

What's New with Falcon Next-Gen SIEM

Features and functionality announced at
Fal.Con 2025

CrowdStrike is redefining security operations for the agentic era, unveiling AI-powered next-gen SIEM innovations that transform complex SIEM operations into intuitive experiences to accelerate threat detection and maximize SOC efficiency. With the acquisition of Onum, CrowdStrike is now supercharging these innovations with real-time pipeline intelligence and autonomous in-stream detection directly in CrowdStrike Falcon® Next-Gen SIEM.

Onum: Real-time data pipelines to power the AI-native SOC

Security teams are drowning in data while adversaries move at machine speed. Legacy SIEMs can't keep up, forcing teams into costly tradeoffs that create blind spots, noise, and delayed detections. Onum changes the game with real-time telemetry pipelines that transform data in motion into high-fidelity intelligence. By delivering the right data to the right place at the right time, Onum accelerates Falcon Next-Gen SIEM adoption and powers the SOC for the agentic security era.

- **Accelerates Falcon Next-Gen SIEM onboarding:** Simplify migration with instant ingestion and optimization of telemetry from any source.
- **Stops drowning in noise:** Filter and enrich data in milliseconds, reducing alert fatigue and analyst burnout.
- **Reduces costs with smarter data:** Cut storage and ingestion overhead by up to 50% with optimized, high-value streams.¹
- **Fuels AI-powered defense:** Get AI-ready, high-fidelity telemetry that boosts Falcon detections and agentic automation.
- **Transforms SOC efficiency:** Process up to 5x more events per second² and achieve up to 70% faster³ incident response.

Together with Falcon Next-Gen SIEM, Onum sets the new standard for SOC transformation — empowering security teams to move faster, cut through the noise, and stop breaches in the agentic era.

Key new features

- **Eliminate data chaos:** Onum delivers the right data, in the right place, at the right time.
- **Battle-ready AI agents:** Uplevel analyst performance and transform complex SIEM operations with intuitive, conversational experiences.
- **AI-powered SOAR:** Respond to threats at lightning speed by combining user-friendly workflow automation, dynamic case management, and breakthrough AI capabilities.
- **Centralized content:** Realize value faster with out-of-the-box integrations and content.

¹ This number is a projected estimate of average benefit based on Onum'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 a customer's module deployment and environment.

² 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.

³ This number is a projected estimate 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.

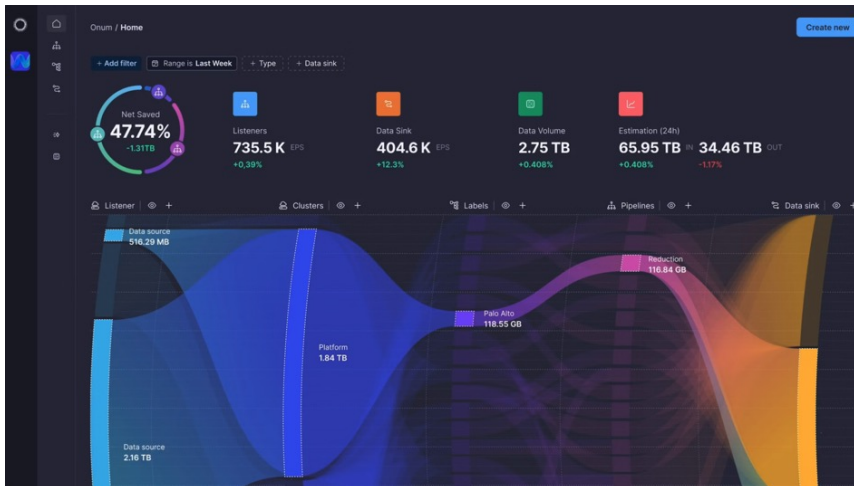


Figure 1. By processing data at the source, Onum enables real-time decisions while simplifying complex workflows and cutting costs.

Key capabilities

Transform Complex SIEM Operations with Intelligent Agents

Leverage the power of natural language interactions to derive instant insights, optimize detection rules, and automate workflows without specialized expertise. Intelligent agents eliminate operational complexity, allowing analysts to focus on what matters most — staying ahead of threats. By combining advanced AI capabilities with human expertise, security teams can now operate with unprecedented speed and precision across the entire threat detection and response lifecycle.

- **Search Analysis Agent:** Analyze complex queries by naturally asking questions about security event data through an intuitive chat interface. Analysts can explore security data relationships, receive instant insights, and analyze findings through clear, actionable formats, making advanced event searching and complex threat hunting accessible to all.

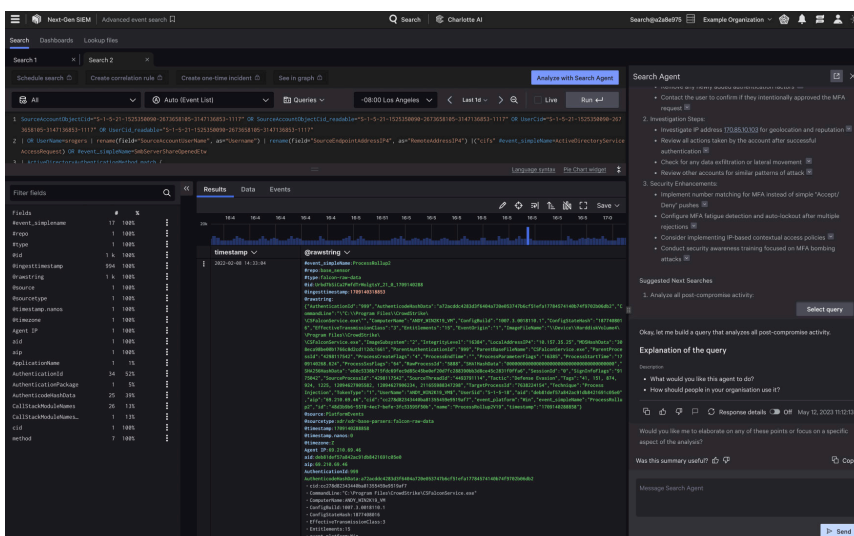


Figure 2. Ask questions about your security event data in natural language to receive instant insights and analysis.

- **Correlation Rule Generation Agent:** Create optimized detection rules with an intelligent assistant that dynamically generates detection rules. This AI agent provides guided authoring experiences for analysts of all skill levels, eliminating the need for query language expertise while enabling high-quality detection rules.

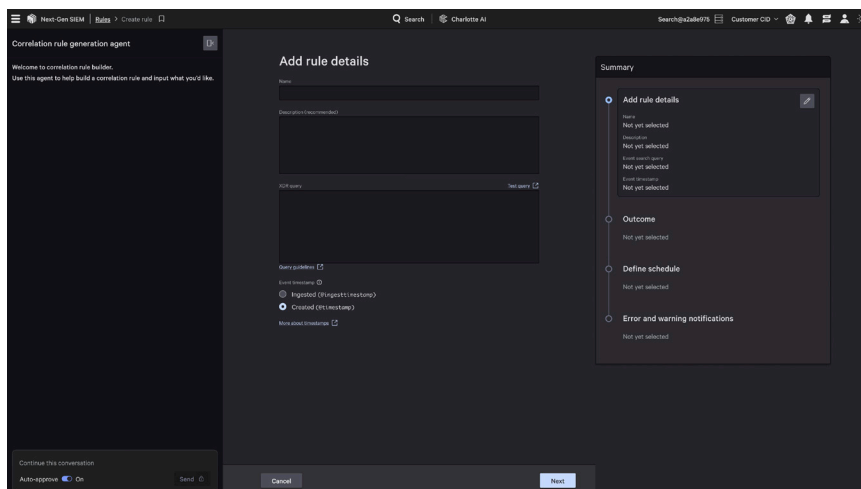


Figure 3. Generate, validate, and optimize detection rules without being a query language expert.

Falcon Next-Gen SIEM by the numbers

- Up to **150x** faster search for rapid detection and incident response⁴
- **2,500+** SOAR actions for instant productivity and faster response
- **1PB/day** of data ingestion, driving scale and full visibility
- Up to **80%** cost savings to maximize ROI⁴

Power Faster and Smarter SOAR with Conversation AI Agents

Security teams are slowed down by complex SOAR platforms, repetitive tasks, and manual coding requirements. CrowdStrike Falcon® Fusion SOAR combines intuitive workflow automation, dynamic case management, and breakthrough AI capabilities to let security teams operate at lightning speed. Respond to threats faster while giving your team valuable time back.

- **Workflow Generation Agent:** Convert prompts into SOAR workflows using AI and natural language to create complex workflows directly from the no-code workflow builder. This AI agent eliminates the need for specialized expertise, enabling users of all skill levels to build sophisticated automation workflows efficiently in minutes.

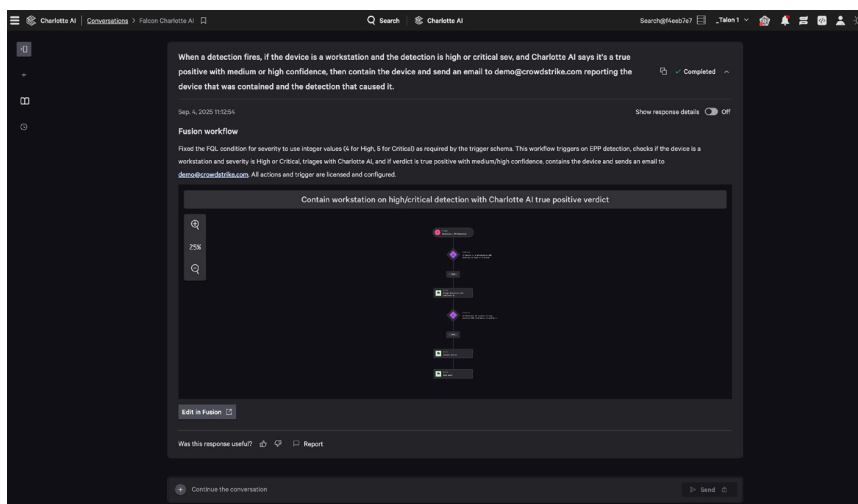


Figure 4. Turn prompts into playbooks at the speed of AI, from simple tasks to advanced agentic workflows, activating AI reasoning and action across the SOC.

⁴ 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.

- **Data Transformation Agent:** Normalize data for interoperability with an AI agent that simplifies data transformation between security tools through natural language inputs. Users can effortlessly convert data formats without requiring coding expertise or complex syntax knowledge, streamlining integration across the security stack.

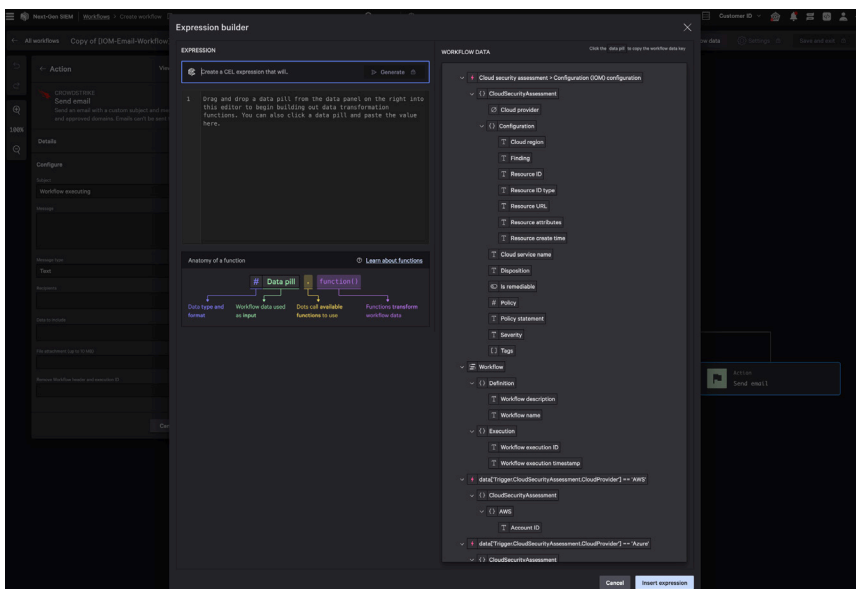


Figure 5. Accelerate data transformations use cases, such as building advanced conditions, without the need to learn another expression language.

- **Case management enhancements:** Streamline investigation and response with efficiency, accuracy, and consistency to reduce response time. With the new enhancements, security teams will be able to mirror ServiceNow cases, merge cases, and automatically create cases from correlation rules — all in one unified workspace.

Get Rapid Value with Out-of-the-Box Content

The unified content library provides security teams with a central hub to access and deploy readily available content for Falcon Next-Gen SIEM. Analysts can discover various content types and deploy in minutes to maximize value from Day One and adapt to threats fast.

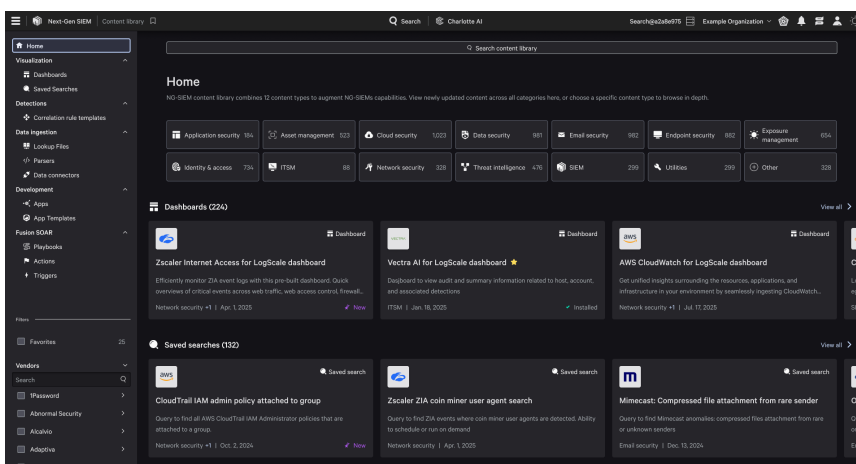


Figure 6. Discover and deploy out-of-the-box content from the unified content library.

With the unified content library, your team will streamline the onboarding experience with new content, such as parsers, dashboards, and queries, complementing existing SOAR integrations, playbooks, and CrowdStrike Falcon® Foundry apps.

Drive smarter security operations with the power of AI

Falcon Next-Gen SIEM redefines security operations by combining intelligent agents, advanced detections and UEBA, and AI-powered SOAR in one powerful platform. From natural language workflow creation to dynamic threat detection and unified case management, security teams can now operate with unprecedented efficiency. Organizations can deploy enterprise-grade SIEM capabilities that scale on demand.

Experience the future of security operations, where AI-powered threat detection and response meets human expertise to stop breaches faster than ever before.

Free Trial

Availability of Future Products

This data sheet includes descriptions of products, features, or functionality which may not be currently generally available. Any such references are provided for information purposes only. The development, release, and timing of all features or functionality remain at our sole discretion and may change without notice. These statements are subject to risks, uncertainties, and assumptions that may cause actual results to differ materially from those expressed or implied. Customers should make purchasing decisions based only on services and features that are currently generally available. For more information on our existing offerings please talk to your CrowdStrike representative.

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/>

