>SOLUTION BRIEF_

Ensure long-term success with Cribl and Elastic.

THE CHALLENGE

Enterprises leveraging the Elastic Stack to query and correlate observability and security-relevant data need a pipelining solution that provides a cost-effective way to retain high-fidelity data long-term.

THE SOLUTION

The Cribl suite of products powers IT and Security teams in data collection, processing, and querying telemetry data to enhance insights while flexing with industry standards.

THE BENEFITS

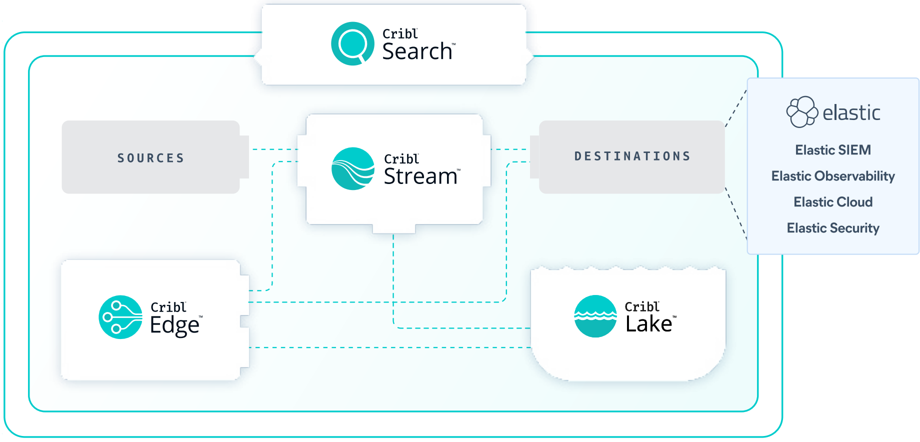
- Reuse your existing data sources and agents to route data to the Elastic Stack.
- Achieve big savings by retaining data in lower-cost object storage or a data lake.
- Make it easier to migrate your data from older versions of Elastic
- Eliminate data with little analytical value before sending to Elastic to control costs.
- Easily execute data migrations at scale from one tool to another.

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

The power of Cribl and Elastic.

The Elastic Stack is widely recognized for its robust data querying and scalability, catering to organizations that manage large datasets. To get the most out of these capabilities, many are turning to Cribl, the Data Engine for IT and Security. The Cribl suite of products streamlines data integration across various sources into multiple tools, without the burden of new infrastructure. This approach supports cost-effective data retention and provides the flexibility required to adapt to new business strategies and explore varying use cases. Together, Cribl and Elastic help organizations turn their data deluge into a strategic advantage, converging efficient management with precise compliance and actionable insights.

To continue performing searches at lightning speed with indexed logging tools like Elasticsearch, those same organizations are turning to Cribl Stream. They need pipelines with the flexibility to get data into multiple tools 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 a solution that gives them flexibility to make new business decisions and test out new use cases, regardless of the amount of data they have, the products they use today, or the tools they may turn to in the future.

Cribl and Elastic help organizations turn their data deluge into a strategic advantage, converging efficient management with precise compliance and actionable insights.

Cribl improves the management and control of enterprise logging and security pipelines, by helping Elastic customers transition from existing onboarding systems.

The benefits of using Cribl with Elastic.

Reuse your existing data sources and agents to route telemetry to the Elastic Stack.

Send data from any Elastic source to the most effective Elastic destinations, or leverage low-cost object storage 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 they require. Let different departments choose different analytics environments without having to deploy new agents or forwarders.

Make it easier to migrate your data from older versions of Elastic – or from one tool to another.

Cribl Stream is a universal receiver and router, enabling Elastic customers to smoothly and securely migrate workloads to the latest version of Elastic products — without worrying about dropping or losing data. The same approach works wonders for Elastic users looking to move over to Elastic from a competitor solution.

Eliminate data with little analytical value to control costs.

Cribl can help reduce 30% or more of ingested log volume — controlling costs and pre-conditioning data in flight to improve system performance. Elastic customers can easily eliminate duplicate fields or event streams, null values, and any elements that provide little analytical value. They can also filter and screen events for dynamic sampling, 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.

SALLY.

> "We don't want our security engineers spending hours becoming wizards in Elastic, Logstash, and syslog-ng. With Cribl, they don't have to, which frees up more time for our real jobs – security."
>
> **Sheldon Carmichael**
> Information Security Architect

Summary.

The Elastic Stack is a powerful observability and security platform. As with any platform or combination of tools, organizations must constantly evolve their data management strategy to successfully execute projects. Now, more than ever, companies need to solve new challenges without a significant increase in budget. Cribl can help enhance any investment in platforms like the Elastic Stack.

Adding Cribl Stream to the Elastic Stack gives companies the flexibility to choose the tools they need, giving more control over their data for better outcomes and lower costs. Plus, it provides a way to get any data into the formats needed for any destination. Simply put, Cribl lets enterprises observe more with the Elastic Stack, while paying a lot less and reducing the effort of their teams.

With Cribl, Elastic customers can:

- Reuse your existing data sources and agents to route data to the Elastic Stack.
- Achieve big savings by retaining data in lower-cost object storage.
- Make it easier to migrate your data from older versions of Elastic.
- Eliminate data with little analytical value to control costs.
- Easily navigate data migrations at scale from one tool to another.

Together, Cribl and Elastic give businesses of all sizes access to world-class data analytics at scale while making the most of their resources, ensuring long-term success.

To get started with Cribl and Elastic today, click here. The Cribl Slack Community is also a great place to connect with leaders from other teams leveraging both Cribl and Elastic.

ABOUT ELASTIC

Elastic is the company behind the Elastic Stack — that's Elasticsearch, Kibana, and Beats. From stock quotes to Twitter streams, Apache logs to WordPress blogs, Elastic helps people explore and analyze their data differently using the power of search. Find out more at www.elastic.co.

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-0007-EN-2-0524