CASE STUDY | FINANCIAL SERVICES

How Baird **Modernized Security Data Operations** and Improved Visibility

with Cribl Stream and Cribl Edge

Baird is a financial services organization operating a large and complex environment, with more than 1200 servers and over 1TB of data outflow per day. As data volumes increased and infrastructure expanded, the team encountered growing operational friction in its existing SIEM and log collection approach.

To address these challenges, Baird adopted Cribl in 2024, deploying Cribl Stream and Cribl Edge as a centralized data pipeline between log sources and downstream platforms.

Establishing a vendor-agnostic data control layer

To future-proof its data infrastructure and manage complex objectives—including ingesting cloud data and preparing for a SIEM migration—Baird needed a way to introduce control over data collection and routing without disrupting existing systems.

Cribl provided a solution by acting as a vendor-agnostic middle layer between log sources and the SIEM, while also introducing visibility directly into the data pipeline. Using Cribl Stream for routing and Cribl Edge for centralized collection, Baird added a control point in its telemetry pipeline while preserving its existing investments.

This architecture also made it possible to bring in cloud systems like Microsoft Azure. Previously, ingesting that would have required routing logs through on-premises collectors before sending them to the SIEM. With Cribl Stream, Baird can ingest and process these data sources directly and forward them downstream.

> "The quality of our data has vastly improved, which helps to make sure that queries run by our analysts against that data are trusted. The onboarding of new data sources has now been well documented and is easily repeatable, making our engineers more productive."
>
> **MIKE REINECK | DIRECTOR OF IT SECURITY | BAIRD**

Additionally, the team can see events coming into Cribl systems, monitor how data moves through the pipeline, and validate what is being sent out, giving them a clear view into whether data is flowing as expected, from an event count and volume perspective. This allows Baird to confirm that they are not unintentionally dropping events and that normalization does not significantly increase outbound data volume.

Highlights

- Centralized data pipelines across 1,200+ servers and 1TB+ of daily data using Cribl Stream and Cribl Edge
- Gained more visibility into inbound and outbound data flow
- Enabled Azure and other cloud data ingestion without on-prem routing complexity
- Improved data consistency and visibility while routing and bifurcating logs to multiple destinations

Cribl | BAIRD

Baird implemented Cribl Stream and Cribl Edge alongside a move to a new SIEM, with pipelines established within a couple of weeks. Cribl now serves as the data pipelining solution for Baird to ingest, normalize, and route data to different destinations, such as their SIEM and observability systems.

Ensuring data consistency though normalization

For Baird, Cribl is essential for normalizing and fixing data sources before sending them to downstream platforms. The team doesn't focus heavily on reducing data volume in Stream, instead prioritizing having as much data as possible available for reporting.

Baird uses Cribl Stream extensively for routing and normalization, including correcting formatting issues and enriching events with additional metadata. This has improved the quality of data and helped ensure that it is parsed correctly within the SIEM.

One example is Baird's ingestion of Microsoft Azure events through Event Hubs. These events originate from different PaaS services and do not follow a consistent format. Baird uses Cribl Stream to normalize these variations so that outbound data is consistent, improving downstream parsing and overall data health, resulting in higher confidence during investigations.

Centralizing endpoint management

Baird uses Cribl Edge to collect events across both Windows and Linux servers. One of the primary reasons for selecting Edge was the need for a central management point, rather than an individual endpoint management.

With Cribl Edge, the team now manages configurations from a single interface. They are now able to maintain a regular update schedule and make configuration changes more easily through the UI.

Cribl Edge also enables processing directly on the endpoint, including normalization and selective filtering. Baird uses this capability to drop some unwanted events at the source, reducing some noise in the system and controlling SIEM ingest.

TL; DR

- By implementing Cribl Stream and Cribl Edge, Baird introduced a centralized data pipeline that improves visibility into data flow and provides more control over how data is collected and routed.
- Cribl enabled Baird to ingest cloud sources like Microsoft Azure, normalize inconsistent data, and deliver more reliable data to downstream platforms.
- With centralized endpoint management and flexible routing to multiple destinations via Cribl Stream and Cribl Edge, Baird now operates a more manageable and scalable security data pipeline.

"Knowing that our data is well parsed means that we can trust the results when we're hunting for anomalies, or just reporting on something in general."

MIKE REINECK
Director of IT Security
Baird

"Having a single management plane has been nice, it was a key feature we were looking for. With Cribl Edge we have a regular update schedule, which has security benefits that we didn't have before."

MIKE REINECK
Director of IT Security
Baird

PRODUCTS USED

Cribl Stream™ Cribl Edge™

Cribl®

The AI Platform for Telemetry

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

CS-0052-EN1-0626