>SOLUTION BRIEF_

Accelerate business productivity, prevent threats, and achieve analytics speed and scale with Cribl and Anomali

THE CHALLENGE

Organizations need a solution to contend with the modern security landscape, and leverage AI to identify weaknesses and take proactive steps to address them.

THE SOLUTION

Cribl's data management pipeline and the Anomali's AI-Powered Security Operations Platform offer a comprehensive view of your environment, enabling organizations to quickly identify and respond to operations and threats.

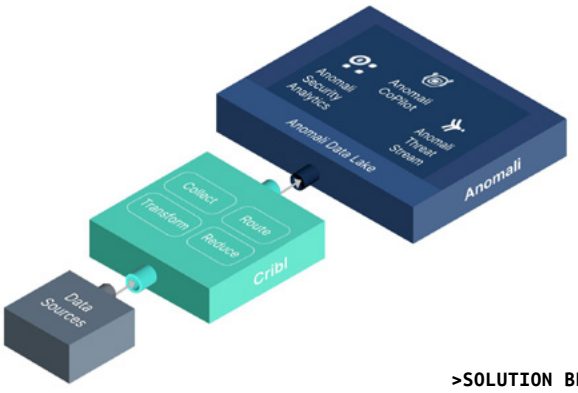
THE BENEFITS

- AI-Powered analyst efficiency
- Maximize security investments
- Increased scale and performance with an integrated platform
- AI-powered threat intelligence for real-time decision making

Together, Cribl and Anomali provide a comprehensive solution for processing machine data (including logs, instrumentation data, application data, security data, and metrics). Discover how the Anomali AI-Powered Security Operations Platform can deliver mind-blowing speed, scale, and performance at a reduced cost.

To protect the environment and stay ahead of every threat, organizations need to process extreme volumes of data from every system across their business and perform correlations that make sense. The challenge grows every year as data volumes increase by orders of magnitude. Organizations need a solution that can contend with the modern security landscape across their business, protect against the latest threats, detect suspicious activity quickly, and leverage a safe and intelligent Anomali Copilot.

By eliminating parsing, indexing, and archiving, the Anomali AI-Powered Security Operations Platform enables organizations to search petabytes of data in seconds to detect and respond to threats before they cause damage. Anomali Security Data Lake eliminates the need for another big data engine, significantly reducing operating costs. As a result, the Anomali AI-Powered Security Operations Platform, in conjunction with the Cribl data pipeline, enables complete visibility, detection, investigation, response, and remediation in a fraction of the time of other tools.



> "By eliminating parsing, indexing, and archiving, the Anomali AI-Powered Security Operations Platform enables organizations to search petabytes of data in seconds to detect and respond to threats before they cause infrastructure, economic, and reputational damage. In conjunction with Cribl's data management pipeline, customers achieve complete visibility, detection, investigation, response, and remediation at a fraction of the time and cost of other solutions."

Why Cribl and Anomali?

Relevant intelligence analysis

Before sending raw security data to Anomali, Cribl can enrich it with additional context to make it more useful. In doing so, Anomali can better correlate and analyze threats, resulting in more accurate detections. Anomali receives only high-quality, relevant intelligence data from Cribl, increasing its accuracy and efficiency in defending the environment.

Optimized security data flow

Cribl's ability to route specific data types to targeted destinations ensures that Anomali will only receive the security data it needs. With Cribl, data can be transformed into a format best suited to Anomali, ensuring seamless integration and better application of Anomali's capabilities. This reduces unnecessary processing, making it an ultra-performing AI-powered security operations platform.

The fastest path to incident response

Cribl's real-time data collection and processing allow Anomali to receive relevant, up-to-date information – crucial for timely and effective incident response. Anomali can provide better context for incident investigation, allowing for more informed and faster decisions during the investigation process.

Centralized security data management

Cribl delivers comprehensive control over multiple security data sources, simplifying data pipeline management and ensuring consistent and reliable data flow to Anomali. Cribl's flexible data routing and transformation capabilities make integrating diverse data sources easier and more efficient, enhancing Anomali's ability to analyze and respond to threats.

Summary

When the Cribl data management pipeline is integrated with Anomali, it creates a powerful AI-powered security operations platform suited to every organization seeking modern defense capabilities. Cribl's solution provides a superior foundation to ingest and process large amounts of data, allowing Anomali to detect threats and suspicious activity more efficiently, in real-time. With Cribl and Anomali organizations are able to quickly identify and mitigate potential threats, doubling the value of their security data.

Get started with Anomali and Cribl today at www.anomali.com

ABOUT ANOMALI

Anomali is an AI-Powered Security Operations Platform that is modernizing security operations with the omnipresent, intelligent, and multilingual Anomali Copilot that provides first-in-market speed, scale, and performance at reduced costs.

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, and Cribl Search, the industry's first search-in-place solution. 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-0032-EN-1-0224