>SOLUTION BRIEF_

Optimize your Observability Pipeline for Cost and Scale with Cribl Stream™ + Splunk

THE CHALLENGE

Enterprises leveraging Splunk for data ingestion and analytics need an observability solution that scales well with their business requirements and provides a cost-effective way to retain data long-term.

THE SOLUTION

Cribl Stream is an essential part of observability, providing a pipeline that works with all tooling, keeps costs down, and scales with any business – making it the perfect complement to Splunk.

THE BENEFITS

- Unlock analytic capacity in Splunk by routing data to the most cost-effective destinations
- Improve system performance by removing extraneous fields, null values, and duplicate events
- Aggregate logs into metrics for reduction at scale
- Replay data at any time to Splunk for analysis
- Seamlessly migrate workloads to Splunk Cloud

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

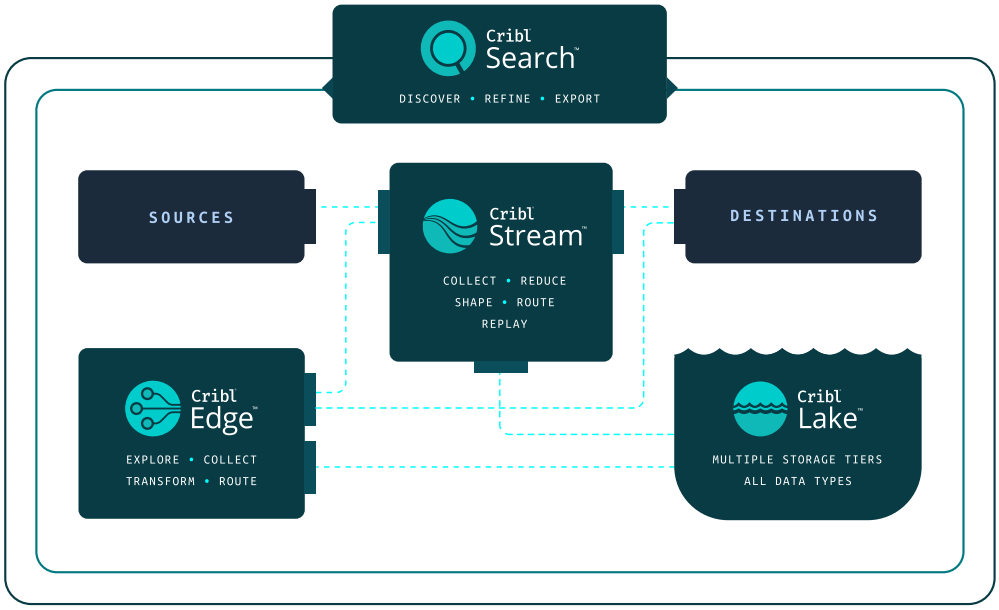
The Power of Cribl Stream and Splunk

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. Enterprises that want to ingest and interpret data from multiple sources are choosing Splunk, because it provides one of the most comprehensive observability experiences out there.

To further scale the observability foundation they have laid with Splunk, those same organizations are also turning to Cribl for similar reasons. They need an observability solution with the flexibility to get data into multiple tools from multiple sources without adding new infrastructure and agents. These companies also need a tool that can flex with them – deployable on-premises or in the cloud. At the same time, they need an observability solution that gives them the ability to make new business decisions and test out new use cases at scale, regardless of the amount of data they have. Cribl addresses these concern with a dual offering of Cribl Stream and Cribl Edge. Cribl Stream is an observability pipeline that you can seamlessly plug into the middle of an existing environment. Providing the flexibility to route, shape, restructure, and enrich data from any source to any destination, without having to add new infrastructure or agents. Cribl Edge is a next generation observability agent, allowing administrators to collect and process observability data – logs, metrics, application data, etc. – in real time, from Linux machines, apps, microservices etc., and deliver them to Cribl Stream or any supported destination. Now companies requiring an observability solution can leverage Cribl Stream or Edge, independently or in combination, to gain control over their data and simplify observability efforts.

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

Stream can help reduce as much as 50% of ingested log volume to control costs and improve system performance.



Splunk customers can easily eliminate duplicate fields, null values, and any elements that provide little analytical value.

The Benefits of Using Cribl to Optimize a Splunk Deployment

Unlock more analytic capacity in Splunk.

With Cribl Stream or Edge, organizations can free up valuable analytic capacity in Splunk by sending data to the most cost-effective destinations, like object storage, for long-term retention. This separates companies' Splunk 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 tooling schema they require.

Improve system performance by removing extraneous fields, null values, and duplicate events.

Using Cribl Stream or Edge can typically reduce 30% or more of ingested log volume to control costs and improve system performance. Splunkt customers can easily eliminate duplicate fields, null values, and any elements that provide little analytical value using dynamic sampling. From the same interface, they can filter and screen events or aggregate log data into metrics for volume reduction at scale – all while keeping a full-fidelity copy in low-cost storage to replay if needed.

Aggregate logs into metrics for reduction at scale.

In the same interface, a Cribl's observability solution gives Splunk customers the power to filter and screen events for dynamic sampling, or aggregate log data into metrics for volume reduction at scale. Once aggregated, administrators will see a major reduction in event counts and data volume, and then can choose whether to send those metrics to Splunk for further analysis, or a dedicated time series database for efficient storage and retrieval.

Replay data at any time to Splunk for analysis.

Cribl's Stream or Edge are the best way to replay multiple data formats to Splunk for analytics. Not only can administrators use Stream as a universal receiver to collect from any machine data source and schedule batch collection from multiple APIs, but they can also recall data from low-cost object storage and send those logs to Splunk for later investigations with ad hoc data collection.

Cribl Stream is an 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 splunk.

Seamlessly migrate workloads to Splunk Cloud.

Because Cribl Stream is a vendor agnostic, universal receiver and router, new Splunk 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 Splunk users looking to upgrade existing Splunk Cloud infrastructure or move over to Splunk Cloud from a competitor solution.

Summary

On a quest to ingest and interpret their data, many companies have turned to Splunk. These same enterprises also need an observability tool that scales well with their business requirements and provides a cost-effective way to retain data long-term. Cribl provides an 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 Splunk.

With Cribl Stream, Splunk customers can:

- Unlock analytic capacity in Splunk by routing data to the most cost-effective destinations
- Improve system performance by removing extraneous fields, null values, and duplicate events
- Aggregate logs into metrics for reduction at scale
- Replay data at any time to Splunk for analysis
- Seamlessly migrate workloads to Splunk Cloud

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

To get started with Splunk and Cribl today, download Cribl Stream to process up to 1 TB/day of Splunk data for free. The Cribl Slack Community is also a great place to connect with leaders from other teams leveraging both Splunk and Stream.

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

SB-0005-EN-2-0624