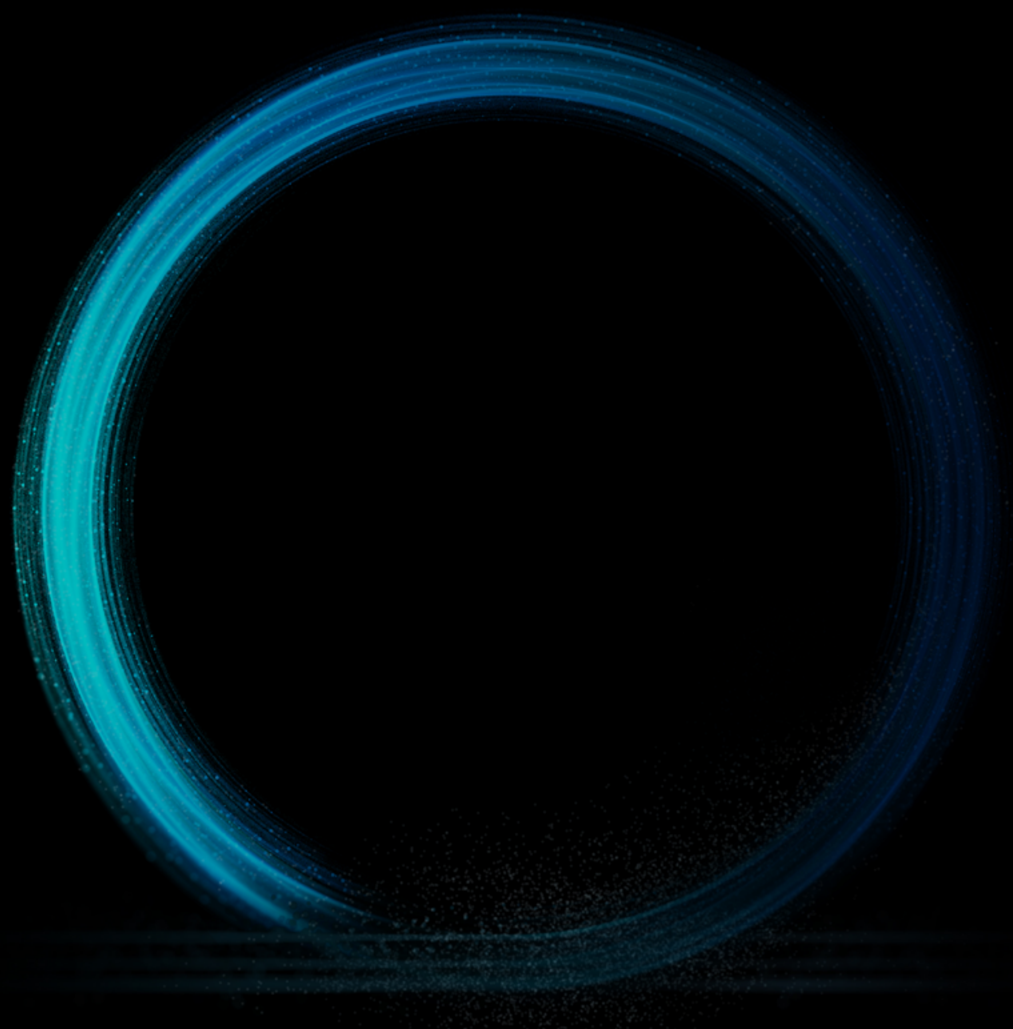
SOLUTION BRIEF

Cribl LogStream™ Replay



THE CHALLENGE

Organizations need a way to analyze data from batch sources to complement streaming data. Retaining data in analytics systems can be too expensive – teams need a way to store it cheaply and analyze it when needed.

THE SOLUTION

LogStream lets you land data in lower-cost storage and replay it to an analytics system later. LogStream collects data from APIs, processes it, and replays it through LogStream.
You can reprocess and route replayed data to any destination while keeping the original version.

THE BENEFITS

- Easily collect data from multiple sources, including REST APIs
- Schedule batch collection jobs for routine processing and routing
- Route data to low-cost object store for durable, indefinite retention
- Replay data from object storage to analytics systems as needed

SOLUTION BRIEF

Cribl LogStream™ Replay

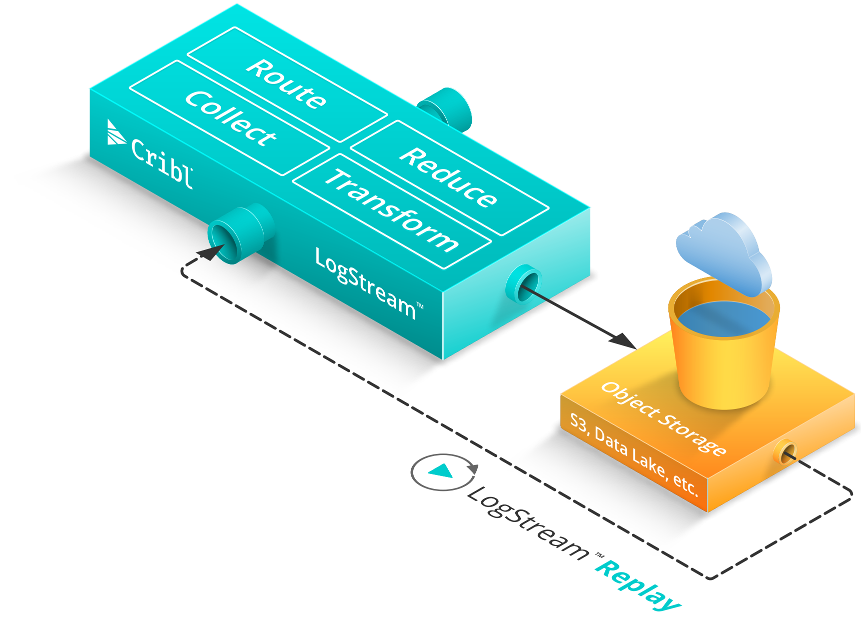
Replay observability and security data to the best analytics system whenever you need insights. Get the right data, in the formats required into the tools you choose. Streamed in real-time, collected on-demand, or collected on an easily configured schedule.

The Challenge

Getting all of the data you need to analytics systems, to drive insights for observability and security efforts, can be very difficult. Organizations are exhausted from using the wide range of labor-intensive workarounds to get this data. At the same time, the costs associated with storing this data are exploding. This creates difficult decisions about how much data they can afford to keep, and what the consequences may be if they discard data.

The Cribl Solution

LogStream is the best way to replay multiple data formats to your analytics tools. Use LogStream as a universal receiver to collect from any machine data source – and even to schedule batch collection from multiple APIs. In addition, recall data from low-cost storage, to replay logs to analytics tools for later investigations with ad-hoc data collection.



Facets of LogStream™ Replay

ROUTE FULL-FIDELITY DATA TO OBJECT STORAGE

Send data to the most effective destinations, including low-cost storage locations like S3, and file systems and data lakes for long-term retention. You can replay this data later if needed. You can be more discerning about what you pay to analyze now, and what you store cost-effectively to replay later.

REPLAY DATA TO ANALYTICS SYSTEMS

LogStream introduced the concept of batch log reprocessing with Replay. In addition to processing streaming data, LogStream allows you to collect data from a wide range of data sources, including object storage and REST APIs. Even if most of the data you analyze is in real time, empowering batch processing and Replay significantly expands not only the sources of data you analyze, but also when you can analyze this data. Batch collection and Replay give you control over your data.

COLLECT AND REPLAY FROM MULTIPLE SOURCES

With LogStream, you can process and replay logs and metrics data from all REST endpoints. Cribl offers several different ways to discover and retrieve REST data, with both known-structure and schema-agnostic retrieval options.

LogStream receives and replays data from many APIs and other data sources. These include Kinesis Firehose via the Kinesis HTTP endpoint, and raw HTTP data. LogStream can also replay batch data collected from the Office 365 Service Communications API, for service incidents on Microsoft cloud services. Similarly, LogStream can replay batch data from the Office 365 Management Activity API, for actions and events on Azure Active Directory, Exchange, SharePoint, and other Microsoft servers.

SCHEDULE BATCH COLLECTION FOR REPLAY

Scheduled Data Collection and Replay enables you to set recurring schedules for the distributed collection of data from multiple sources, and for replay to an analytics tool. LogStream allows you to configure collections based on resource filters and constraints. You can also limit concurrent running instances of ad-hoc and scheduled jobs.

BETTER SECURITY BREACH INVESTIGATIONS

Many security breaches are discovered long after they start, sometimes several years later. Most companies do not retain the data in their analytics systems that they would need to investigate these breaches, for more than a few months. LogStream allows you to park full-fidelity data in a low-cost storage location for years, if not indefinitely.

When security breaches are discovered, LogStream can efficiently collect data from object storage. LogStream then replays security data to any SIEM or UEBA systems, to quickly diagnose and resolve existing breaches and potential threats. LogStream enables an affordable way to retain more data for longer periods of time – while still making that data easily accessible for necessary investigations, whenever they happen.

Summary

Replay is a powerful feature of Cribl LogStream that introduces the concept of batch data processing and streaming to observability and security analytics tools. LogStream is the best way to unlock the value of data from any source, and to replay it to analytics systems to uncover insights. In one tool, an easy way to replay collected data from multiple sources.

Vendor-agnostic. Scheduled or on-demand.

ABOUT CRIBL

Cribl is a company built to solve customer data challenges and enable customer choice. Our solutions deliver innovative and customizable controls to route security and machine data where it has the most value. We call this an observability pipeline, and it helps slash costs, improve performance, and get the right data, to the right destinations, in the right formats, at the right time. Join the dozens of early adopters, including market leaders such as TransUnion and Autodesk, to take control and shape your data. Founded in 2017, Cribl is headquartered in San Francisco, CA. For more information, visit www.cribl.io or our LinkedIn, Twitter, or Slack community.