

Falcon Next-Gen SIEM: Simplify Security Data Onboarding

Reimagine speed, control, and visibility from Day One

Complexity is the enemy of security

With the volume and variety of security data continuing to grow, organizations struggle to efficiently ingest, normalize, and correlate information from disparate sources. CrowdStrike Falcon® Next-Gen SIEM eliminates these data silos by unifying security telemetry across the enterprise within a single AI-native platform. And CrowdStrike Falcon® Onum streamlines data ingestion and transformation, ensuring that every piece of security telemetry is enriched, structured, and ready for analysis. By simplifying data onboarding and normalization, teams can accelerate detection, investigation, and response without the complexity of traditional SIEM solutions.

Build an AI-ready foundation with Falcon Onum

Falcon Onum transforms data onboarding 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, Falcon Onum accelerates Falcon Next-Gen SIEM adoption and powers the SOC for the agentic security era.

- **Ingest Anything Instantly:** Get real-time telemetry routing from any source — normalized, enriched, and ready for detection.
- **From Prompt to Pipeline:** The Data Onboarding Agent turns natural language into working pipelines in minutes.
- **Stop Drowning in Noise:** Filter and enrich data in milliseconds, reducing alert fatigue and analyst burnout.
- **Reduce Costs with Smarter Data:** Cut storage and ingestion overhead by up to 50% with optimized, high-value streams.¹
- **Fuel AI-powered Defense:** Get AI-ready, high-fidelity telemetry that boosts Falcon detections and agentic automation.
- **Transform SOC Efficiency:** Process up to 5x more events per second² and achieve up to 70% faster incident response.³

Key benefits

- **Up to 3x Faster Deployment⁴:** Key data sources like endpoint, identity, and cloud telemetry are already part of the Falcon platform — no integration or duplication needed.
- **Flexible Data Ingestion:** Ingest data from other tools using a variety of methods, including hundreds of prebuilt connectors, cloud connectors, and open log collectors.
- **Parsers in Minutes:** Create and modify AI-generated parsers that are compliant with CrowdStrike Parsing Standards (CPS) in minutes to extract and normalize log data.
- **Unified, Real-time Visibility:** Continuously monitor connection and parser health with a centralized dashboard that eliminates guesswork and enables fast troubleshooting.

¹ These numbers are projected estimates of average benefit based on Onum's the company'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.

⁴ Results are from a customer. Individual results may vary.

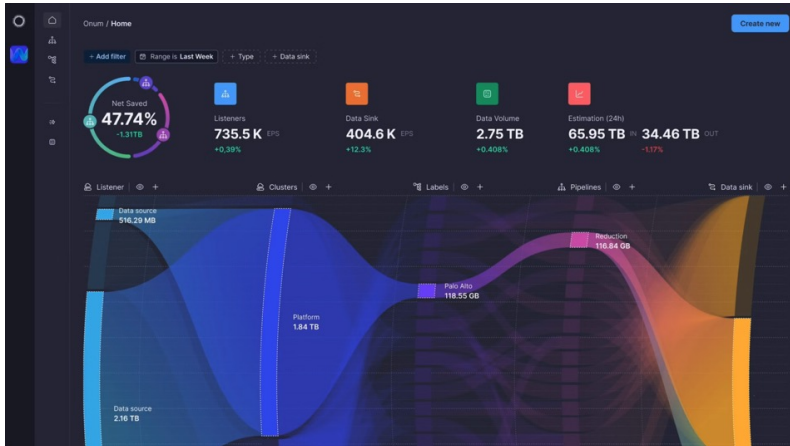


Figure 1. By processing data at the source, Falcon Onum enables real-time decisions while simplifying complex workflows and cutting costs.

Extend visibility across your ecosystem

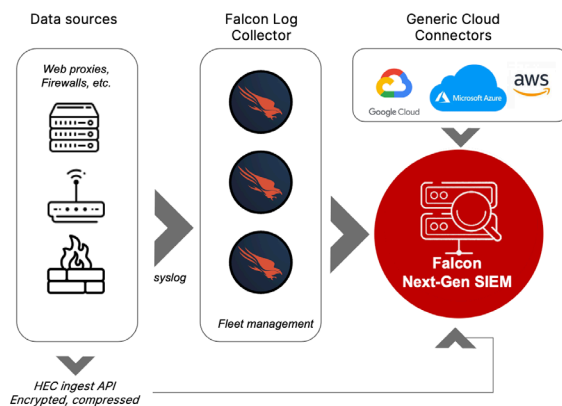


Figure 2. Extend visibility to existing tools outside the Falcon platform using a lightweight collector, prebuilt connectors, or native streaming for ingestion from any data source

Falcon Next-Gen SIEM also offers key data built in, flexible collectors, and a variety of pre-built connectors.

- **Native Visibility, No Configuration:** Endpoint, cloud, identity, and threat intelligence data is instantly available for analysis via the Falcon sensor and platform.
- **Lightweight, Flexible Log Collector:** Use the Falcon Log Collector (FLC) for highly scalable ingestion, or bring your own logshipper like Vector or Fluentd.
- **Centralized Fleet Management:** Streamline your log collection infrastructure with unified management. Deploy, configure, and monitor your entire fleet from a single console with real-time visibility.
- **Expanding Set of Prebuilt Connectors:** CrowdStrike's rapidly growing ecosystem supports firewalls, email security, cloud infrastructure, and more. The CrowdStrike Marketplace makes it easy to discover and deploy solutions to fit your organization's needs.
- **Generic Cloud Connectors:** Easily retrieve data in cloud storage and collect other relevant cloud security logs from AWS, Google Cloud, and Azure.

Accelerate AWS visibility with Quick Start for AWS

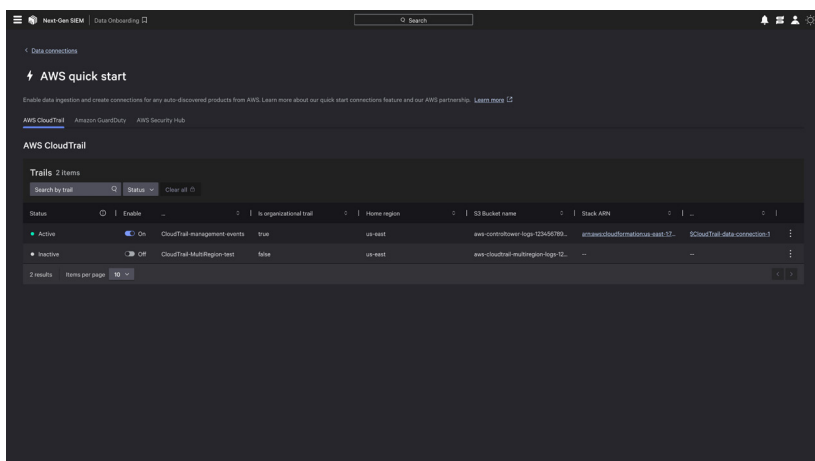


Figure 3. Automate onboarding for AWS data sources in minutes, not months.

Falcon Next-Gen SIEM Quick Start for AWS gives teams visibility from Day One by simplifying and automating data onboarding for AWS services like CloudTrail, Security Hub, and GuardDuty.

- **Set Up in One Click:** Connect key data sources, enable parsers for normalization, and deploy detection rules automatically through an intuitive onboarding wizard without requiring manual configuration or special permissions.
- **Discover Blind Spots:** Automatically surface AWS log sources not yet monitored for ingestion.
- **Gain Unified Visibility:** Instantly ingest and analyze data from AWS alongside telemetry from the Falcon platform and all of your security tools — accelerating detection, investigation, and response.

Parsers built by AI, refined by humans

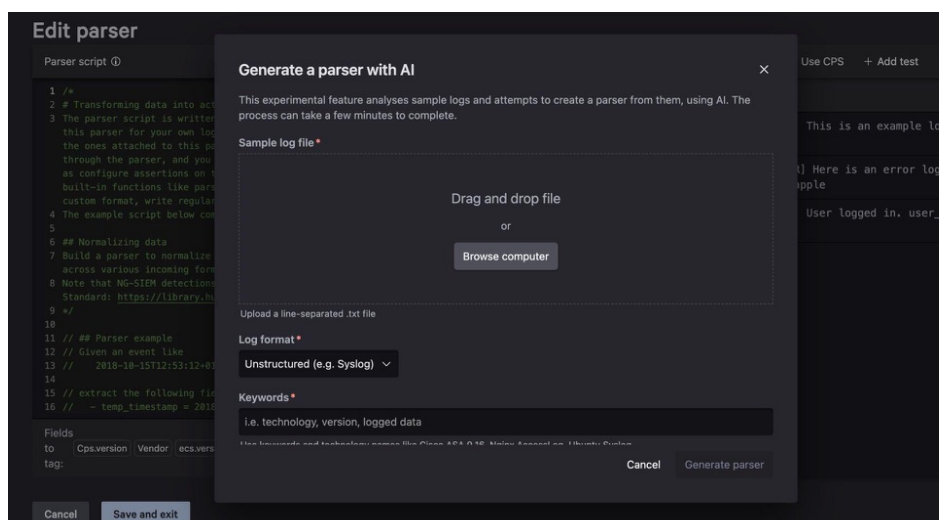


Figure 4. The AI-generated Parsing tool in Falcon Next-Gen SIEM allows teams to upload sample logs and use AI to automatically generate parsers in minutes

Getting data in is only part of the challenge — teams also need to ensure it's formatted, normalized, and actionable. AI-generated parsers in Falcon Next-Gen SIEM radically simplify parser creation and reduce cycles spent on manually reviewing documentation and parser validation. Centralized lifecycle management with automated versioning, change tracking, and configurable auto-update policies ensures consistency across all instances.

- **AI-Generated in Minutes:** Upload sample logs and leverage large language models to automatically generate, classify, and normalize the parser — no manual mapping required.
- **Built to CrowdStrike Parsing Standards (CPS):** Output is CPS-compliant, validated, and tested to ensure parser integrity across log types.
- **Customizable and Scalable:** Easily fine-tune or clone existing parsers to adapt to new sources or as log formats change.

Unified control with the Data Connections dashboard

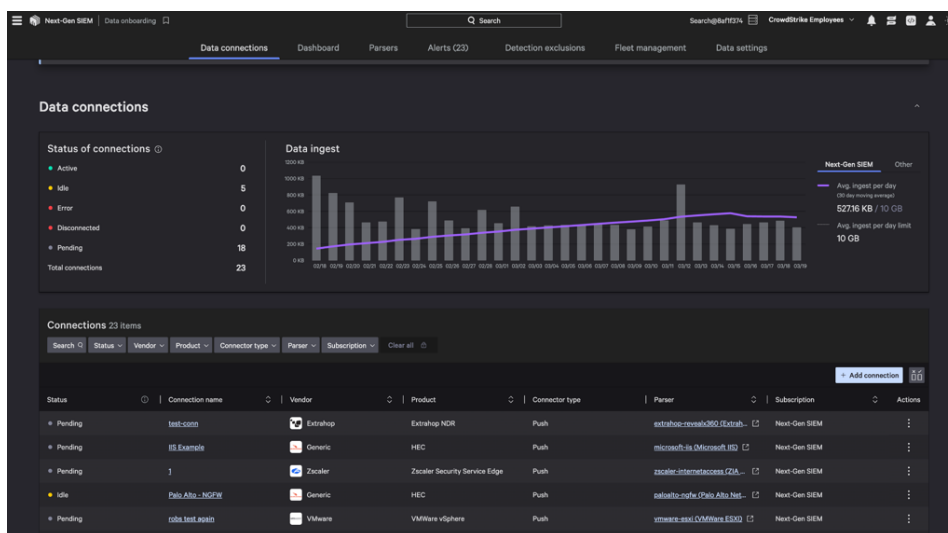


Figure 5. The Data Connections interface lets analysts monitor and manage connectors in real time

Once data starts flowing, SOC teams need confidence that it's working as expected. The **Data Connections** interface offers real-time control and visibility in one place.

- **Unified Management:** Discover, configure, and monitor data connectors and associated parsers from a single UI.
- **Real-Time Monitoring:** Instantly detect pipeline issues like broken connectors or parsers, and view associated parsers or custom mappings. Easily see ingestion patterns and volume over time.
- **Precise Troubleshooting:** Seamlessly pivot to query event history or error analysis for a specific connector or parser, enabling immediate action.

Seamless discovery of more content

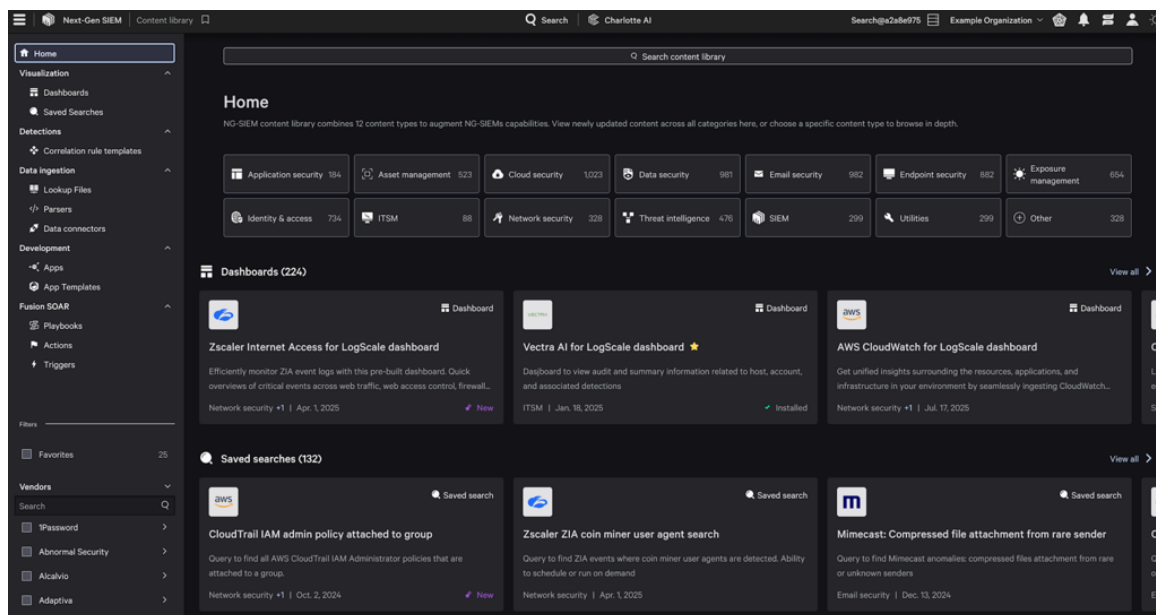


Figure 6. Discover and deploy out-of-the-box content from the unified content library.

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

- **Streamlined Onboarding Experience:** New content includes parsers, dashboards, and queries, complementing existing CrowdStrike Falcon® Fusion SOAR integrations, playbooks, and CrowdStrike Falcon® Foundry apps.

[Watch a Demo](#) →

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/>

