>CASE STUDY_

Fast Food Chain Cuts Data Egress Costs, Resolves Data Compatibility Issues and Transforms Observability Strategy

HIGHLIGHTS

- 66% reduction in syslog data volume, reduced overall log storage costs from $70,000/month to $30,000/month.
- 10x reduction in storage costs for meeting compliance requirements.
- Improved troubleshooting via in-flight data enrichment and real-time data visualization.

This global fast food chain, with over 35,000 locations in 100 countries, started a global observability initiative to streamline data collection, standardize logging, and reduce storage costs. The network infrastructure and operations team focuses on global monitoring at scale, managing thousands of sites, data centers, and platforms around the world–and need maximum efficiency when handling such a vast scale.

By sending IT and security logs to multiple tools, the team found most of their time consumed by repetitive data onboarding tasks. They saw an opportunity to optimize by implementing a unified observability pipeline, leveraging Cribl Stream to centralize and streamline their data flow. Cribl quickly became more than just a tool; it was a strategic partner, reshaping their observability approach.

Powering Multiple Observability and Security Tools with a Unified Telemetry Data Pipeline

As a multinational enterprise, there are various stakeholders for the company's observability data, Stream ensures the right data gets to the right place.

> **"We need to ship our security logs to at least three different teams, all with different security platforms. We also put the logs in Amazon S3 for long-term data retention and storage. Using Cribl reduces the complexity of that deployment, making it easy to stream the data to multiple destinations."**
>
> **—Senior Technical Product Manager**

Before implementing Cribl, the organization was spending valuable resources to stream multiple copies of the same data to all of their monitoring tools.

"Having Cribl just eliminates a lot of complexities and allows you to be more creative. it makes evaluating and onboarding new tools faster and makes your other tools better."

"Since we brought on Cribl, we no longer have to send the same copy of our syslog data from the source to multiple places. Our log volume has been reduced essentially by two-thirds."

—Senior Technical Product Manager

The network infrastructure and operations team also uses Cribl to handle their volume-intensive firewall logs, consolidating all the data from their restaurants into a single, daily integration. This process reduces bandwidth even further — consolidated data is sent to AWS and then pushed to necessary destinations from there, streamlining data egress from 600 MBps to 200 MBps–equating to a log volume reduction in the neighborhood of 131 TB/month.

Reduced Costs of Compliance and Data Storage

Reductions in data volume have also had some downstream effects. Since they can keep full-fidelity copies of their data in low-cost storage like S3, the costs and complexity associated with meeting compliance requirements have dropped significantly.

"After we use Cribl to stream data to S3, the only costs are for AWS storage, which is much cheaper compared to other platforms. We're talking about a reduction from 20-30 cents per gigabyte to just 2 cents per gigabyte."

—Senior Technical Product Manager

When one internal group switched from storing logs in New Relic to sending them through Cribl Stream to S3, they saw a significant reduction.

"We had a situation where one team was spending $70,000/month for log storage. When we optimized and routed that data with Cribl, we were able to send only what was relevant for New Relic monitoring and dashboards, and send the rest of the data to S3. We're saving $40K per month because of Cribl from this one use case."

—Senior Technical Product Manager

As they move forward from the beginnings of their Cribl deployment, the organization expects to see more use cases and success.

"We tested two new vendors by feeding them the same data with Cribl stream, and saved a ton of time on testing and deployment."

Kicking Off a Global Security Operations Center Initiative

The benefits of Cribl extend beyond just the network infrastructure and operations team. The incident management team uses Stream to correlate all the data moving through its AIOps platform, and the security team plans to use it to deploy their global Security Operations Center (SOC) initiative.

"We'll use Google Chronicle to integrate all the logs and data sources for our global SOC project. The plan is to move all the data through Cribl Stream so we can make use of all of the capabilities that other tools lack."

—Senior Technical Product Manager

Having all the data in one centralized location has simplified the process of sending data to different internal teams and onboarding data from new applications.

"Cribl has really helped us deploy new tools faster. It takes away the complexity of onboarding data and new tools, and if another team is interested in a data source, we can just create a feed for them."

—Senior Technical Product Manager

Improved Data Compatibility for a Diverse Tool Set

They also use Cribl Stream to improve the operational efficiency within the organization. When data needs to be cleaned up before it's stored or shared, it's easy to get rid of the noise.

"Cribl helps us solve standardization issues like incorrect host names or timestamps. We can fix log names, get rid of duplicate IDs, and shape or transform the data for better compatibility between our tools."

—Senior Technical Product Manager

The formatting capabilities have come in handy for a number of different projects, allowing the team to come up with creative solutions to unique problems.

"When our Palo Alto Networks log collector was showing the collector name as the host instead of the firewall name, we used Cribl to correct it. We also transformed DNS logs from .csv to another format that was more compatible with our security analytics platform."

—Senior Technical Product Manager

Enriching Data for Troubleshooting; Transforming Data for Compatibility

The fast food chain also uses Cribl Search to examine historical logs when they encounter network issues. If the security team needs information about specific IPs or users, the network infrastructure and operations team find it using Search and generate a file to pass along. Querying the data in place before deciding which (if any) data to move eliminates noisy data thus accelerating the performance of their AIOps platform.

To make that data as useful as possible for troubleshooting, they use Cribl Stream to add relevant tags to events.

> **"The biggest value we see from Cribl is being able to transform data in flight. We can add city, region, or country names so that data is enriched and normalized before it's ingested into another platform and used for correlation analysis. Other platforms just aren't designed for this level of enrichment."**
>
> **—Senior Technical Product Manager**

These enrichments allow their AIOps tools to correlate issues across different sites and regions. For example, if multiple sites in the same city experience problems simultaneously, the AIOps software can use the Cribl-added enrichments to identify and analyze the situation, significantly speeding time to resolution.

The organization has also benefited from real-time data visualization within Cribl Stream.

> **"Tapping into the logs to see real-time volume and events per second really helps us with troubleshooting. Being able to see bytes per second now vs the weekend or other times has been helpful for trending and planning."**
>
> **—Senior Technical Product Manager**

TL;DR

- **Cribl enabled efficient data streaming to multiple destinations, reducing log volume by two-thirds, saving network bandwidth, and reducing egress costs.**
- **Creating a data pipeline improved overall data standardization and compatibility across diverse tools.**
- **Easier to visualize logs, volume, and events per second for better network management.**
- **Using Cribl Search to examine historical logs when troubleshooting network issues, helping them save on ingestion costs by only pulling relevant data.**

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

CS-0031-EN-1-1124