

CrowdStream

Streamline setup and accelerate time-to-value of next-gen SIEM and log management

Say goodbye to deployment headaches

Simply getting data into a traditional SIEM can feel like an uphill battle. Security teams must collect, parse and correlate log data from a myriad of sources. As data sources proliferate, teams struggle under the weight of complex, costly processes. You deserve better.

CrowdStream: Data onboarding made easy

CrowdStream makes data onboarding a breeze, letting you seamlessly collect and route data from any source into CrowdStrike Falcon® Next-Gen SIEM and CrowdStrike® Falcon LogScale™. Leveraging Cribl's powerful data pipeline technology, CrowdStream delivers a fast, cost-effective solution that speeds up adoption and time-to-value.

As a native feature of Falcon Next-Gen SIEM and Falcon LogScale, CrowdStream simplifies deployment and management, enabling you to quickly get up and running. This means you can begin threat hunting, investigating and stopping attacks, and achieving compliance faster.

CrowdStream redefines data management by simplifying collection and offering optional enrichment, normalization and filtering of data. This integrated capability gives you total control over your data — boosting security, ensuring compliance and streamlining governance so you can focus on what matters: protecting your organization.

Key benefits

Easily connect and route data from any source to the CrowdStrike Falcon® platform while minimizing the complexity and cost of connecting data sources

Enhance threat hunting with blazing-fast search and enrichment across all of your data

Unlock the potential of the AI-native SOC by seamlessly migrating from legacy logging platforms to Falcon Next-Gen SIEM

Improve security and compliance postures with features such as data masking, enrichment and selective filtering

Key capabilities

Easily Connect and Route Data from Any Source

Using CrowdStream, you can simplify deployment and dramatically accelerate the adoption of Falcon Next-Gen SIEM and Falcon LogScale. CrowdStream offers out-of-the-box integrations to collect data from a broad set of applications and devices using over three dozen data sources. You can use the CrowdStream universal receiver to ingest data from almost any data source and replay data later if needed. And by routing all of your data to the Falcon platform, you can centralize your data for blazing-fast search and real-time visibility to eliminate threats.

Supercharge Threat Hunting with Data Enrichment

Falcon Next-Gen SIEM helps you quickly hunt down targeted attacks, insider threats and evasive malware. CrowdStream takes threat hunting to the next level by providing you additional insights and intelligence. Because CrowdStream can enrich your data with third-party information such as geolocation and threat intelligence before it's collected by Falcon Next-Gen SIEM, your hunters have greater context to quickly analyze query results and expedite response.

Accelerate Investigations with GenAI and High-Speed Search

With CrowdStream, it's easier than ever to investigate incidents and pinpoint the root cause and scope of attacks. CrowdStream can normalize data into a consistent format before it's routed to the Falcon platform, making data immediately actionable. By correlating data from multiple sources, you can detect cross-domain attacks. You can dramatically speed up investigations with search performance that's up to 150x faster than legacy SIEMs and collaborate instantly to quickly take action. To speed up analysis, the Incident Workbench provides a complete picture of an attack in an elegant visual graph that correlates users, entities and threat context.

Maintain Compliance by Masking Sensitive Data

CrowdStream gives you visibility and control over your data pipeline, so you granularly control what data to route to Falcon Next-Gen SIEM or Falcon LogScale. You can granularly mask or truncate personally identifiable information (PII) and other sensitive data. You can also optionally remove extraneous fields, null values and duplicate events. CrowdStream lets you aggregate logs into metrics for reduction at scale or replay data at any time for analysis.

Seamlessly Migrate to CrowdStrike

Because CrowdStream is a vendor-agnostic universal receiver and router, Falcon customers can smoothly and securely migrate from legacy SIEM platforms without worrying about dropping or losing data. Whether you are migrating from a self-hosted SIEM deployment or a cloud data lake, CrowdStream's ability to ingest data from your existing agents and infrastructure, then route that data to the Falcon platform or AWS S3 object storage in full fidelity, can make SIEM migrations easy.

Modernize Your SOC in a Fraction of the Time

Falcon Next-Gen SIEM stops breaches by unifying data, threat intelligence and workflow automation on one complete AI-native SOC platform. Built from the ground up around a modern security analyst experience, it amplifies the speed and efficiency of incident response. Your team can search up to 150x faster¹ and scale to 1PB/day of data ingestion while achieving up to 80% cost savings compared to legacy SIEMs.² By making the data onboarding process easier, CrowdStream lets you unlock the value of Falcon Next-Gen SIEM faster, so you can hunt down and eliminate advanced threats and achieve compliance.

Test-drive Falcon
Next-Gen SIEM



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/>

Follow us: [Blog](#) | [X](#) | [LinkedIn](#) | [Facebook](#) | [Instagram](#)

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

¹ Results are from a customer. Individual results may vary.

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 the individual customer's module deployment and environment.