CrowdStrike Solutions

CROWDSTRIKE

Falcon LogScale Solution Brief:

CrowdStream

Accelerate the adoption and time-to-value of CrowdStrike Falcon® LogScale

Collecting and Processing All Your Logs Can Be a Nightmare

To stay ahead of cybersecurity threats, you need real-time visibility and comprehensive data at your fingertips. However, you may be struggling to efficiently collect, normalize, and correlate data from all of your log sources. Onboarding log data often burdens security, IT and DevOps teams with complex and costly processes, especially as data volumes and sources grow.

CrowdStream Makes Data Onboarding a Dream

CrowdStream is a native capability of CrowdStrike Falcon® LogScale that lets you easily collect and route data from any source using Cribl's observability pipeline technology. CrowdStream provides an elegant, fast and cost-effective way to get data into Falcon LogScale to greatly accelerate the adoption of log management.

CrowdStream is included with Falcon LogScale, a modern log management platform that provides blazing-fast search, real-time alerting and customizable dashboards for compliance, threat hunting and historical investigations. By making data onboarding easier, CrowdStream revolutionizes the way you onboard and manage log data by simplifying data collection and optionally enriching, normalizing and filtering data.

With the addition of CrowdStream, Falcon LogScale provides end-to-end log management and observability — from data collection to analysis and visualization — for a broad array of security, IT and compliance use cases.

CrowdStream is available at no additional cost for up to 10 GB of daily streaming data to CrowdStrike Falcon® platform customers.

Key Benefits

Easily connect and route data from any source into CrowdStrike Falcon LogScale while minimizing the complexity and cost of connecting data sources.

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

Take advantage of log management at petabyte scale by seamlessly migrating from legacy logging platforms to Falcon LogScale.

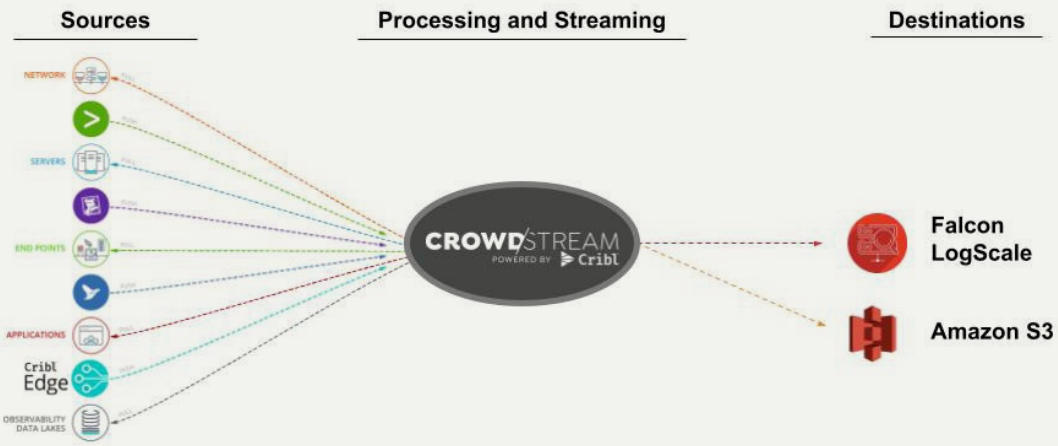
Improve security and compliance postures with features such as data masking, enrichment and selective filtering.

Key Capabilities

Easily Connect and Route Data from Any Source to Falcon LogScale

Using CrowdStream, your security, IT and DevOps teams can dramatically accelerate the adoption of 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 Falcon LogScale, you can centralize your data for blazing-fast search and real-time visibility to eliminate threats.

An advanced observability pipeline for Falcon LogScale powered by Cribl technology



Enhance Threat Hunting and Gain Investigative Context with Data Enrichment

Falcon LogScale 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 LogScale, your hunters have greater context to quickly analyze query results and expedite response.

Accelerate Investigations with 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 Falcon LogScale, making data immediately actionable. By correlating Falcon platform data including endpoint, cloud and identity events with third-party data, Falcon LogScale provides a complete picture of an attack and lets you drill down into individual events for rich investigative details.

Maintain Compliance and Improve Data Governance by Masking Sensitive Data

CrowdStream gives you visibility and control over your observability pipeline, so you granularly control what data to route to Falcon LogScale or object storage. You can granularly mask or truncate personally identifiable information (PII) and other sensitive data before it is sent to Falcon LogScale. 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 Logging to Falcon LogScale Cloud

Because CrowdStream is a vendor-agnostic universal receiver and router, Falcon LogScale customers can smoothly and securely migrate from legacy logging platforms without worrying about dropping or losing data. The same approach works for Falcon LogScale users looking to migrate from a self-hosted Falcon LogScale deployment or move to Falcon LogScale from an alternative log management solution.

Deploy Petabyte-Scale Log Management in a Fraction of the Time

Falcon LogScale empowers you to log everything to answer anything in real time. Through a modern architecture and advanced compression technology, Falcon LogScale minimizes computing and storage resources, offering **up to 80% savings** compared to alternative solutions, while delivering high-speed search and unparalleled performance. By making the data onboarding process easier, CrowdStream lets you unlock the value of Falcon LogScale faster and do more with log management than ever before.

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.**

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Try Falcon LogScale free for 30 days

Learn more at **www.crowdstrike.com**