>SOLUTION BRIEF_

Take control over your federal observability data with AWS and Cribl.

Unlock data from proprietary formats to gain control over your data with Cribl. Route it, shape it, store it, and then replay the important data to the right tools and teams.

The challenge.

While log analytics solutions have come a long way, public sector organizations are still lacking flexibility when viewed through the lenses of ingest, search speed, scale, and usability. Many tools and platforms make it difficult to send data to third-party analytics vendors—they want you to use their stack. Federal operations and security teams are stuck with data in expensive cold storage that is held in proprietary formats and requires a manual process to thaw data and transform it back to the original format.
On top of this, with the exponential growth of data volumes and an increased number of federal data and logging mandates to address, agencies are unable to get visibility over data, take control of data sharing with other teams, and afford the increasing costs that come with storing it. All of this leads to a disjointed understanding of the security, performance, and general health of your environment.

DID YOU KNOW?

You can deploy Cribl solutions in your AWS GovCloud environment to ensure you meet security and compliance requirements at every stage of your cloud journey. Leverage Cribl's CloudFormation template on AWS Marketplace to help you get up and running.

The solution.

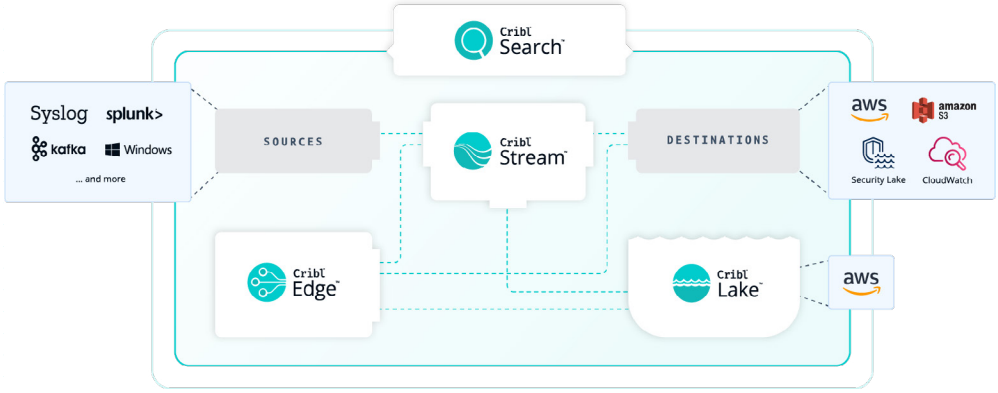
Cribl's next-generation data engine is built specifically for IT and Security data and provides a unified data management solution for exploring, collecting, processing, and accessing data at scale. Whether you're looking to export large volumes of data with minimal impact on your existing logging solution or want to fork open-format data off to low-cost storage to meet retention requirements, Cribl has you covered.
With complete control and flexibility to access, explore, discover, collect, and process data at scale, enterprises can experience the difference between an alright analysis experience to a great analysis experience. The best part? It works with all of your tools without needing new agents deployed. Get the right data, where you want, in the formats you need. Instrument everything, analyze more data, and pay less. Query your data wherever it lives, and finally go from petabytes to insights.

- **Cribl Stream** – A data collection, reduction, enrichment, and routing system for IT and security data. Retain a full-fidelity data copy in a lower-cost cloud storage and replay/analyze that data when needed.
- **Cribl Edge** – An intelligent, scalable, edge-based data collection system for logs, metrics, and application data. Enable administrators to easily provision datasets to their security and operation teams.
- **Cribl Search** – Find and access data regardless of where it is landed and in any format. Perform federated search-in-place queries on any data, in any form without having to move it or index it first.
- **Cribl Lake** – A simplified storage solution that allows organizations to easily store, manage, and access data. Leverage open formats — no pre-defined schema required, unified security with rich access controls, and centralized access to all IT and security data.

CUSTOMER STORY

The Accenture Federal Services team is using Cribl Stream to deliver fast, accurate decision-making power to their major federal customer in a high-stakes environment. With growing traffic levels of over 5TB a day, the customer is aggregating data feeds from agencies across 90 separate sites as well as a variety of types of custom sensor data.

Cribl Stream within the AWS GovCloud ensures that the data ingested is clean and in the right formats, providing visibility into the integrity of the content being acquired and processed.



Use cases.

Speed up cloud migrations.

Move to the cloud faster or upgrade existing cloud infrastructure to help you hit timelines without risk of losing data. Freeing your data from proprietary formats opens up flexibility to take on future migrations and room for additional data sources to onboard.

Easily meet mandate requirements.

Collect and store AWS CloudTrail logs, VPC Flow Logs, and any other AWS high-priority data types defined by the M-21-31 memorandum to swiftly address current logging and data retention mandate requirements and gain the flexibility to comply with future executive orders.

Route and enrich security.

Streamline data onboarding from third-party sources and increase the value of data by enriching it with context like GeoIP and known threats databases before reaching any storage tooling. Plus, send a full-fidelity copy of security data to S3, and route it to any analytics tool of your choice and replay it any time for future analysis.

Retain a full-fidelity data copy in a lower-cost cloud storage, but still be able to replay and analyze it at will.

Enable administrators to easily provision datasets to their security and operation teams.

Perform federated search-in-place queries on any data, in any form.

Simplified storage solution that allows organizations to easily store, manage, and access data.

Summary.
Cribl helps you unlock more options for your data – and your organization. It goes beyond just collecting data from any source and delivering it anywhere. Cribl gives you control to choose the best tools for your use case and send the right data to the right teams – regardless of your current vendor.

With Cribl's suite of products, customers can:

- Accelerate cloud migrations
- Enrich and route data from any source to the most cost-effective destination
- Reduce data volume to keep costs down while meeting retention mandates

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

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-1-0524