, it consolidates AI-powered detections, investigation workflows and recommended response actions across all data on one platform, managed through a single console.

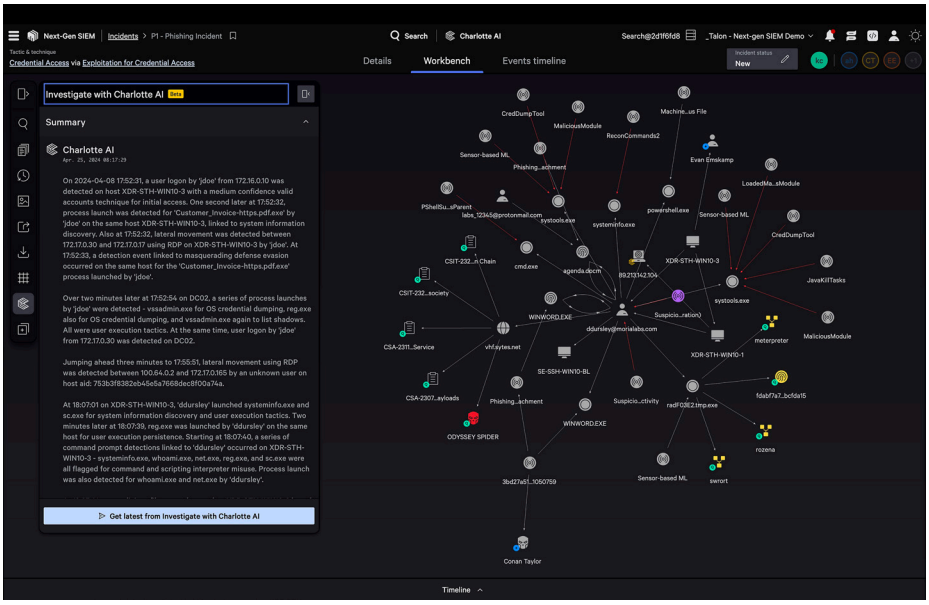
Your team can detect and respond faster than you ever thought possible with real-time alerts, live dashboards and world-class intelligence. Your threat hunters can scour petabytes of data at blazing-fast speed with index-free search. AI-assist features transform your entire SOC team into experts by correlating threats with adversary behavior to reveal the timeline and impact of an attack and automating manual investigation steps. What took hours or days now takes minutes — and years of human expertise will help power every decision your team makes.

Key benefits

- Achieve instant time-to-value with critical data already in the CrowdStrike Falcon® platform and easily extend data collection to third-party data sources
- Reduce mean time to respond and say goodbye to tedious tasks with workflow automation
- Coordinate response across your infrastructure and drive any endpoint remediation action through tight integration with the Falcon agent
- Slash SOC costs by consolidating tools and streamlining operations on a single-agent, single platform architecture

CrowdStrike Products

Falcon Next-Gen SIEM



Swiftly analyze incidents in the Falcon Next-Gen SIEM Incident Workbench

Falcon Next-Gen SIEM reimagines security operations by delivering a cloud-native, petabyte-scale platform that gives you unprecedented visibility across all of your users and data. The lightweight 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.

Superior outcomes at a fraction of the cost of legacy SIEMs

With Falcon Next-Gen SIEM, you can safeguard your business with industry-leading, comprehensive security from the company that understands adversaries better than anyone. You can rest easy knowing experts from the world's top managed detection and response (MDR) provider are working around-the-clock for you. And for the first time ever, your team can leverage one unified data platform to hunt down and eliminate threats, address compliance and overcome any security challenge you face.

Key capabilities

Detect in real time with unified data

- **Out-of-the-box integrations that unlock the power of your security ecosystem:** Leverage a growing set of data connectors to easily collect data from any source so you can spend more time fighting threats and less time onboarding data.
- **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).

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 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

- **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. More than 125 workflow actions 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 CrowdStrike Falcon agent for rapid response and optional recovery.

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/

Request a free demo →