CHAOSSEARCH | Cribl

SOLUTION BRIEF

Gain Unlimited Visibility Over Logs with Cribl and ChaosSearch

SOLUTION BRIEF

Gain Unlimited Visibility Over Logs with Cribl and ChaosSearch

Remove cost and retention limitations to drive full visibility and access for search and analysis across ALL your logs.

The Challenge

Traditional SIEM, Application Performance Monitoring (APM) and Observability tools are very popular today because they use metrics and logs to provide a data-driven way to run the business. But as the ingest rate from all types of logs approaches 1TB per day, each of these tools can become too complex and too costly to operate. In addition, there is a growing desire to prevent vendor lock-in when using cloud-based services, maintaining full control of the log data stored and avoiding the costly data retrieval fees when exploratory analysis is required.

When facing this scenario, SREs and SecOps teams are forced to make risky tradeoffs between the breadth of captured data and how long they can retain it. If they shorten retention time to save money as their ingest rate rises, will they still be able to use data to determine root cause of their most prized customer? Logs are useless until you need them, and when logs are needed to resolve time-critical events like incident investigation, threat hunting, and malware research, companies resort to throwing money at the problem. But even then, analytics tools are only as good as the data they receive, they don't provide visibility across the entire log data set, making the CIO wonder whether this is all worth the cost. There must be a better way.

The Solution

Cribl Stream combined with the ChaosSearch Data Platform provides an elegant solution to overcome this challenge. First, Cribl Stream's out-of-the-box solution acts as a universal collector and receiver of security data sources, allowing SREs and SecOps teams to quickly ingest and normalize data using a best-in-class user experience. By leveraging Cribl Stream's data filtering capabilities, users can not only remove unwanted or duplicated log data, but also enrich it with context - automatically adding related data from external sources — all in real time.

After filtering and enriching the log data, Cribl Stream allows users to route it to multiple destinations — your SIEM, APM, and/or Observability solution — in addition to sending ALL the data to low-cost storage locations, like Amazon S3. Storing an additional copy of raw logs in cloud object storage allows customers to mitigate the costly vendor's re-hydration and data retrieval fees, but also enables ChaosSearch to provide full visibility and instant access to all their data.

THE CHALLENGE

Organizations facing increasing ingest costs and vendor lock-in are now forced to make tradeoffs between the breadth of captured data and how long they can retain it.

THE SOLUTION

Cribl Stream™ gives organizations the ability to filter and enrich log data, keeping only the data they need. Combined with the ChaosSearch Data Platform, customers can reduce costs, and maintain control – searching through stored data easily.

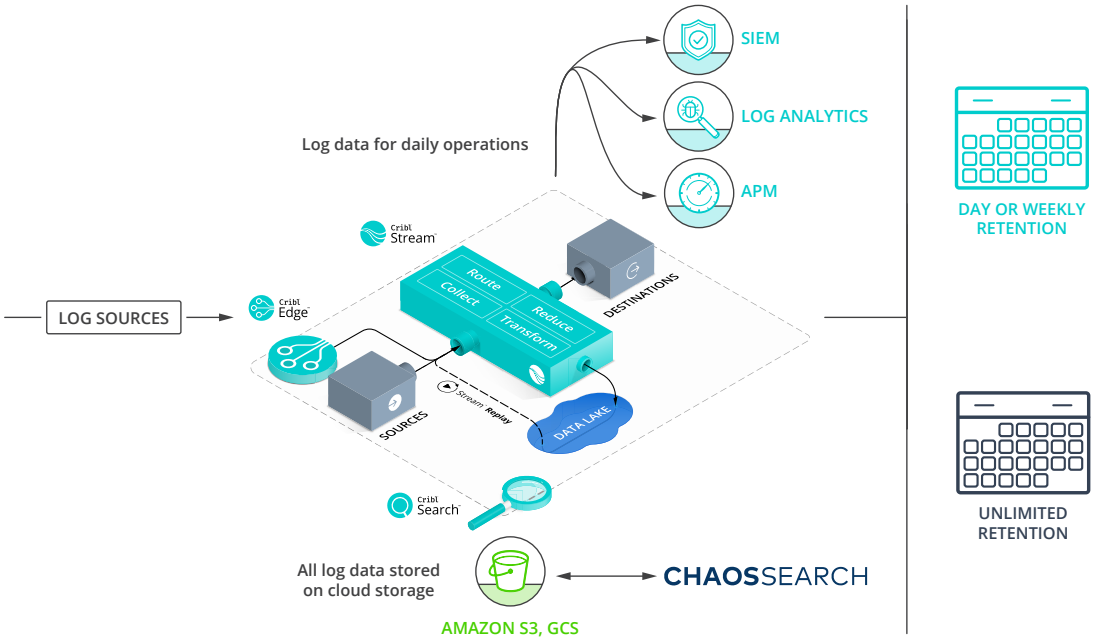
THE BENEFITS

- Collect data from any source and format into any scheme
- Filter and enrich log data to optimize the collection process
- Route to multiple destinations, including low-cost storage locations
- Search and analyze log data at scale
- Centralized repository gives instant visibility across all log data

CUSTOMERS USING CRIBL STREAM AND CHAOSSEARCH CAN LEVERAGE CURRENT SIEM, APM, AND OBSERVABILITY SOLUTIONS AT AN OPTIMAL LEVEL, AVOIDING RE-INGESTION COSTS AND STRICT DATA RETENTION LIMITS

ChaosSearch is delivered as a fully managed true SaaS solution, able to search and analyze raw log data at scale, directly from Amazon S3 without the need for any transformation. With ChaosSearch, SREs and SecOps teams now have a centralized repository where they can get instant visibility across ALL their log data stored, skipping the lengthy and costly process required by other solutions to transform and move the data in preparation for search and analysis.

The ChaosSearch platform changes the economics of operational analytics and serves as a new valuable tool to enable cost effective incident investigation, threat hunting, and malware research to support all the SIEM/APM/Observability tools. By using ChaosSearch for investigation and the analytics tools for just monitoring and response, you get the best of both worlds - keep using the monitoring tools you trust, but now the TCO becomes predictable and less likely to overrun due to shorter retention times and the elimination of rehydration.



The Benefits of using ChaosSearch with Cribl's Observability Solution

SIMPLIFY LOG DATA COLLECTION

Stream can translate and format data into any tooling schema, meaning you can collect all of your data once and repurpose it for any destination. This process reduces the duplication of data ingestion and allows different teams to pick the best analytics solutions. Customers who have an existing log collection or aggregation tier system can route the data to Amazon S3 while not impacting their existing solution.

UNLIMITED LOG RETENTION

Remove cost-related constraints by keeping all the log data on low-cost cloud object storage like Amazon S3, and enjoy unlimited log retention to support your analysis, investigation and research needs from this single source of truth.

INSTANT ACCESS AND FULL VISIBILITY INTO ALL LOG DATA

ChaosSearch transforms cloud object storage (Amazon S3) into a hot operational data lake, making log data instantly available for query and analysis. Avoid time-consuming re-hydration processes (and associated unexpected charges) before you can access your log data, especially in events like a security incident investigation where time to access data plays a critical factor.

Summary

Cribl Stream combined with the ChaosSearch Data Platform allows customers to leverage their current SIEM, APM and Observability solutions at an optimal level, enjoying the full breadth of capabilities but avoiding stretching the ingestion and retention limits of these tools, and the associated increase in complexity and cost.

With Cribl Stream and ChaosSearch customers can:

- *Simplify collection data by formatting into any tooling schema*
- *Keep all log data on low-cost storage options like Amazon S3*
- *Get instant access to their log data directly from Amazon S3 using ChaosSearch*
- *Reduce cost and complexity of the existing SIEM, APM and Observability tools*
- *Enjoy unlimited log retention in a very cost-effective way*
- *Improve incident investigation, threat hunting, and malware research capability by analyzing all your log data*

To get started with Cribl Stream and ChaosSearch today, **click here to try Cribl Stream Cloud** for free and **here to start a free trial of ChaosSearch**.

ABOUT CHAOSSEARCH

ChaosSearch empowers data-driven businesses like Blackboard, Equifax, and Klarna to Know Better™, delivering data insights at scale while fulfilling the true promise of data lake economics. The ChaosSearch Data Lake Platform indexes a customer's cloud data, rendering it fully searchable and enabling data analytics at scale with massive reductions of time, cost, and complexity. The Boston-based company raised $40M Series B in December 2020 and is hiring to support its hyper growth. For more information, visit **ChaosSearch.io** or follow us on Twitter **@ChaosSearch** and **LinkedIn**.

ABOUT CRIBL

Cribl makes open observability a reality for today's tech professionals. The Cribl product suite defies data gravity with radical levels of choice and control. Wherever the data comes from, wherever it needs to go, Cribl delivers the freedom and flexibility to make choices, not compromises. It's enterprise software that doesn't suck, enables tech professionals to do what they need to do, and gives them the ability to say "Yes." With Cribl, companies have the power to control their data, get more out of existing investments, and shape the observability future.Founded in 2017, Cribl is a remote-first company with an office in San Francisco, CA. For more information, visit **www.cribl.io** or our **LinkedIn**, **Twitter**, or **Slack** community.