>SOLUTION BRIEF_

# EL3 made easy: Cribl Stream for federal event log management.

## THE CHALLENGE

A recent executive order directed federal agencies to improve cybersecurity investigative and remediation capabilities. Agencies must reach the highest level of logging maturity to meet 2024 requirements.

## THE SOLUTION

Cribl Stream acts as the strategic control plane between logging sources, analytics platforms, and repositories – supporting the most critical elements of EL3 maturity by augmenting existing logging environments. With Stream, federal agencies can accelerate time to maturity without expensive, risky lift-and-shift tactics.

## THE BENEFITS

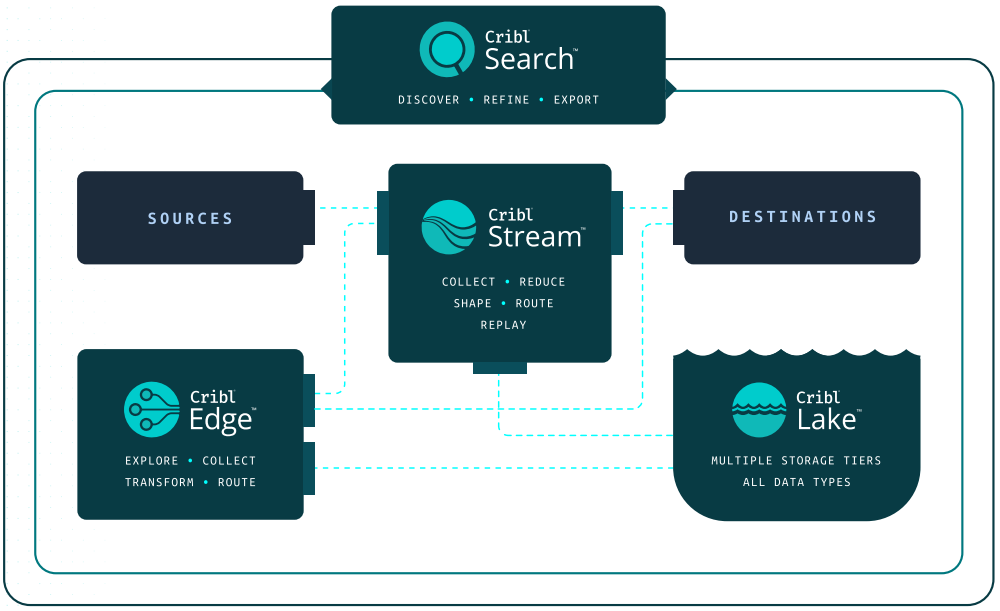
- Route data from any source to the most cost-effective destination.
- Get further insights into organizational data by aggregating logs into summary metrics.
- Redact personally identifiable information (PII) from data in flight.
- Monitor observability pipelines in real time to inform critical decisions.

**Accelerate log management maturity with the leading data processing engine.**

A recent executive order directed federal agencies to take decisive action to improve cybersecurity investigative and remediation capabilities. Effective policies around logging, retention, and management are essential for improving these capabilities, and OMB-issued guidance details a maturity model for event log management. With Cribl Stream, advanced maturity is within reach for federal agencies.

Federal agencies are still challenged to reach the highest logging maturity levels before a new threat intelligence platform rolls out in 2024[1]. Using Cribl Stream as the strategic control plane between logging sources and the range of analytics platforms and repositories in use, federal agencies can accelerate their time to maturity without expensive, risky lift-and-shift tactics.

Out of the box, Cribl Stream supports the most critical elements of each maturity level by augmenting your current logging environment.



## How it works.

Streams processing engine  sits between the multiple sources of log data in your agency, allowing you to route, filter, enrich, redact, and govern data in flight – before it reaches downstream analytics and security tools. Purpose-built for logging and event data, Stream offers native protocol support, rich data management capabilities, and role-based access control for use in the most demanding environments.

### Route data from any source to the most cost-effective destination.

With Cribl Stream, agencies can send data to the most effective destinations, including low cost storage locations like Cribl Lake or customers choice of  object stores for long-term retention and compliance with CISA and FBI standards and regulations. Administrators can quickly route data to the best tool for the job — or all the tools for the job — by translating and formatting data into the tooling schemas agencies require. Different departments in each organization can choose different analytics environments without deploying new agents or forwarders or diverting funds from digital transformation.

### Get further insights into organizational data by aggregating logs into summary metrics.

Cribl Stream gives agencies the power to extract fields of interest and publish the result to metrics. Once aggregated, agencies will see a major reduction in event counts and data volume, freeing up valuable licensing capacity in their analysis tools. Stream also enables flexibility and choice for federal agencies, giving these organizations the option to send the resulting metrics to their analytics tool(s) or route them to a dedicated time series database for efficient storage and retrieval. Using these methods, agencies can get further insights into their data and better understand new data sources they are onboarding as part of any digital transformation efforts.

**Reduce as much as 50% of ingested log volume, to control costs and improve system performance.**

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

### Redact personally identifiable information (pii) from data in flight.

Use Cribl Stream's out-of-the-box Mask function to mask or obfuscate data in motion. Put simply, organizations can encrypt sensitive data in real time before it is forwarded to and stored at a destination, ensuring anonymity for every data type. Stream helps agencies comply with evolving privacy and confidentiality regulations.

### Monitor observability pipelines in real time to inform critical decisions.

Stream also gives federal agencies the ability to reduce management overhead, with a robust and easy-to-use GUI-based configuration and testing interface. Operators can capture live data and monitor their observability pipelines in real time, enabling further visibility to inform maintenance and other critical business decisions.

1 Internal reference https://www.gao.gov/assets/d24105658.pdf

**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-0024-EN-2-0524