Cribl

Liberate your data from vendor lock-in with Cribl and AWS.

Unlock data from proprietary formats to gain control over your data with Cribl. Shape it, store it, replay it, and route only the important data to any destination.

The challenge.

While log analytics solutions have come a long way, customers are still lacking flexibility when viewed through the lens of ingest, search speed, scale, and usability. Many tools and platforms make it difficult to send data to third-party analytics vendors – they want you to use their stack. Enterprises are stuck with data in expensive cold storage that isn't searchable, held in proprietary formats, and requires a manual process to thaw data and transform it back to original formats.

On top of mounting pressure of exponentially growing data volumes, IT and security teams are unable to get visibility over their data, leverage that data, and afford the high costs that come with storing it. You need the tools to analyze the widest set of data possible to truly understand the security, performance, and general health of your environment, and make the most out of your existing investments.

The solution.

So what do you do with all that data? Cribl's suite of products help you get complete control over your IT and security data, whether you want to route it, process that data in-flight, search it, and more. With Cribl, you can export large volumes of data with minimal impact to your existing logging solution. You can fork open-format data off to low-cost storage, reducing storage requirements related to retention and freeing up ingest volume for additional data sources.

The best part? It works with all of your tools without needing new agents deployed. Cribl's suite of products was built around protocols first, and can be customized around specific vendors as needed. Bring any source into the equation, and send that data to any system of analysis — or to multiple destinations at a time.

THE CHALLENGE

Enterprises are dealing with data stuck in expensive cold storage that isn't searchable, held in proprietary formats, and requires a manual process to transform back to original formats.
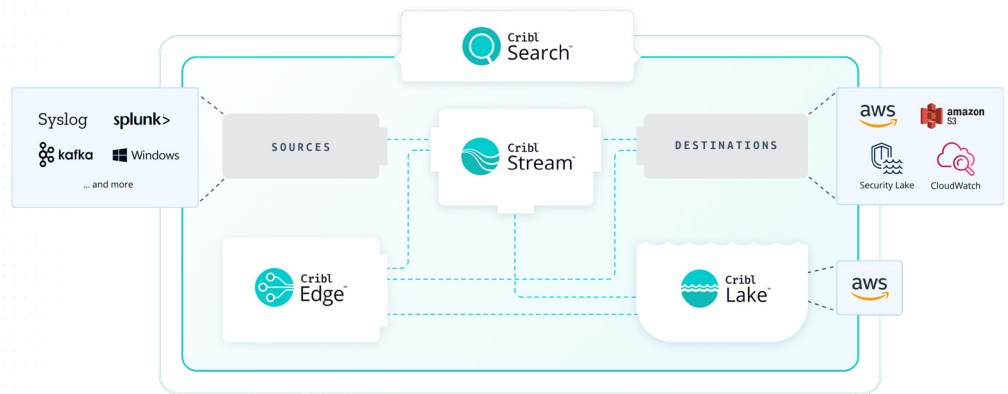
THE SOLUTION

Get complete control over your IT and security data, whether you want to route it to any tool, process it, replay it from low-cost object storage, search it, and more.

THE BENEFITS

Control Your data:
- Speed up cloud migrations.
- Quicker M&A.
- Route and enrich security data.

Route and process.

Discover, collect, and process data in real time, from your Linux or Windows machines, apps, microservices, etc. Get flexible options on a rich user interface for dropping, masking, and transforming data on the fly from all of your sources to the tools you choose. Filter, reduce, enrich, and aggregate the data, as well as transform proprietary data into an open format so that the data is in your control, making it infinitely usable across all of your observability and security tools.

Replay and search.

Replay fundamentally changes how organizations manage data by providing an easy way to ingest and re-ingest data into systems of analysis selectively. Route data to low-cost, long-term object storage, such as S3. Then, replay only the important information in any format to any destination. Efficiently search and parse through data at the source with Cribl Search. With a cost-effective way to explore all that data, you can query data at rest, at the edge, and in S3 without needing to bring data back in or store it in local storage.

Collect and scale.

Developers can easily share EKS data between security and operations, optimize data collection, and route to multiple destinations. With Cribl Edge, automatically collect logs, metrics, and application data at scale in any Linux or Windows environment.

Use cases.

Speed up cloud migrations.

Move to the cloud faster or upgrade existing cloud infrastructure with a data engine that can help you hit timelines without risk of losing data. Freeing your data from proprietary formats opens up flexibility to take on future migrations and room for additional data sources to onboard.

Quicker M&A.

An M&A is incredibly labor intensive for teams that need to share data with the acquirer for complete coverage, especially if it's locked in proprietary formats. Cribl Stream lets you make a proxy for M&A data - route important data to an existing SIEM alongside a copy back to mothership with the additional safeguards needed to mask sensitive data and protect PII.

Route and enrich security data.

SecOps teams need to reduce security data signal-to-noise ratio to get the best results from large, diverse datasets, but extracting the right information in real-time is difficult due to sheer volume. Use an easy UI to manage data and remove noise, enrich data with threat intelligence, and route it to your analytics tool of choice. Send a full fidelity copy of security data to S3, then replay data on demand into an analytics platform if an investigation comes up, reducing storage costs by 25% depending on your use case.

Summary.

Cribl enables observability by giving you the power to make choices that best serve your business, without the negative tradeoffs. As your goals evolve, you have the flexibility to make new choices including new tools and destinations. Cribl simplifies observability by putting the data you want, in the formats you need, wherever you want it to go.