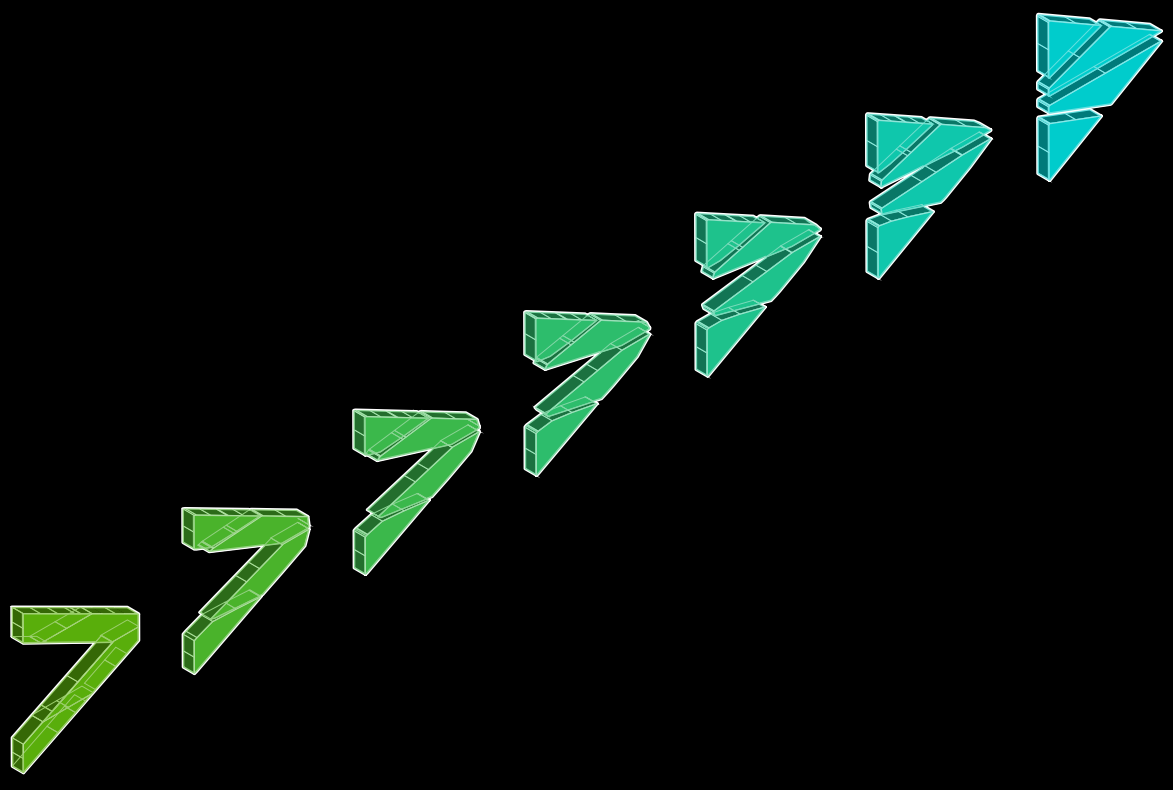
splunk> | Cribl

SOLUTION BRIEF

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



SOLUTION BRIEF

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

Together, Cribl LogStream 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 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 LogStream 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

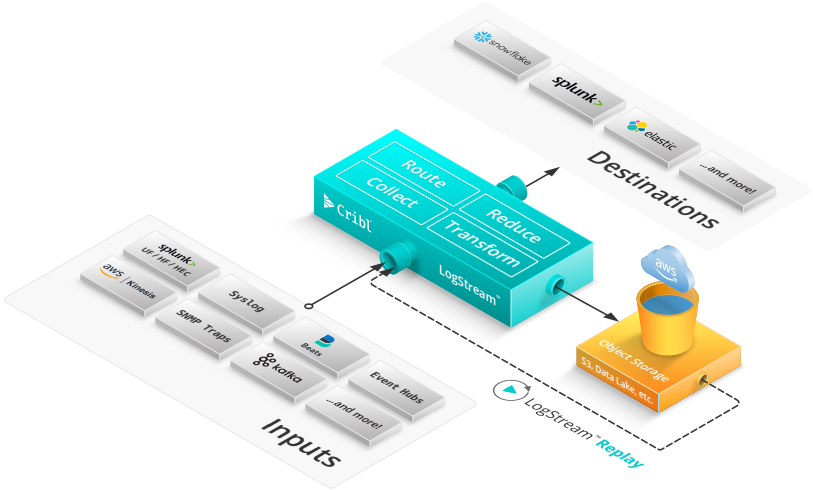
- Unlock analytic capacity in Splunk by routing data to the most cost-effective destinations
- Improve system performance by removing extraneous fields, null values, and duplicate events
- Aggregate logs into metrics for reduction at scale
- Replay data at any time to Splunk for analysis
- Seamlessly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

The Power of Cribl LogStream 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 enterprises are turning to Cribl LogStream. They need an observability pipeline with the flexibility to get data into tools like Splunk from multiple sources without adding new infrastructure and agents. These companies also need a cost-effective strategy for retaining data long-term. At the same time, they need an observability solution that can grow with their business requirements, regardless of the amount of data they have, the products they use today, or the tools they may turn to in the future.

Together, Cribl LogStream 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.



LOGSTREAM 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 Splunk with LogStream

UNLOCK MORE ANALYTIC CAPACITY IN SPLUNK

With Cribl LogStream, 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

LogStream 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 of machine or security that provide little analytical value – all while keeping a full-fidelity copy in low-cost storage.

AGGREGATE LOGS INTO METRICS FOR REDUCTION AT SCALE

In the same interface, LogStream 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 LogStream is the best way to replay multiple data formats to Splunk for analytics. Not only can administrators use LogStream 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.

SEAMLESSLY MIGRATE WORKLOADS TO SPLUNK CLOUD

Because Cribl LogStream is a 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.

CRIBL LOGSTREAM 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.

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 LogStream 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.

With Cribl LogStream, 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 LogStream 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 LogStream today, **download Cribl LogStream** to process up to 5 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 LogStream.

ABOUT SPLUNK

Splunk is the world's first Data-to-Everything Platform designed to remove the barriers between data and action, so that everyone thrives in the Data Age. They're empowering IT, DevOps and security teams to transform their organizations with data from any source and on any timescale. With more than 6,000 employees in 27 offices worldwide, they're building a future where data provides clarity, elevates discussion and accelerates progress for innovators in IT, security, DevOps and more. Find out more at **splunk.com**.

ABOUT CRIBL

Cribl is a company built to solve customer data challenges and enable customer choice. Our solutions deliver innovative and customizable controls to route security and machine data where it has the most value. We call this an observability pipeline, and it helps slash costs, improve performance, and get the right data, to the right destinations, in the right formats, at the right time. Join the dozens of early adopters, including market leaders such as TransUnion and Autodesk, to take control and shape your data. Founded in 2017, Cribl is headquartered in San Francisco, CA. For more information, visit **www.cribl.io** or our **LinkedIn**, **Twitter**, or **Slack** community.