

Falcon Next-Gen SIEM: AI-driven Enhancements

Supercharge and transform your SOC with AI, automation, and adversary intelligence

In threat detection and response, time is everything. Adversaries are getting faster, breaking out from compromised endpoints in as little as **51 seconds**. Yet security teams are held back by the very tools meant to help them — tools that are slow, disjointed, and overly complex. They are overwhelmed by lengthy deployment processes, endless, low-fidelity alerts, and manual investigations. While security teams make progress, it's still an uphill battle — one where AI and automation can deliver a decisive advantage.

CrowdStrike Falcon® Next-Gen SIEM optimizes every stage of the security operations process with automation and AI that help security analysts work faster and smarter. With its streamlined data onboarding experience, redefined approach to user and entity behavior analytics (UEBA), integrated case management, and GenAI-powered security orchestration, automation, and response (SOAR) workflows, your team can make SIEM data actionable faster, focus on the threats that matter most, and streamline investigation and response — so you can boost productivity and reduce your mean time to respond (MTTR).

Key capabilities

Make SIEM Data Actionable Faster with a Simplified Data Onboarding Experience

Security teams often encounter significant challenges when deploying a SIEM, impacting operational efficiency, scalability, and detection accuracy. Falcon Next-Gen SIEM reimagine the data onboarding experience, which combined with AI-assisted parser creation and agile rule development, reduces the friction and accelerates time-to-value. With a smoother onboarding experience, security teams can start getting value from their data right away and focus on security, not busywork.

Key features

- **Streamlined data onboarding:** Get value from new data sources in minutes with an intuitive data onboarding experience, AI-generated parsers, and scalable rule creation.
- **Expert-led threat hunting:** Augment your threat hunting capabilities with the unmatched expertise of CrowdStrike Falcon® Adversary OverWatch™.
- **Context-rich UEBA:** Reduce false positives, prioritize real threats with an AI-powered risk score, and automatically gather context to make fast, informed decisions.
- **Analyst-centric case management:** Centralize investigations, enhance collaboration, and orchestrate response — from a unified source of truth.
- **Agentic AI-powered SOAR workflows:** Harness state-of-the-art large language models (LLMs) in SOAR workflows to build configurable agentic AI-powered workflows.

Falcon Next-Gen SIEM: AI-driven Enhancements

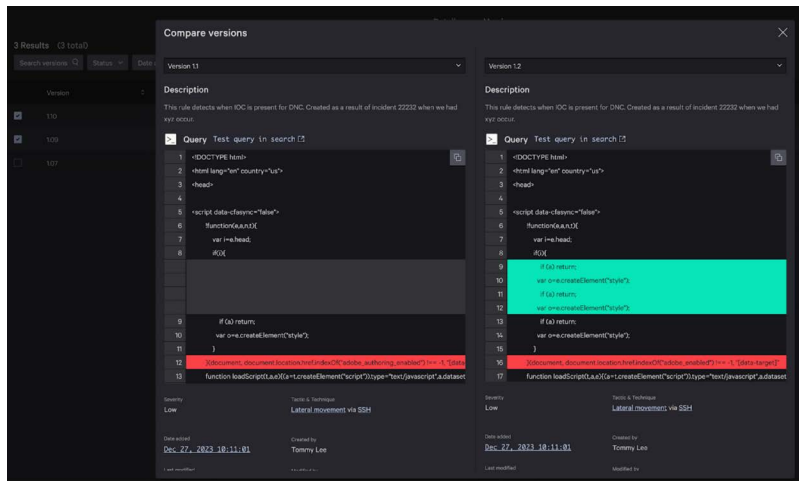


Figure 1. The Detection-as-Code authoring experience enables security teams to build complex detection rules by applying software engineering principles.

- **Simplify setup with a streamlined data onboarding experience:** SIEM data onboarding is often complex and resource-heavy. Falcon Next-Gen SIEM simplifies the process with an enhanced experience that helps teams quickly ingest log sources and monitor connections for optimal efficiency. The new Data Connections page offers a unified view to discover, configure, and manage data sources. Analysts can validate status, track parsers and custom mappings, visualize ingestion patterns, and troubleshoot issues in real time.
- **Reduce parser setup time from days to minutes with AI-generated parsers:** Building parsers used to require specialized skills. Now, AI removes the complexity. Powered by advanced LLMs, CrowdStrike's AI-generated parsers automatically create validated parsers built to CrowdStrike Parsing Standard (CPS), ensuring consistency, reliability, and easy customization. Parsers integrate seamlessly with data connectors, streamlining log ingestion and optimizing performance to fit your needs.
- **Build, customize, update, and scale detection rules with Detection-as-Code:** Falcon Next-Gen SIEM's Detection-as-Code experience lets security teams easily build and manage advanced detection rules. By applying software engineering principles to detection engineering, teams can uncover threats faster while maintaining scalable, auditable, and robust detection. This structured framework simplifies rule deployment, version control, and auditing — reducing risk and ensuring long-term agility.

Falcon Next-Gen SIEM by the numbers:

- **150x** faster search to speed up detection, investigation, and response
- **1PB/day** of data ingestion at massive scale for real-time security operations
- **325+** data sources supported for rich visibility, deep context, and better detections
- **Up to 4.7 trillion** events processed per day by Falcon Adversary OverWatch
- **1,500+** SOAR actions to boost productivity and accelerate response
- **Up to 80%** cost savings compared to legacy SIEM¹

¹ These numbers are projected estimates of average benefit based on 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 an individual customer's module deployment and environment.

Shift to Proactive Security Operations with AI-Powered Threat Hunting

Threat hunting adds strategic depth to security operations by empowering you to proactively catch threats early and actively searches for signs of compromise using human intuition, threat intelligence, and data queries. Falcon Next-Gen SIEM enables threat hunting at unmatched speed and scale with natural language or structured queries to search data, superior threat intelligence to enrich hunts, graph visualizations to understand relationships, and CrowdStrike Charlotte AI™ to summarize findings or assist with hypotheses.

You can further amplify your threat hunting efforts with the expertise of Falcon Adversary OverWatch Next-Gen SIEM, the industry's only managed threat hunting solution that proactively hunts adversaries everywhere across all attack surfaces, leveraging first-party endpoint, identity, and cloud data, and third-party Falcon Next-Gen SIEM data. Complementing Falcon Next-Gen SIEM, Falcon Adversary OverWatch delivers real-time, expert-driven threat hunting across network edge devices, SaaS applications, email security, and operating systems — stopping adversaries before they breach the network.

Reduce False Positives with Context-rich User and Entity Behavior Analytics (UEBA)

Technology and adversaries are continuously evolving, and with context-rich UEBA, CrowdStrike will redefine how organizations detect, prioritize, and triage threats. Adversaries deliberately navigate environments in ways that appear normal to avoid triggering detection based on abnormal activity. To counter this, it's crucial to analyze detections from all sources — with the right contextual information — to identify malicious behavior.

CrowdStrike's approach to UEBA will let you do this at scale by detecting threats with behavioral detections and analytics and prioritizing high-fidelity detections with an AI-powered risk score that can be further customized by security teams to meet their organization's requirements. Falcon Next-Gen SIEM automates investigations by collecting the relevant entity information needed to visualize and understand attacks — all within a fully integrated, unified security platform designed to stop breaches.

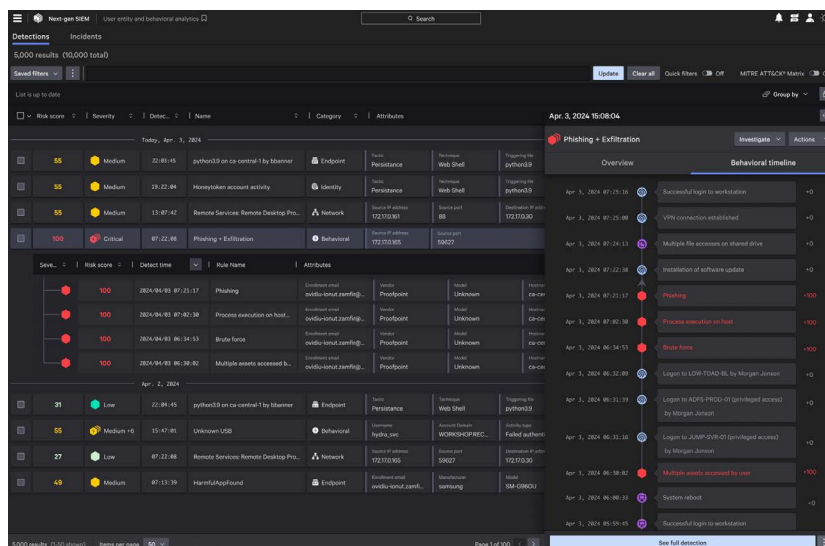


Figure 2. UEBA provides an AI-powered risk score to prioritize high-fidelity detections at scale and automate entity resolution to accelerate the investigation process.

With context-rich UEBA, security analysts can:

- **Detect unknown and evasive threats with high-fidelity behavioral detections:** Modern adversaries continuously evolve their tactics, techniques, and procedures (TTPs), making signature-based detections insufficient. Advanced behavioral detections can identify stealthy, multi-stage attacks by analyzing the sequence and relationship between events. Falcon Next-Gen SIEM leverages unmatched data — combining comprehensive endpoint telemetry from the CrowdStrike Falcon® platform with third-party data — to deliver superior behavioral detections. Analysts can use built-in detections or create their own with a guided authoring experience. By focusing on how attackers operate — rather than indicators of compromise (IOCs) and signatures — security teams can reduce false positives and find stealthy threats faster.

These behavioral detections are in addition to behavioral analytics provided by CrowdStrike Falcon® Identity Protection. Behavioral analytics offers deep visibility into user and entity behavior and accurate threat identification by establishing baselines of normal user activity and detecting anomalies. And, the recent innovations from Falcon Identity Protection deepen the integration with Falcon Next-Gen SIEM and CrowdStrike Falcon® Fusion SOAR, empowering users to identify and prioritize threats with identity-driven dashboards and automatically kick off the response process with multifactor authentication (MFA) and Active Directory response actions.

- **Prioritize alerts with confidence with an AI-powered, high-confidence risk score:** Analysts can focus on the threats that matter most by prioritizing detections based on a dynamic detection score for all alerts across first-party and third-party data. The detection score is powered by machine learning, enriched with insights from CrowdStrike Falcon® Complete Next-Gen MDR, and customizable based on each organization's needs and risk tolerance. A clear explanation of the score is readily available to analysts, helping them understand how the score was calculated and guiding them through investigation and remediation steps.
- **Save time with automatic entity resolution across first-party and third-party alerts:** Falcon Next-Gen SIEM unifies rich endpoint telemetry, broad third-party data, and industry-leading threat intelligence to deliver automatic entity resolution — eliminating the tedious, manual task of identifying and linking users and hosts across sources. Security analysts can easily correlate and track entities across massive datasets with contextual information, such as agent ID, IP address, username, and email address. They can also visualize risk trends and attack timelines to better understand the steps taken by the adversary and make informed decisions.

Streamline Investigation and Response with Centralized Case Management

Case management will empower analysts to handle investigation and response with greater efficiency, accuracy, and consistency, reducing response time. With integrated case management at the core of Falcon Next-Gen SIEM, security analysts can centralize insights, understand relationships, and collaborate effectively to resolve incidents faster than ever.

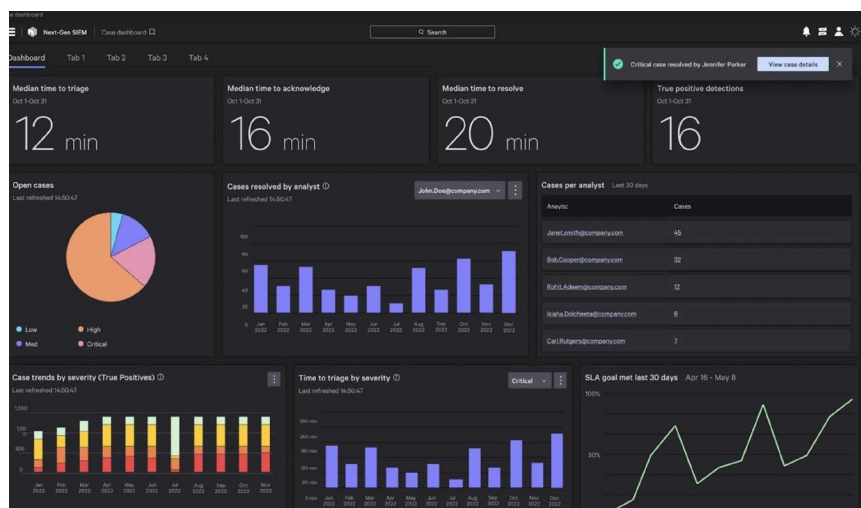


Figure 3. The Case Management dashboard enhances SOC daily operations with a unified view of key metrics to continuously improve performance.

By centralizing investigations, security teams can:

- Drive cohesive response with case management as the unified source of truth:** Falcon Next-Gen SIEM delivers a case-centric approach to investigation and response, improving workflows with robust case management that becomes the source of truth across the SOC. Cases can be created automatically from detections or manually using standardized or custom templates to define how an analyst should triage and respond to the case. Once created, case management orchestrates analyst assignments, notifications, SLAs, and escalations, ensuring efficient coordination. Seamless integration with the Workbench and Investigate with Charlotte AI enhances the analyst experience by providing at-a-glance visualizations, real-time collaboration, and expert-level AI assistance for tasks such as case summarization.
- Take decisive action with Falcon Fusion SOAR's workflow automation:** Falcon Fusion SOAR integrates seamlessly with Case Management to automate manual, repetitive tasks, freeing analyst time to focus on high-value operations. From auto-generating cases and adding contextual data to triggering enrichments and taking action, Falcon Fusion SOAR orchestrates workflows to reduce time to resolution. By automating any action as a workflow step, security teams will be able to automate end-to-end case resolution, from basic triage to high-volume use cases such as phishing. Additionally, it orchestrates investigation and response across the Falcon platform and third-party tools, featuring bi-directional integration with leading IT ticketing systems like ServiceNow for a cohesive and comprehensive response.

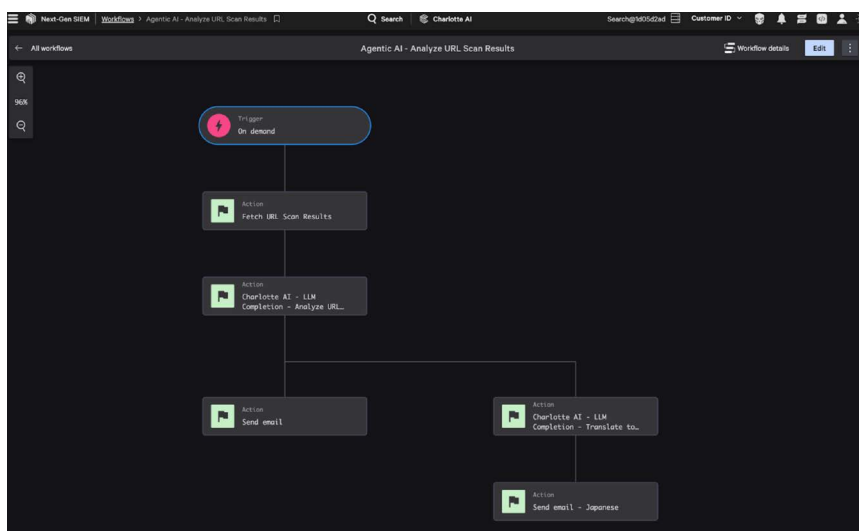


Figure 4. Reimagine workflow automation with Charlotte AI Agentic Workflows.

Furthermore, Falcon Fusion SOAR empowers your security teams to create powerful AI workflows that harness state-of-the-art LLMs, powered by Charlotte AI. Security analysts, of varied skill levels, will be able to design, test, and deploy sophisticated agentic sequences configured to the triggers, LLMs, data inputs, and actions of their specification.

- **Optimize SOC performance continuously with actionable, data-driven metrics:** Case management dashboards allow SOC managers to monitor operational efficiency with detailed case metrics, including mean time to triage, median time to acknowledge, and mean time to resolve. Additionally, it provides visibility into open cases, case trends by severity, analyst workload, and SLA performance over time.

Consolidate Security Operations in the Industry-Leading Falcon Platform

Built on the AI-native Falcon platform, Falcon Next-Gen SIEM transforms your SOC with automation and AI, enabling security teams to operate at high speed with greater efficiency and precision — all from a unified platform designed to stop breaches. Falcon Next-Gen SIEM's seamless integration with other CrowdStrike modules and services, such as Falcon Identity Protection, Charlotte AI, and Falcon Adversary OverWatch, provides security teams with more robust capabilities and elite threat hunters to accelerate threat detection, hunting, and response.

Free trial

Availability of Future Products

The product descriptions in this data sheet include forward-looking statements including, but not limited to, statements concerning feature availability, and the benefits and capabilities of our current and future products and services. Customers should make decisions to purchase products and services based on 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/>

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

