>SOLUTION BRIEF_

Improve interoperability and search with Cribl and Amazon Security Lake.

Increase flexibility and streamline security data management and insights with Cribl and Amazon Security Lake.

The challenge.

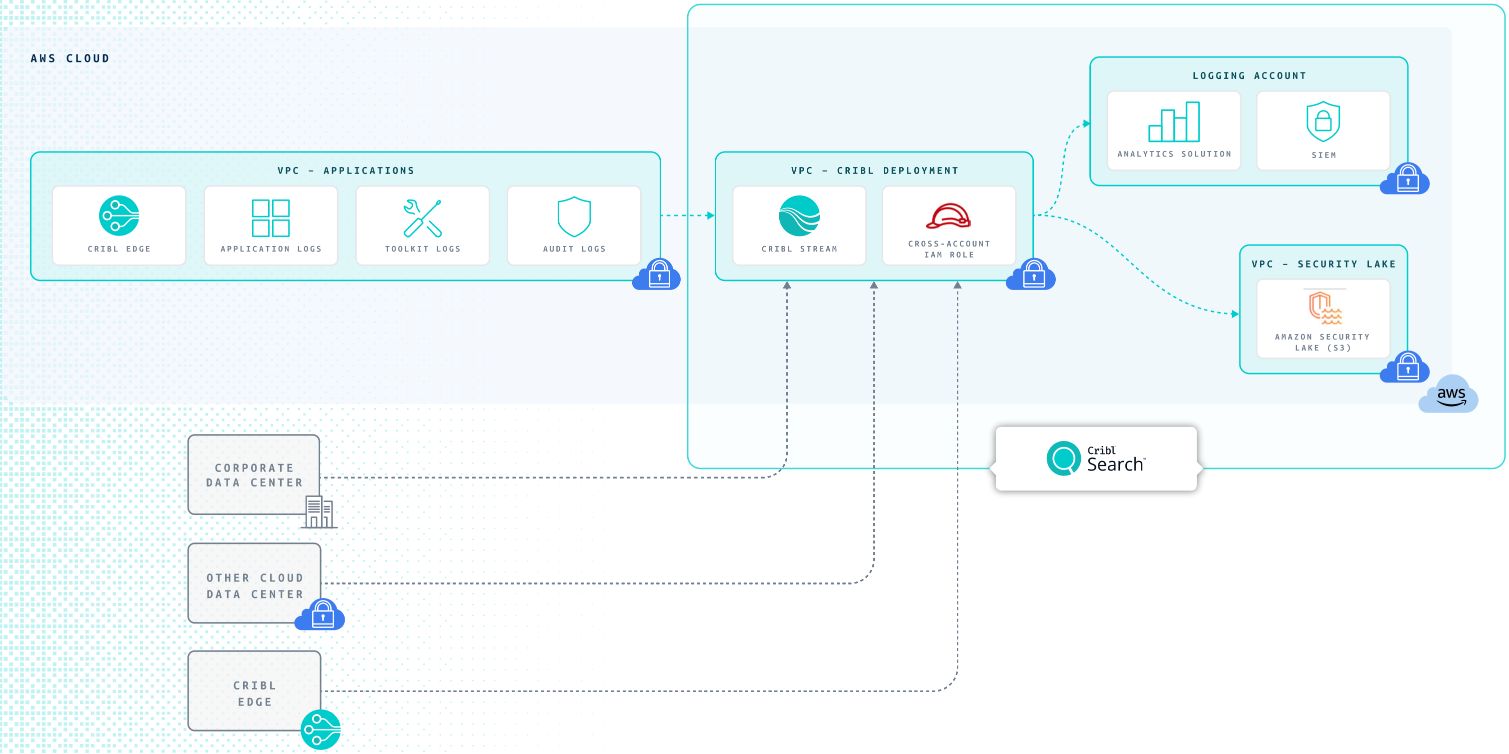
Security professionals are trying to consolidate security data from diverse sources and normalize the data to a common standard in a scalable way. They need a simple way to get the best insights to monitor, detect, and respond to threats and vulnerabilities. Meanwhile, data is growing at 28% CAGR, and rarely in the 'correct' or same format. Many times that data is locked in proprietary formats and tooling, with teams struggling to get the insights from the data they have. Security teams must be able to quickly and cost-effectively analyze relevant data across multiple tools, technologies, and vendors.

The solution.

Cribl's suite of products empowers enterprises using Amazon Security Lake to handle surging security data volumes by simplifying their data management. But, how? By making it easy to ingest third-party data, transform data into Open Cybersecurity Schema Framework (OCSF) format, replay data as needed, and search data at rest. Customers can use Cribl Stream to ingest data from any cloud, on-premises, and custom sources. Then, with Cribl Packs convert it to OCSF format and send it to a customer-owned, purpose-built data lake that centralizes the data, making it more useful while cutting down storage costs. Since OCSF is an open standard that can be adopted in any environment, application, or solution provider, it fits right in with your existing security standards and processes. Plus, Cribl Search allows users to search and explore data at rest and selectively target events to send right to a SIEM or other system of analysis. This way, security analysts can quickly normalize data, effectively respond to threats, and use the datasets from their Security Lake environment to their full potential.

ABOUT AMAZON SECURITY LAKE

Amazon Security Lake automatically centralizes security data from AWS environments, SaaS providers, on-premises environments, and cloud sources into a purpose-built data lake stored in the customer's account. With Security Lake, you can get a more complete understanding of your security data across your entire organization. Security Lake has adopted the Open Cybersecurity Schema Framework (OCSF), an open standard. With OCSF support, the service normalizes and combines security data from AWS and a broad range of enterprise security data sources.



The benefits.

Route data from third-party sources to Amazon Security Lake.

Accelerate data onboarding from third-party sources with Cribl Stream to gain greater visibility across your security and operating environments while protecting workloads, applications, and data.

Search data in Security Lake at any time.

Increase the scope of analysis by mining data at rest in Security Lake with Cribl Search for quicker searches and deeper insights. If necessary, replay only the critical data to other tools for analysis for later investigations with ad hoc data collection in any tooling schema required.

Transform data to OCSF in the required open schema specifications.

Seamlessly enrich raw data and shape it to Security Lake specifications for Parquet schema with a repeatable process that requires minimal effort for modifications.

Together, Cribl and Amazon Security Lake provide a way for teams to support massive amounts of data and quickly make sense of all the information without breaking the bank.

Customer story.

"Cribl has been instrumental in our transition to Amazon Security Lake, providing us the freedom and flexibility to work with the tooling of our choice as an agnostic data broker. Thanks to Cribl, we're able to streamline data transformation to OCSF and ingestion to Security Lake, and we've gained enhanced data search."

Troy Wilkinson

Chief Information Security Officer, Interpublic Group

The summary.

Bringing together data from on-premises and cloud sources into a purpose-built storage solution is key to protecting the modern enterprise. You simply have to always be improving workload, application, and data security, and increasing visibility for the org. That's easier said than done, though. A large part of the problem is dealing with a huge amount of data. Now imagine all that data coming in from a ton of different sources. This data is often stuck in complex formats that don't work well together, making it hard to see the full picture. Security experts need a straightforward way to quickly make sense of all this information, using various tools and systems without breaking the bank.

Cribl, the Data Engine for IT and Security, gives AWS customers the freedom to pick OCSF-enabled tools and services that meet their needs without having to reformat their data on their own. Teams can collect and analyze data from endpoint, network, application, and cloud sources in a standardized format allowing for quick identification and response to security events. Plus, they can maintain more granular access controls while staying compliant and managing storage costs.

aws PARTNER

- Security software competency
- Data and analytics software competency
- Public Sector
- Amazon Linux ready
- AWS Graviton ready

With Cribl, customers can:

- Route data from third-party sources to Amazon Security Lake
- Transform data to OCSF, making sure it fits the needed open schema requirements
- Search data in Security Lake to speed up investigations

Get started.

- Learn how Cribl can help you with your AWS use case with a custom demo.
- Check out our AWS-validated OCSF post-processing pack in our Cribl Packs Dispensary.
- Get up and running quickly with our Amazon Security Lake destination title.
- Route, process, replay, and search up to 1 TB of data free with Cribl.Cloud on AWS Marketplace today.

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

SB-0026-EN-1-0424