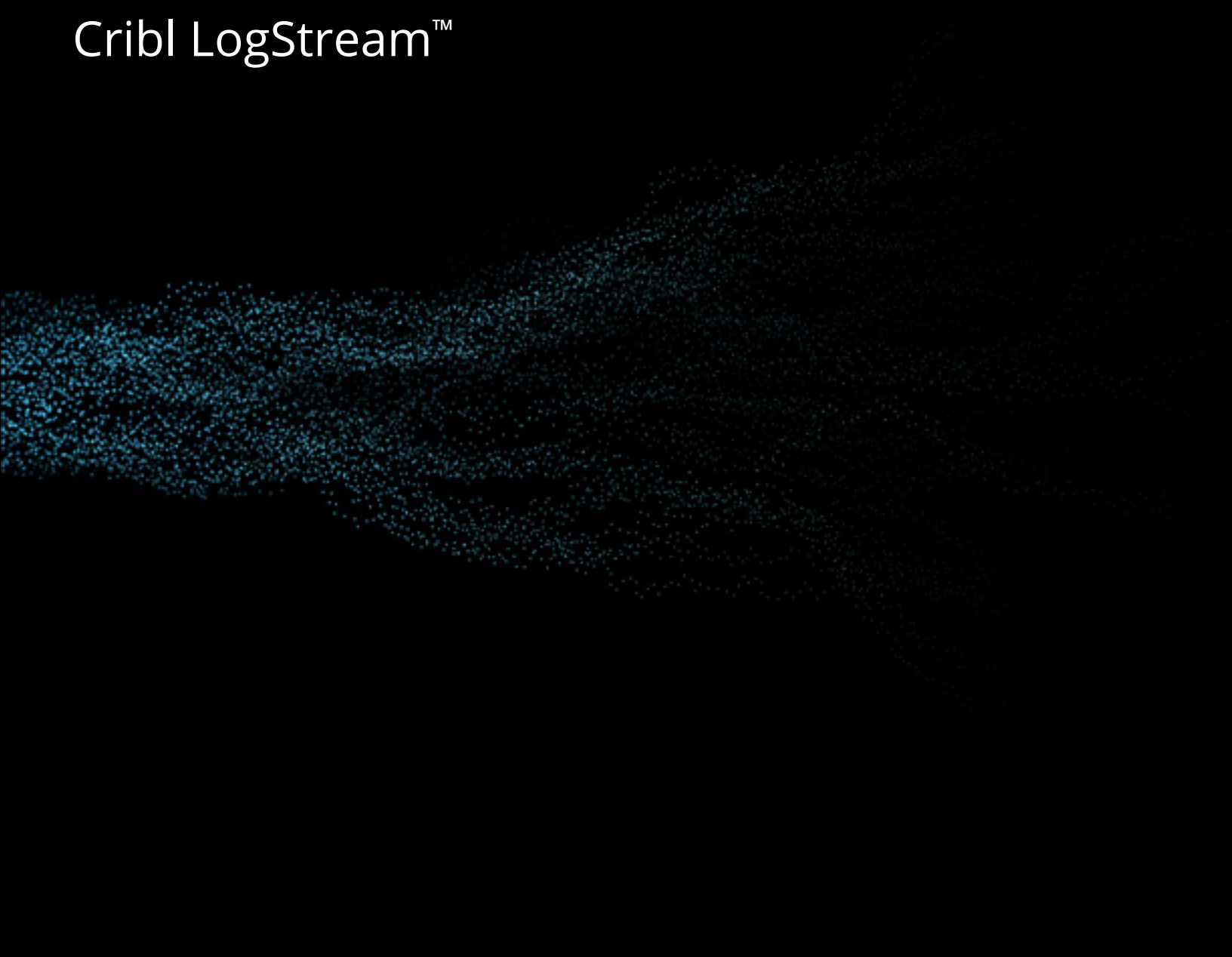# Cribl LogStream™

Cribl LogStream™

Making choices to optimize observability usually involves tradeoffs among budget, flexibility, and visibility. LogStream helps you make the best choices without those tradeoffs.

The Challenge

Data is growing year over year, and at the same time, companies are trying to analyze new sources of data to get a complete picture of their IT and Security environments. They need flexibility to get data into multiple tools, from multiple sources, but don't want to add a lot of new infrastructure and agents. These companies need a better strategy for retaining data long-term that is also cost-effective.

The Cribl Solution

LogStream is a log router that gives you the flexibility to route, shape, restructure, and enrich data from any source to any destination without adding new agents. Gain control over your data and simplify your observability efforts. Instrument everything, analyze more data, and pay less.

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 staff and

THE SOLUTION

LogStream is a log router 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.
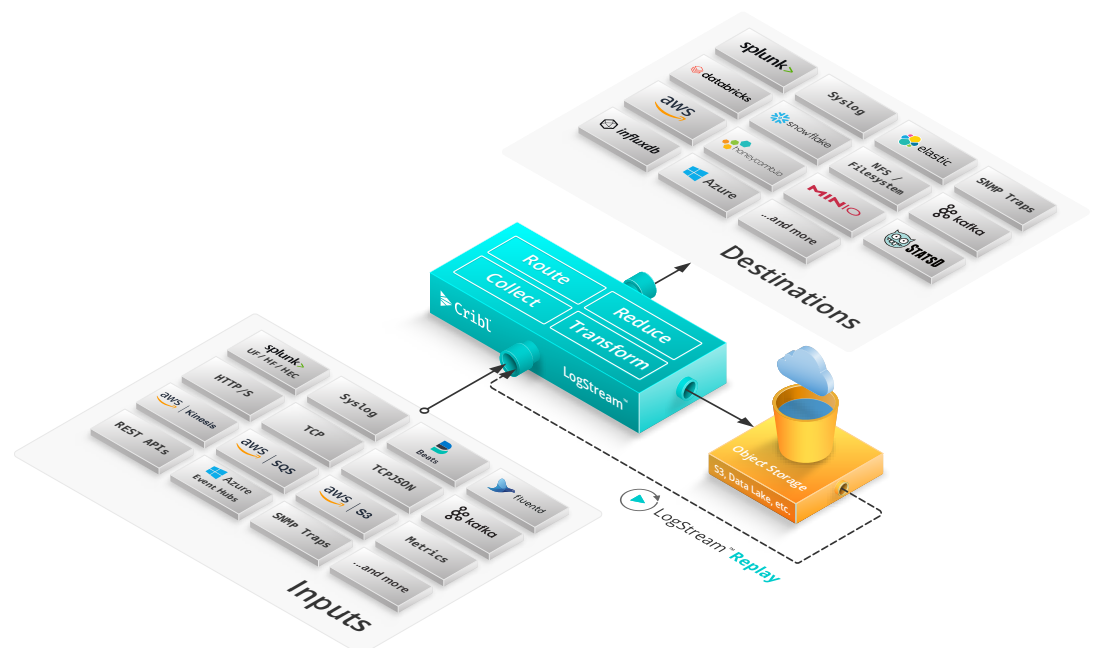
THE BENEFITS

• Control your data and send it to the right teams and the right tools

• Flexibility to add any analytics tool without adding new agents

• Simplify observability, with a universal log router for any tooling environment

• Instrument everything, analyze more, pay less

Facets of Cribl LogStream™

DATA ROUTING

Send data to the most effective destinations, including low-cost storage locations like S3 for long-term retention. 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 you require. Let different departments choose different analytics environments without having to deploy new agents or forwarders.

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 this without worry: You can keep a full-fidelity copy in a low-cost destination, and replay it later if needed.

DATA COLLECTION AND REPLAY

LogStream is the best way to get multiple data formats into your analytics tools. Use the LogStream universal receiver to collect from any observability data source – and even to schedule batch collection from multiple APIs. In addition, use ad-hoc data collection to recall data from low-cost storage, when you need to replay logs to analytics tools for later investigations.
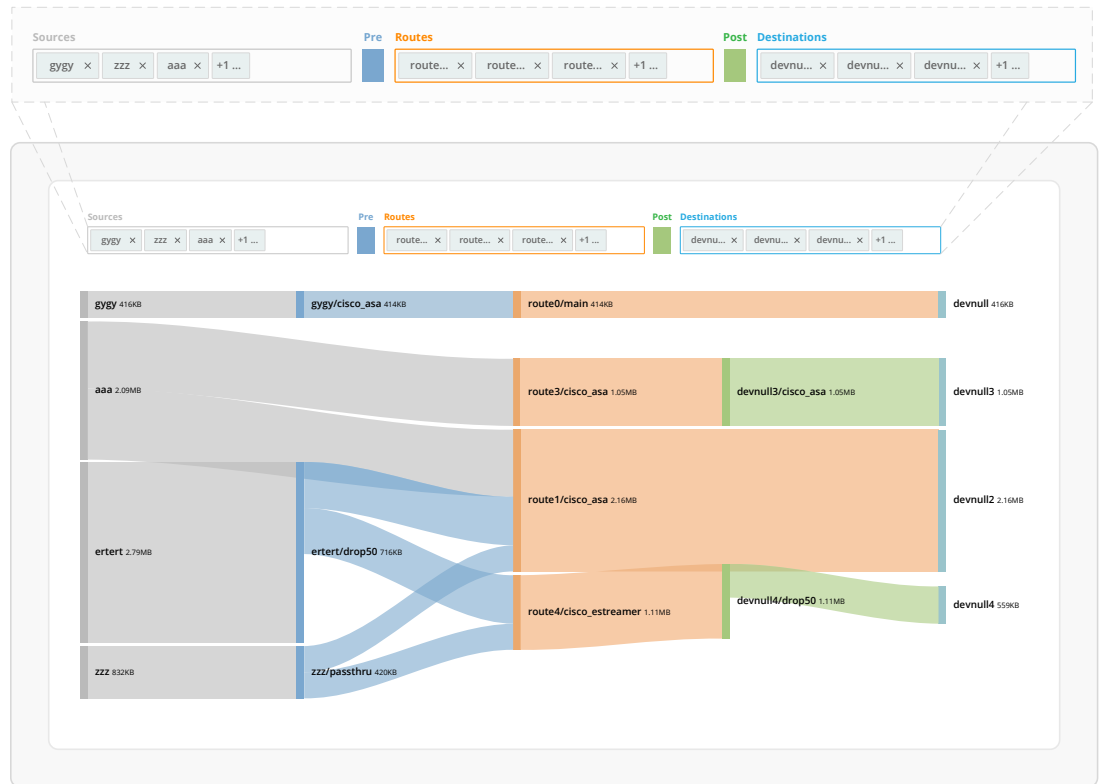
DATA SHAPING

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

LOGSTREAM 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 LogStream 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 LogStream investment.

CONTROL YOUR DATA

Reduce management overhead, with robust and easy-to-use GUI-based configuration and testing. Capture live data and monitor your observability pipeline 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 LogStream on-premises, or use our cloud implementation.

Sources
gygy × zzz × aaa × +1 …
Pre Routes
route… × route… × route… × +1 …
Post Destinations
devnu… × devnu… × devnu… × +1 …

Sources
gygy × zzz × aaa × +1 …
Pre Routes
route… × route… × route… × +1 …
Post Destinations
devnu… × devnu… × devnu… × +1 …

gygy 416KB — gygy/cisco_asa 414KB — route0/main 414KB — devnull 416KB

aaa 2.09MB — route3/cisco_asa 1.05MB — devnull3/cisco_asa 1.05MB — devnull3 1.05MB

route1/cisco_asa 2.16MB — devnull2 2.16MB

ertert 2.79MB — ertert/drop50 716KB

zzz 832KB — zzz/passthru 420KB — route4/cisco_estreamer 1.11MB — devnull4/drop50 1.11MB — devnull4 559KB

Summary

Cribl 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 to go.