>CASE STUDY_

At an International Convenience Store Conglomerate, Cribl Stream Paid for Itself by Optimizing Logs—Now It's Simplifying Compliance and Increasing Business Visibility

HIGHLIGHTS

- Stream helped reduce the volume of logs sent to Splunk by 50%, Windows logs by 53%, Okta logs by 61%, firewall logs by 41% for firewall and Windows Service logs by 40%.
- Onboarding new sources to Splunk now takes less than an hour, down from a full week.
- Cribl Stream simplified PCI DSS compliance by automatically applying the right retention periods based on the data type.
- Stream enabled developers and application admins easy access to application events and monitor resources, to quickly identify performance issues.

An international convenience store conglomerate operates 14,000 convenience stores in 20 countries and supplies jet fuel to more than 140 airports. Business is growing—and so is the log data produced by security devices, servers, and applications running in multiple clouds and colocation facilities in North America and Europe.

"We used to route all security log data to Splunk for monitoring," says the international convenience store's Security and Compliance Director, IT. "But only a small fraction of the 25 billion monthly events we see are significant. To make the most of our volume-based Splunk license, we had to be strategic about which data we were sending to Splunk for analysis."

While he was at it, the director also wanted to start collecting application event data for the developers who produce the games on their website, which brings customers into stores to collect their prizes. Otherwise, developers would find their own ways to get that data, a security risk.

Cloud Egress and License Savings "Right Out of the Box"

The convenience store conglomerate found its answer in Cribl Stream, recommended by Trace3, an IT service provider. "We liked the flexibility of having a single observability pipeline that can collect data from any source and forward it to any destination, including Splunk or a data lake in AWS S3," says Security and Compliance Director, IT. Cribl worker nodes installed in public clouds encrypt, compress, reduce, and enrich log data before forwarding it to the destination.

> **"On the first day of the proof of value I knew we'd found our solution. Right out of the box Cribl Stream reduced log volume, cloud egress costs, and Splunk license costs."**
>
> —Security and Compliance Director, IT

> "When we plug a new data source into Cribl Stream, we can sort out what we need to ingest into Splunk in less than an hour, sometimes minutes, and adjust the filter on the fly. Adding a new data source in Splunk typically took a full week."
>
> —Security and Compliance Director, IT

During the proof of value, the team saw:

- **53% reduction** in size of Windows logs by cleaning up white space, dropping low-value fields like comments, and reformatting in JSON.
- **61% reduction** in size of Okta logs and 47% fewer logs by dropping synthetic log data.
- **41% reduction** in firewall logs .
- **40% reduction** in size of Windows Service logs.
- **99% reduction** in number of Perfmon logs and 93% reduction in size of Perfmon logs.

More Splunk License Headroom, New Data Sources In Minutes

The data volume that Splunk ingests dropped by about half, freeing up existing license for more data sources. Equally valuable, adding new data sources for security investigations now takes minutes instead of days.

> **"When we plug a new data source into Cribl Stream, we can sort out what we need to ingest into Splunk in less than an hour, sometimes minutes, and adjust the filter on the fly. In contrast, adding a new data source in Splunk typically took a full week. We've shifted our efforts from mundane work like adding data sources to strategic activities that strengthen security and compliance."**
>
> **—Security and Compliance Director, IT**

Simpler Compliance with Automated Retention

Cribl Stream also simplified compliance with Payment Card Industry Data Security Standards (PCI DSS) rules. Depending on the nature of the data, retention periods vary from 90 days to 13 months. For simplicity's sake, the company used to retain it all for 13 months.

> "Right out of the box Cribl reduced log volume, cloud egress costs, and Splunk license costs."
>
> —Security and Compliance Director, IT

> **"Now that we have Cribl Stream look at the host, user, and event type to fork the relevant events to the Splunk index with the right retention period, storage costs have dropped."**
>
> **—Security and Compliance Director, IT**

Getting the Right Data to the People Who Need It

Having met goals to reduce log volume and costs, the team is starting to use Cribl Stream to help IT and security practitioners work smarter. For example, to record changes to a SaaS application that's subject to SOX controls, the director quickly wrote a script that detects file changes and who made them. Cribl Stream forks the information to a Splunk index. "Automating this process satisfies the auditors and our own internal controls," the director says.

Windows admins can more quickly zero in on performance issues thanks to the more compact Perfmon logs. A Cribl lookup table filters the data based on host and process names, ignoring processes that are currently running. Developers can see significant application events and monitor resources. "We're pulling application logs into Cribl and then forking them to developers' Slack channels," the director explains.

> “Reduction in log volume paid for Cribl out of the box—and everything else is gravy. When I talk to people about Cribl, I say, ‘Make a wish list for what you want to do with your log data and take that wish list to Cribl. Don’t just ask them to do what you’re already doing today because with Cribl you can do much more.’”
>
> —Security and Compliance Director, IT

And Cribl Stream saved the day when Splunk temporarily couldn’t retrieve log data from some cloud apps. the team temporarily pointed all data sources to Cribl, which forwarded the important log data to Splunk. “Reduction in log volume paid for Cribl out of the box—everything else is gravy,” the director says.

> **“When I talk to people about Cribl, I say, ‘Make a wish list for what you want to do with your log data, and take that wish list to Cribl. Don’t just ask them to do what you’re already doing today because with Cribl you can do much more.’”**
>
> **—Security and Compliance Director, IT**

Find out how your business can implement an observability pipeline to parse, restructure, and enrich data in flight, while cutting costs and simplifying operations.

Get Cribl, and take control of your data.

TL;DR

- Reduce log volume and Splunk license costs.
- License costs dropped because Cribl Stream filters the data ingested by Splunk.
- Compressing and reducing data in the cloud reduces cloud egress costs.
- Adding a new data source takes less than an hour—down from one week.
- PCI DSS compliance is simpler because data sources can be tagged with the right retention period.
- Cribl Stream forwards significant application events to game developers’ Slack channel, helping to improve quality and accelerate cycle time.

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-0018-EN-2-0524