Secure your SIEM migration today

Accelerate your journey to better security with Cribl's industry-first observability pipeline

OVERVIEW

When you're modernizing your SIEM and integrating new security tools, your telemetry data arrives in disparate formats. You also know that your security data must be stored, processed, and retained for compliance. How can you ensure you have a secure, efficient, and confident SIEM migration in this environment?

Data keeps growing—and it's coming in faster—but IT budgets aren't keeping up.

28%

CAGR of telemetry data creating massive implications for storage and analysis.[1]

[1] Cribl Eight Steps to SEIM migration white paper

7%

IT budget growth rate; IT budgets are vastly outpaced by data growth

Why build a modern, vendor-agnostic security data strategy?

28%

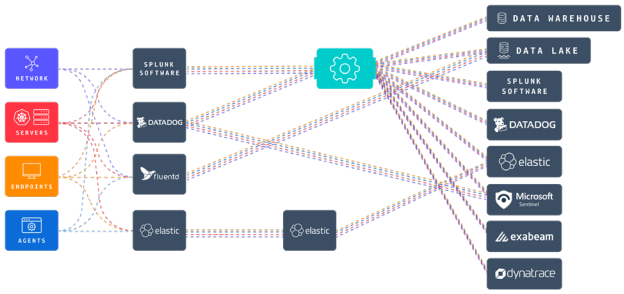
Operational burden reduction, simplifying the management of data pipelines, and minimizing infrastructure overhead.

45%

Faster speed of collecting, processing, and routing data to its final destination.

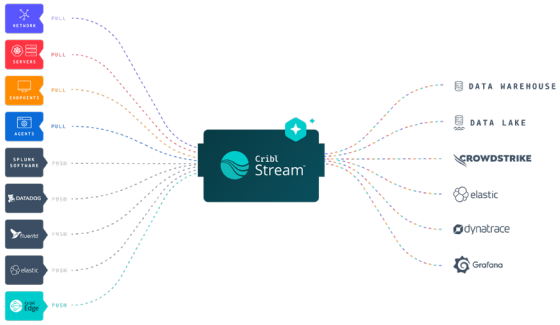
BEFORE

The Reality of Data Growth*



AFTER

Driving Security Outcomes Through Better Data*



With Cribl, optimizing your SIEM migration is a straightforward process. First, you get in control of your telemetry by converging all your sources into Cribl Stream. You can also collect and analyze data at the source using our Cribl Edge agent.

KEY BENEFITS

Send all your data to your SIEM

A telemetry pipeline can handle data quality so the new SIEM is not flooded with duplicate or low-fidelity data. Improving data quality allows you to increase cost efficiency while leading to reduced fatigue, faster response, and overall better security outcomes.

Ensure a secure integration

A telemetry pipeline facilitates a secure and efficient SIEM migration by simultaneously feeding both legacy and new SIEMs. This maintains security posture while allowing comprehensive testing on a cloned production dataset in the new SIEM, minimizing risks.

Avoid vendor lock-in

Freeing data intake from particular SIEM platforms enables security teams to respond swiftly to evolving risks, optimize resource allocation, and enhance overall system efficiency, irrespective of their existing SIEM setup or future technology choices.

Optimize storage and retention

Storing all logs in SIEMs increases storage expenses without necessarily improving security. A comprehensive telemetry pipeline allows engineering teams to manage data costs effectively by tiering data based on its value and storing it accordingly.

Note: Every SIEM is different! Check out our white paper for more guidance on requirements gathering, mapping existing use cases, and validating detection coverage in the new environment.

>"SECURE YOUR SIEM MIGRATION TODAY"_

Total telemetry control to support migrations

Taking control of your telemetry data means shifting from managing security tools to strategically leveraging your security data. By focusing on telemetry first, you gain the **choice**, **flexibility**, and **control** to direct security data to the most appropriate systems and storage. This approach also enables you to optimize the data's value, no matter how you use it for security monitoring or investigations.

Data optimization by source

39%
Syslog Collector

64%
Cloud Activity Logging

48%
Windows Event Logs

71%
Secure Web Gateway

49%
Endpoint Detection and Response (EDR)

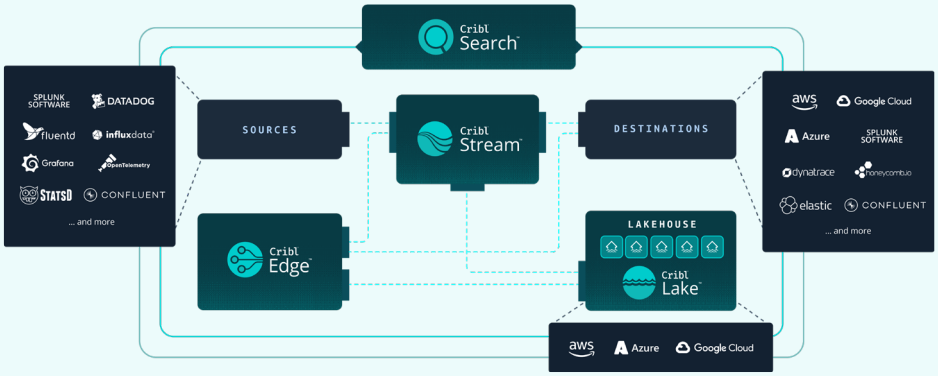
74%
Database Activity Monitoring Logs (SQL)

49%
Next-Generation Firewall/ Network Security

A **complete** observability pipeline—from source to lake.

STREAM

Cribl Stream is a data pipelining engine for routing and processing IT and security data. With Stream, you can route, reduce, reformat, enrich, or shape data from any source to any destination – allowing you to control, optimize and add context to all your data sources.



Cribl works with any vendor, so you can too

Get logs, metrics, and traces from any source to any destination.

Cribl consistently adds new integrations so you can continue to route your data to and from even more sources and destinations in your toolkit. Check out our integrations page for the complete list.

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

>"SECURE YOUR SIEM MIGRATION TODAY"_