SOLUTION BRIEF

Cribl and CrowdStrike Falcon® LogScale

Together, Cribl and CrowdStrike give you a clean, efficient way to get data into the CrowdStrike Falcon® platform, speed up XDR adoption, and use Falcon LogScale to lower the cost of traditional observability and log management.

The challenge

Data volumes are growing in every industry. You keep adding new data sources to get better answers, but that creates new problems.

This data is essential for SecOps, ITOps, and DevOps teams to improve performance, support the business, and protect the environment. Yet when you try to capture and analyze massive amounts of data, you quickly run into issues with scale, complexity, and cost.

The solution

Enterprises that need to ingest and interpret data from many sources are turning to Falcon LogScale for centralized, cost-effective log management and observability.

Falcon LogScale delivers fast, scalable access to all log and event data so you can:

- Explore critical log information quickly
- Eliminate blind spots
- Find the root cause of incidents faster

The Cribl suite of products gives IT and security teams powerful data collection, routing, and processing capabilities. You can send data to multiple destinations without adding new infrastructure or agents.

You can deploy Cribl on-prem or in the cloud. Either way, you get a proven solution that lets you:

- Make data-driven decisions at scale
- Test new use cases across huge data volumes
- Keep control over where your data goes and how it's used

Cribl and CrowdStrike Falcon LogScale: better together

Together, Cribl and Falcon LogScale give organizations of any size world-class data ingestion and analytics while optimizing for cost and scale.

With the Cribl integration for Falcon LogScale, you can:

- Optimize data and store it in one place
- Improve visibility and control over your environment
- Reduce complexity and context switching for your teams

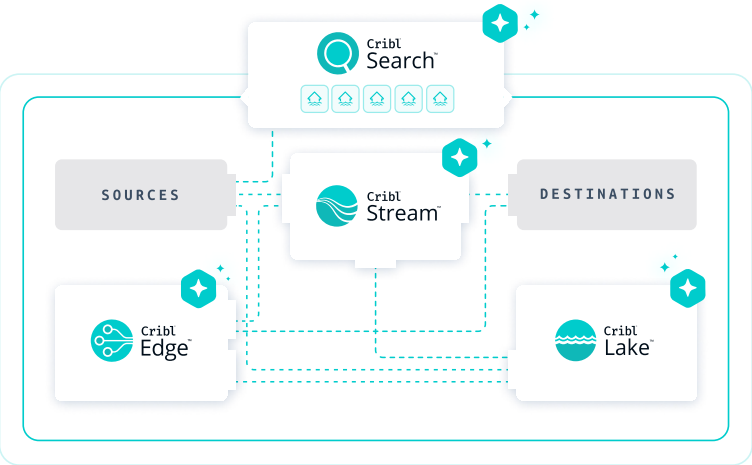
The joint solution

- You're dealing with exploding data volumes and constant pressure to get answers fast.
- Cribl and CrowdStrike Falcon® LogScale help SecOps, ITOps, and DevOps teams improve performance, boost productivity, and strengthen security... without blowing up costs.

Use Cribl Stream to get multiple data sources into Falcon LogScale, so your teams can focus on critical data and high-value work instead of wrestling with tools.

Cribl and Falcon LogScale unify your data sources and give you the flexibility and scale you need from your security and observability tools.

With the Cribl suite of products, you can also free up valuable analytic capacity in Falcon LogScale by offloading data to the most cost-effective destinations, like object storage, for long-term retention.



Cribl and CrowdStrike Falcon LogScale **unify** your data sources, ensuring **flexibility** and **scale** in your observability tools

With Cribl suite of products, organizations can free up **valuable** analytic capacity in Falcon LogScale by sending data to the most **cost-effective** destinations, like object storage, for long-term retention.

Use Cases and Benefits for Cribl and Falcon LogScale

EASILY CONNECT AND ROUTE DATA FROM ANY SOURCE TO THE CROWDSTRIKE FALCON PLATFORM

With Cribl, your security and IT teams can move much faster on holistic XDR and log management. The joint solution cuts down point products by centralizing and normalizing all data inside the CrowdStrike Falcon platform. When you unify data in the Falcon platform, you unlock AI-powered insights and near-instant search at petabyte scale, giving you the real-time visibility you need to eliminate threats, run deep analytics, and hunt adversaries with confidence.

BOOST THREAT HUNTING WITH BLAZING-FAST SEARCH AND ENRICHMENT

CrowdStrike Falcon LogScale helps your team quickly hunt targeted attacks, insider threats, and evasive malware. Your threat hunters can build advanced queries, search for indicators of compromise, and scan petabytes of data at speed to uncover threats. Because Cribl Stream enriches your data with third-party context such as geolocation and threat intelligence before Falcon LogScale collects it, your hunters get richer detail in every result and can move faster from detection to response.

UNLOCK MORE ANALYTIC CAPACITY IN FALCON LOGSCALE

With Cribl Stream or Edge, you can free valuable analytic capacity in Falcon LogScale by sending data to more cost-effective destinations, like object storage, for long-term retention. This approach separates your Falcon LogScale instance (your system of analysis) from your system of record, so you can route data to the best tool for the job, or all the tools for the job, by

translating and formatting it into any schema you need. You also boost system performance by trimming extraneous fields, null values, and duplicate events, aggregating logs into metrics to shrink volume at scale, and replaying data to Falcon LogScale at any time for deeper analysis.

ACCELERATE INVESTIGATIONS BY SEARCHING ACROSS ALL OF YOUR DATA QUICKLY

With Falcon LogScale and Cribl Stream, you can investigate incidents faster and pinpoint both the root cause and the blast radius. Cribl Stream normalizes data into a consistent format before it routes that data to Falcon LogScale. By connecting Falcon platform data with third-party data, Falcon LogScale gives you a complete picture of an attack and lets you drill into individual events for rich investigative detail.

SEAMLESSLY MIGRATE WORKLOADS TO FALCON LOGSCALE CLOUD

Because Cribl Stream is a vendor-agnostic, universal receiver and router, new Falcon LogScale Cloud customers can move on-premises workloads to the cloud smoothly and securely, without worrying about dropped or lost data. The same pattern works for Falcon LogScale users who want to upgrade existing Falcon LogScale Cloud infrastructure or switch from another log management or legacy solution to Falcon LogScale Cloud.

Summary

On a quest to ingest and interpret their data, many companies have turned to Falcon LogScale for centralized log management with real-time insights at scale. To unify your data sources and ensure flexibility and scale in your observability tools in a cost-effective way, the Cribl and Falcon LogScale integration is built to optimize your data and simplify management. Cribl Stream works with any tooling, keeps costs down, and performs well with even the largest amounts of data — making it the perfect complement to Falcon LogScale.

With Cribl Stream and CrowdStrike Falcon® LogScale, customers can:

- Enhance threat hunting with blazing-fast search and enrichment
- Accelerate investigations by searching across all of your data quickly
- Unlock more analytic capacity in Falcon LogScale
- Seamlessly migrate workloads to Falcon LogScale Cloud

Together, Stream and LogScale give businesses of all sizes access to world-class data ingestion and analytics while optimizing for cost and scale, ensuring long-term success.

Click **here** to get started with LogScale and Cribl today.

ABOUT CRIBL

Cribl, the AI Platform for Telemetry, empowers enterprises to manage and analyze telemetry for both humans and agents. Trusted by organizations worldwide, including half of the Fortune 100, Cribl bridges the gap between AI ambition and infrastructure reality. No lock-in. No data loss. No compromises. Cribl's vendor-agnostic platform ensures data remains portable and interoperable. By cost-effectively handling increasing data volume and variety without delay, Cribl gives enterprises the choice, control, and flexibility to build what's next. Founded in 2018, Cribl is a remote-first workforce with an office in San Francisco, CA.

Learn more at cribl.io | **Join our** Slack community
Try Cribl Sandboxes | **Follow us on** LinkedIn **and** X

SB-0072-EN1-0526

Cribl