

Falcon Onum

Supercharge your agentic SOC transformation with clean, high-quality, real-time data

Modern SOC's can't afford telemetry chaos

Today's security environments are overwhelmed with data. As adversaries move faster and telemetry volumes grow, security teams must handle massive amounts of raw, redundant, and unstructured data, often routed through slow pipelines and expensive tools.

Traditional pipelines and manual enrichment can delay insights, reduce detection quality, and increase noise and costs. With SIEM and AI-driven security dependent on clean, high-quality telemetry, SOC's need full control of their data while it is in motion, not after it lands.

From raw logs to ready intelligence in milliseconds

CrowdStrike Falcon® Onum is a high-performance data pipeline that gives security and platform teams precise control over how telemetry is collected, filtered, enriched, and routed before it reaches storage or CrowdStrike Falcon® Next-Gen SIEM.

By simplifying complex pipelines and shaping telemetry at the source, Falcon Onum cuts ingestion volume, sharpens signal clarity, and strengthens detection outcomes.

With clean, structured, and context-rich data flowing into the CrowdStrike Falcon® platform, security teams can reduce cost, improve operational efficiency, and respond to threats faster — all without adding friction or overhead.

Falcon Onum is more than a pipeline — it's the real-time control layer for the agentic SOC. By shaping telemetry at the source, it empowers security and platform teams to move faster, spend smarter, and act in milliseconds, not minutes. With Falcon Onum, security and platform teams stop wrestling with data and can focus on stopping breaches.

Key benefits

- **Faster time to Falcon:** Experience accelerated onboarding into Falcon Next-Gen SIEM, with clean, structured data delivered quickly
- **ROI improvement:** Reduce overhead with smart filtering — cut telemetry ingest and storage costs by up to 50%¹
- **Real-time performance:** Process and route high-volume telemetry with millisecond latency
- **Boosted detection quality:** Apply threat intel, context, and policy at ingest — not post-index
- **Drag-and-drop simplicity:** No regex, no brittle scripts — just powerful, visual pipeline control
- **Built for flexibility:** Route to Falcon, S3, SOAR, or any destination, with no vendor lock-in
- **Scale with confidence:** Process 5x more events per second than the nearest competitor¹

¹Numbers are projected estimates of average benefit based on 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 the customer's module deployment and environment.

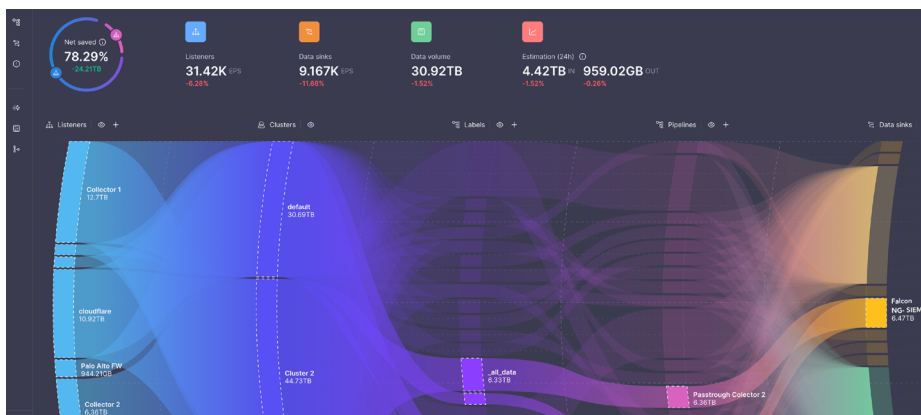


Figure 1. Visualize and control telemetry flow in real time

Key capabilities

Filter Noise at the Source

- Reduce telemetry volume with suppression, redaction, and deduplication
- Allow only high-value data to reach Falcon Next-Gen SIEM and the Falcon platform

Deliver Enriched, High-Fidelity Signals

- Enrich in real time with threat intelligence, geo-IP, user, and asset context
- Improve detection speed and signal clarity without relying on post-processing

Route Intelligently and Rapidly

- Shape and deliver structure data to multiple destination
- Route based on format, policy, region, business logic, and more

Power Multiple Use Cases with a Single Pipeline

- Use one pipeline to serve SIEM, SOAR, storage, and analytics tools
- Eliminate redundant routing logic and reduce operational overhead

Watch this on-demand CrowdCast to see how Falcon Onum powers the Agentic SOC: Accelerate Your Agentic SOC with CrowdStrike Onum

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/>

