>SOLUTION BRIEF_

Cribl and CrowdStrike Falcon® LogScale

THE JOINT SOLUTION

- Organizations are constantly grappling with growing data volumes as they work to get the answers they need from their environments.
- Cribl and CrowdStrike Falcon LogScale's joint solution enables SecOps, ITOps, and DevOps teams to improve performance, drive business productivity, and ensure effective security.

Together, Cribl and CrowdStrike provide an elegant way to get data into the CrowdStrike Falcon® platform by greatly accelerating the adoption of XDR and leveraging LogScale to reduce the cost of traditional approaches to observability and log management.

The Challenge

Data volumes are growing year over year in nearly every industry, and companies continually need to onboard and analyze new sources of data to get the answers they need out of their environments. This data is critical to SecOps, ITOps and DevOps teams as they try to improve performance, drive business productivity, and ensure effective security. But organizations inevitably run into scale and cost issues when attempting to capture what can be massive amounts of data.

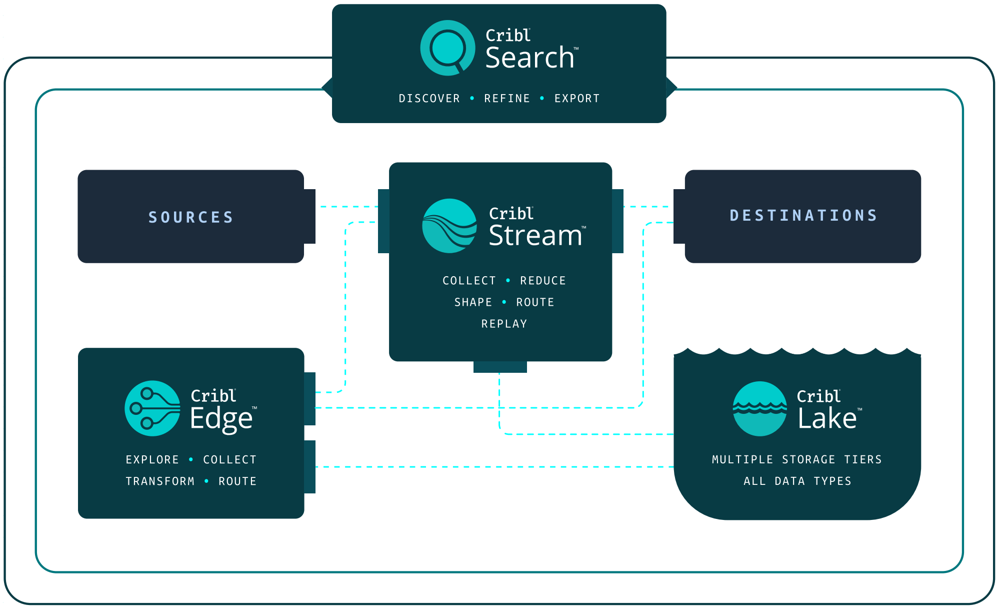
The Solution

Enterprises that want to ingest and interpret data from multiple sources are choosing CrowdStrike Falcon LogScale, because it provides a centralized log management platform with a comprehensive, cost-effective observability experience. Falcon LogScale enhances observability at scale for all log and event data by making it fast and easy to explore critical log information, eliminate blind spots and find the root cause of any incident. The Cribl suite of products empower IT and security teams with top-tier collection, routing, and processing capabilities, enabling them to get data to multiple destinations without adding new infrastructure and agents. Deployable on-premises or in the cloud, Cribl gives IT and security teams an observability solution that unlocks the ability to make data-driven business decisions while testing out new use cases at scale, regardless of their volume of data.

Cribl and CrowdStrike Falcon LogScale: Better Together

Together, Cribl and Falcon LogScale give businesses of all sizes access to world-class data ingestion and analytics while optimizing for cost and scale, ensuring long-term success. The Cribl integration with Falcon LogScale allows you to optimize your data and store it in one place, providing your team with improved visibility and control over your environment at a minimized cost. Stream multiple data sources using Cribl into Falcon LogScale with ease to cut out complexity and minimize context switching, so your team can focus on critical data and tasks.

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



Introducing CROWDSTREAM POWERED BY Cribl

CrowdStream is a CrowdStrike capability that directly connects any data source to the CrowdStrike Falcon platform using Cribl's observability pipeline technology. By sitting between data sources and their destination, CrowdStream lets you easily connect, transform, and route data from any source into the CrowdStrike Falcon platform, accelerating adoption and time-to-value for log management and XDR.

Use Cases and Benefits for Cribl and CrowdStrike Falcon® LogScale

Easily connect and route data from any source to the CrowdStrike Falcon platform

Using Cribl, security and IT teams can dramatically accelerate the adoption of holistic XDR and log management. The joint solution consolidates point products by centralizing and normalizing all data within the CrowdStrike Falcon platform. Unify data within the CrowdStrike Falcon platform for AI-powered insights and near-instant search at petabyte scale to provide the real-time visibility needed to eliminate threats, run deep analytics, and hunt for adversaries.

Enhance threat hunting with blazing-fast search and enrichment

CrowdStrike Falcon LogScale lets you quickly hunt down targeted attacks, insider threats, and evasive malware. Your threat hunters can construct advanced queries, search for indicators of compromise, and swiftly scour through petabytes of data to find threats. Because Cribl Stream enriches your data with third-party information such as geolocation and threat intelligence before it is collected by Falcon LogScale, your hunters have greater context to quickly analyze query results and expedite response.

Unlock more analytic capacity in Falcon LogScale

With Cribl Stream or Edge, 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. This data optimization separates companies' Falcon LogScale instance – or system of analysis — from their system of record, enabling them to route data to the best tool for the job — or all the tools for the job — by translating and formatting data into any schema required. Improve system performance by removing extraneous fields, null values, and duplicate events. Aggregate logs into metrics for reduction at scale, or replay data at any time to LogScale for analysis.

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.

Accelerate investigations by searching across all of your data quickly

With Falcon LogScale and Cribl Stream, it's easier than ever to investigate incidents and pinpoint the root cause and scope of attacks. Cribl Stream normalizes data into a consistent format before it's routed to Falcon LogScale. By correlating Falcon platform data 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.

Seamlessly migrate workloads to Falcon LogScale Cloud

Because Cribl Stream is a vendor agnostic, universal receiver and router, new Falcon LogScale Cloud customers can smoothly and securely migrate on-premises workloads to a cloud environment — without worrying about dropping or losing data. The same approach works wonders for Falcon LogScale users looking to upgrade existing Falcon LogScale Cloud infrastructure or move over to Falcon LogScale Cloud from an alternative log management or legacy solution.

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's observability pipeline that 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 Falcon 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 Falcon LogScale and Cribl today.

ABOUT CRIBL

Cribl, the Data Engine for IT and Security, empowers organizations to transform their data strategy. Customers use Cribl's vendor-agnostic solutions to analyze, collect, process, and route all IT and security data from any source or in any destination, delivering the choice, control, and flexibility required to adapt to their ever-changing needs. Cribl's product suite, which is used by Fortune 1000 companies globally, is purpose-built for IT and Security, including Cribl Stream, the industry's leading observability pipeline, Cribl Edge, an intelligent vendor-neutral agent, Cribl Search, the industry's first search-in-place solution, and Cribl Lake, a turnkey data lake. Founded in 2018, Cribl is a remote-first workforce with an office in San Francisco, CA.

Learn more: www.cribl.io | Try now: Cribl sandboxes | Join us: Slack community | Follow us: LinkedIn and Twitter

©2024 Cribl, Inc. All Rights Reserved. 'Cribl' and the Cribl Flow Mark are trademarks of Cribl, Inc. in the United States and/or other countries.
All third-party trademarks are the property of their respective owners.

SB-0024-EN-2-0624