OVERVIEW

Secure your SIEM migration today

Reduce migration risk, control costs, and keep your security data flexible.

Cribl

The **AI Platform** for Telemetry

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 is growing faster than ever, but budgets aren't keeping up

30%
CAGR of telemetry data creating massive implications for storage and analysis.[1]

[1]Source: IDC

7%
IT budget growth rate; IT budgets are vastly outpaced by data growth

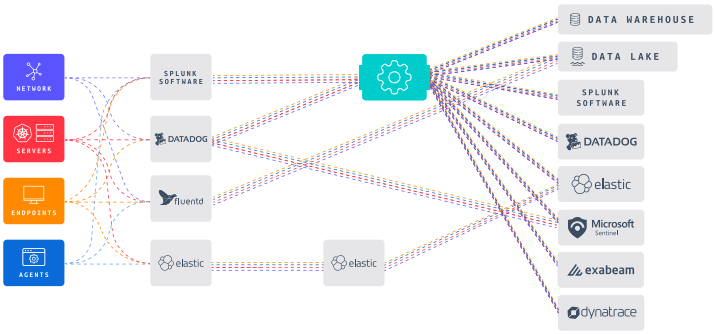
Why build a modern, vendor-agnostic security data strategy?

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.

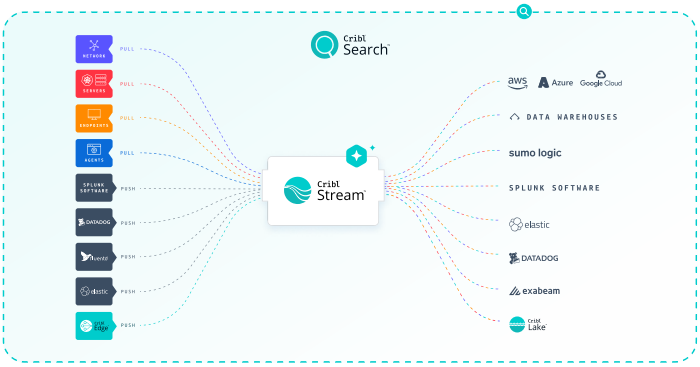
Before

The reality of data growth



After

Driving security outcomes through better data



With Cribl, you get control of your telemetry to simplify SIEM migration. Start by bringing your sources into Cribl Stream. Cribl Edge provides endpoint telemetry collection when agent replacement is needed. Cribl Lake offers tiered, open-format storage to retain bulk and compliance data at lower cost without inflating your SIEM bill, while Cribl Search lets your team query that data wherever it lives.

Key Benefits

Optimize data before it reaches 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

Cribl Stream's telemetry pipeline enables a secure SIEM migration by feeding both legacy and new SIEMs. This maintains security posture while supporting comprehensive testing on a cloned production dataset, minimizing risk.

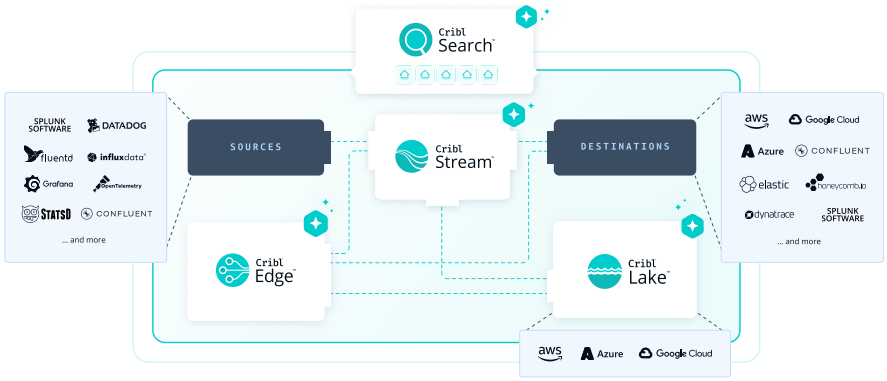
Avoid vendor lock-in

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 a SIEM raises costs without improving security. Cribl Stream sends only high-value data to the SIEM, while Cribl Lake stores bulk data cost-effectively. Cribl Search enables investigation across all data without moving it, helping control costs.

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.



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.

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

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.

elastic | Azure | SPLUNK SOFTWARE
Google Cloud | aws | CROWDSTRIKE
exabeam | WIZ | CONFLUENT

Product Overview

CRIBL STREAM is a telemetry pipeline 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, helping you control costs, add context, and prepare data for AI.

CRIBL EDGE is a vendor-neutral agent that collects, processes, and routes telemetry directly at the source. With Edge, you can centrally manage your agent fleet, reduce data volumes, and deliver the right endpoint data to your SIEM, analytics, and AI tools.

CRIBL LAKE is a turnkey data lake for cost-effectively storing and retaining IT and security data. With Lake, you can tier lower-value and compliance data outside your SIEM while keeping it accessible for investigations and future analysis.

CRIBL SEARCH is a search-in-place solution that lets teams investigate data wherever it resides. With Search, you can query data across Cribl Lake and other object stores, use AI-assisted investigations, and uncover answers without first moving data back into your SIEM.

Cribl

The AI Platform for Telemetry

Learn more at cribl.io | Join our Slack community
Try Cribl Sandboxes | Follow us on LinkedIn and X

OPG-0032-EN-1-0726