

>SOLUTION BRIEF\_

# Cribl Stream

## THE CHALLENGE

Data volumes are growing, and organizations are being asked to analyze new types of data without blowing up their budgets or adding new infrastructure and agents.

## THE SOLUTION

Cribl Stream is a vendor-agnostic data collection, reduction, enrichment, and routing system for IT and security data that allows you to instrument everywhere, gain more insights from analytics tools, and retain more data for longer periods of time, all while paying a lot less.

## THE BENEFITS

- **Control Your Data** – Enforce data policies, standards, and formats across toolsets.
- **Choice and Flexibility** – Add any analytics tool without adding new agents.
- **Observe More** – Streamline data onboarding and collection to expose data you didn't even know existed.
- **Cost-Effective** – Optimize infrastructure, data ingestion, tool performance, and people hours.

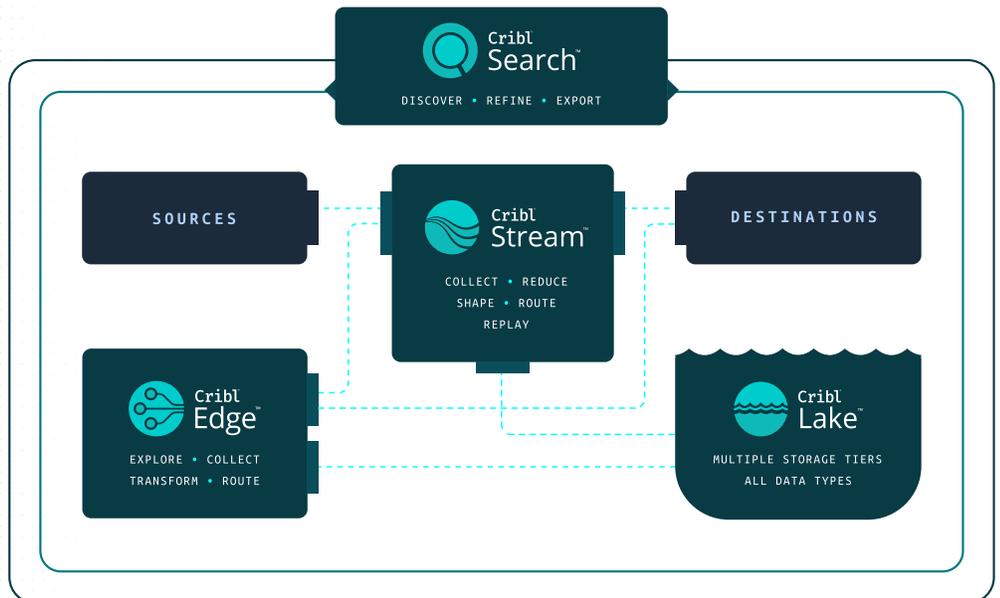
Optimize your IT, security, observability, and telemetry data without the tradeoffs of budget, flexibility, and visibility. Cribl Stream helps you gain the choice and control of getting the data you need, in the formats you want, and sent off to the destinations required.

### The challenge.

IT and Security teams are facing more challenges than ever with dramatically increasing volumes of machine-generated data already growing at 28% CAGR, and the incredible number of shapes and forms that data often takes. Tool complexity and vendor lock-in make sending data to third-party analytics platforms difficult to detect and respond to issues. That's all before adhering to privacy and regulatory standards which can cause significant financial implications.

### The Stream solution.

Cribl Stream is a robust, vendor-agnostic streams processing engine focused on centralized parsing and processing of data. Take any source and use Stream to route, reduce, reformat, enrich, or otherwise structure data in flight then send it to any destination. Delegate access to the appropriate teams with role-based access controls. Cribl enables customers to route a full-fidelity copy of raw data to low-cost storage for long-term retention for compliance / audit purposes and "replay" it to analytics tools to answer questions you didn't predict ahead of time.



## Facets of Cribl's IT and Security solution.

### Data collection and replay.

Cribl Stream is the best way to get multiple data formats into your analytics tools. Use the Stream universal receiver to collect from any data source — or schedule batch collection from multiple APIs. Use ad-hoc data collection to recall data from Cribl Lake (or any other lake solution) when you need to replay logs to analytics tools for later investigations. Not sure if you really need every event to be indexed and available all the time? Send data to low-cost storage and bring it back as needed.

### Data shaping.

Shape all the data you need to drive decisions about your environment. Translate and transform data from all your sources into the tools you choose. Obtain a more complete picture of your data by enriching logs with third-party data. Stream collects data from all your sources and shapes it into actionable logs and metrics for analysis.

### Data reduction.

Reduce as much as 50% of ingested log volume to control costs and improve system performance. Eliminate duplicate fields, null values, and any elements that provide little analytical value. Filter and screen events for dynamic sampling, or aggregate log data into metrics for massive volume reduction. Do all of that without worry: You can keep a full-fidelity copy in low-cost storage or your favorite data lake, and replay it later, if needed.

### Data routing.

Direct your data where it thrives best, including low-cost storage locations, like Cribl Lake or other destinations for long-term retention you can actually afford. Route data to the best tool for the job by translating and formatting data into any tooling schema required. Let different departments choose different analytics environments without having to deploy new agents or forwarders.

### Stream Packs.

Packs are predefined sets of routes and pipelines, data samples, lookups, and other knowledge objects built around common use cases. Packs can be downloaded from our repository and implemented within your Stream instances. Users can also create new Packs to easily share functionality between Leader nodes and Worker groups. Packs are the fastest way to maximize the value of your Stream investment.

**Cribl Stream helps you get the data you want, in the formats you need, to wherever you want it to go.**

## Gain more control, choice, and scalability of your data.

Reduce management overhead, with easy-to-use GUI-based configuration and testing. Capture live data and monitor your data processing engine in real time. Gain further insights with graphical data flow mapping. Take advantage of automated upgrades to easily and efficiently keep a whole fleet of Workers up to date without tedious CLI-based management. Use role-based activity control to ensure that only the right teams are seeing what they need to do their jobs. Manage Stream on-premises, as a hybrid deployment, or use our cloud implementation.

### Summary.

Stream enables observability by giving you the power to make choices that best serve your business, without the negative tradeoffs. As your goals evolve, you have the flexibility to make new choices including new tools and destinations. Cribl simplifies observability by putting the data you want, in the formats you need, wherever you want it to go.

#### 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](http://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-0017-EN-2-0424