CROWDSTRIKE

CrowdStrike Products
Data Sheet

Falcon Next-Gen SIEM

Stop breaches by harnessing the speed and intelligence of the world's leading AI-native security platform

Legacy SIEMs can't keep pace with adversaries

Legacy SIEMs have failed the SOC. Excruciatingly 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.

Legacy SIEMs force security teams to spend more time setting up and maintaining log sources and rules rather than stopping breaches. SOC analysts have no choice but to waste endless hours manually triaging a massive volume of alerts and pivoting from console to console to uncover root cause, with agonizingly slow searches delaying investigations and increasing dwell times.

Soaring SIEM costs compound these risks by preventing teams from logging and retaining all of their data, causing blind spots and missed attacks. It's time for a new approach to security operations.

Pioneering the future of the AI-native SOC

CrowdStrike Falcon® Next-Gen SIEM revolutionizes threat detection, investigation and response by bringing together unmatched security depth and breadth in one unified platform to stop breaches. Falcon Next-Gen SIEM extends the industry's most dominant EDR, threat intelligence and expert services to all data sources for complete visibility and protection. Built from the ground up around a modern security analyst experience, it amplifies the speed and efficiency of incident response, so you can swiftly root out adversaries while slashing SOC costs.

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 up to 150x times faster than legacy SIEMs with index-free search. Analyst-assist technologies transform all of your team members into experts by automating manual investigation steps and giving them a full picture of attacks with rich context. What took eight hours now takes eight minutes — and years of human expertise will help power every decision your team makes.

Key benefits

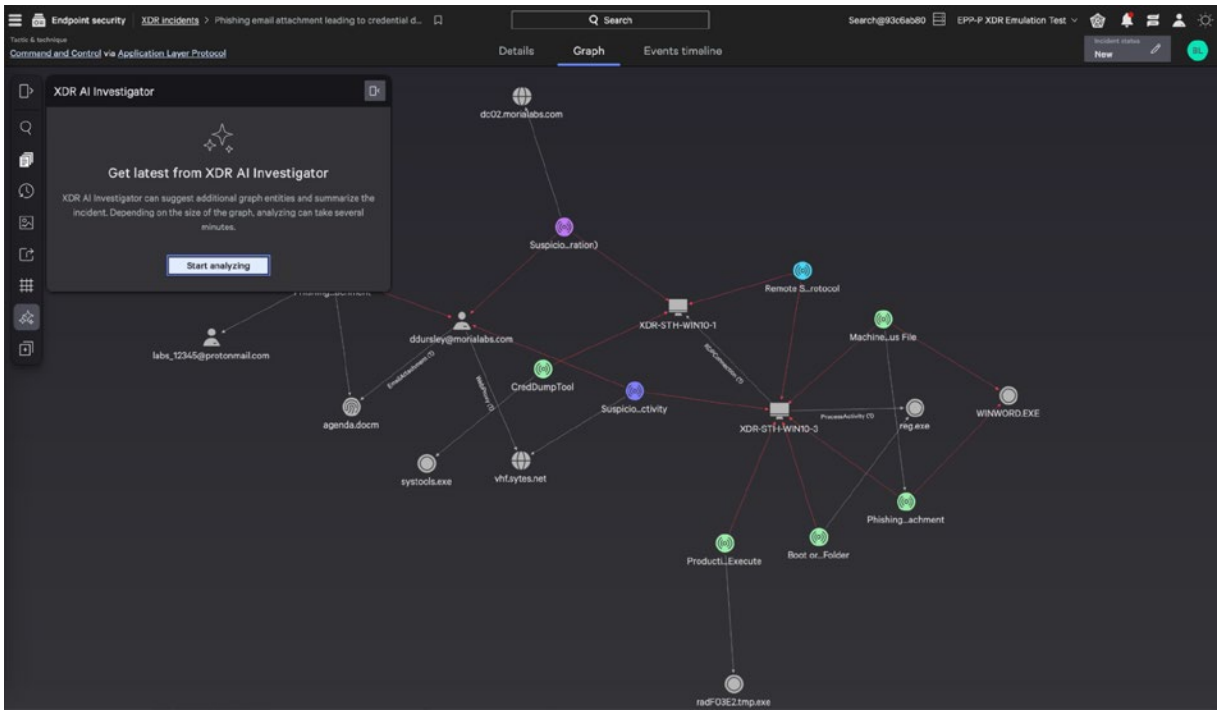
Detect threats in real time with AI-powered analytics and correlation rules

Uplevel your analysts with world-class intelligence and Charlotte AI, the engine powering CrowdStrike's portfolio of generative AI capabilities

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, streamlining operations and reducing capex compared to legacy SIEMs



Swiftly analyze incidents using XDR AI Investigator in Falcon Next-Gen SIEM

Falcon Next-Gen SIEM reimagines security operations by delivering a cloud-native, petabyte-scale platform that gives you unprecedented visibility across your entire digital estate. The lightweight Falcon agent simplifies data collection across endpoints and 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 round-the-clock for you. And for the first time ever, your team can leverage one unified data platform to hunt down and eliminate threats and address the compliance obligations and security challenges you face.

Key capabilities

Immediate time-to-value with simplified data onboarding and high-fidelity detections:

- **Out-of-the-box integrations to unlock the power of your security ecosystem:** Leverage a growing set of native data connectors, the CrowdStream observability pipeline and the Falcon Log Collector 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 instant, native visibility from a unified, lightweight agent for endpoints, identities, cloud workloads and data protection. Break down silos and eliminate duplicate data stores by consolidating all threat detection, investigation and response in one high-performance platform.
- **Leading AI-powered 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).

Lightning-fast analysis with AI-led investigations:

- **Complete context for rapid, informed decisions:** Instantly understand an adversary's entire attack path across any data source with an elegant visual graph that unifies all threat context with user risk, vulnerabilities and asset relationships.
- **AI-native analyst-assist features:** Transform the investigative experience with AI-generated incidents that stitch together all related alerts, context and industry-leading threat intelligence with a plain-language summary of the adversary's actions.
- **Charlotte AI, the ultimate force-multiplier:** Ask any question to streamline investigations leveraging the power of high-fidelity data and generative AI. Users of all skill levels can elevate their ability to stop breaches with the optional Charlotte AI module.

Coordinated response to eliminate threats anywhere in your environment:

- **Fast resolution with fully integrated response:** Speed up investigation and response with leading threat intelligence and automation on your side. More than 125 workflow actions let you fully eradicate threats and free up your team to focus on higher-order operations.
- **Native SOAR capabilities to supercharge productivity:** Instantly stop adversaries with workflow automation, powered by CrowdStrike Falcon® Fusion, to orchestrate remediation actions across the CrowdStrike platform and third-party tools — all from one, unified console.
- **Tight integration with the Falcon agent to drive any endpoint action:** Leverage powerful Falcon platform features, such as Falcon Real Time Response, to contain fast-moving attacks and limit adversary lateral movement using pre-built commands and extensible scripts.

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.

See Next-Gen SIEM in Action →

This document includes forward-looking statements including, but not limited to, statements concerning the expected timing of product and feature availability, the benefits and capabilities of our current and future products and services, and our strategic plans and objectives. Such statements are subject to numerous risks and uncertainties and actual results could differ from those statements. Any future products, functionality and services may be abandoned or delayed, and customers should make decisions to purchase products and services based on features that are currently available.