>SOLUTION BRIEF_

Cribl for Managed Security Services.

DATA MANAGEMENT NEEDS FOR MANAGED SECURITY SERVICES

- Managed security service providers (MSSPs) set up security operations centers (SOCs) for multiple enterprises.
- Each enterprise may configure tools differently and have data in varying formats. Onboarding new data sources, customers, and tenants can be a real pain for MSSPs.
- A unified data processing engine helps MSSPs spend less time managing tools and data, and more time detecting, analyzing, and remediating issues to better protect customers.

The challenge.

Managed security service providers (MSSPs) are an enterprise security team's best friend, often tasked with setting up a security operations center (SOC) or optimizing an existing SOC. Because security data comes in many different formats, it can be a challenge to onboard new sources or tenants, enrich the data with vital context, ensure it lands in the right tools ,and easily access it when you need it. There's no one-size-fits-all approach. MSSPs work with multiple enterprises at once, and those enterprises all configure tools differently. For every new customer that comes onboard, a single provider may have to reinvent the wheel several times, writing custom code and parsers just to get data in.

The solution.

Managed security service providers need a vendor-agnostic IT and Security solution that streamlines data onboarding and routing, enables enrichment of security events, and delivers better security outcomes for their customers. A unified data processing engine gives MSSPs flexibility and repeatability — exactly what they need to help enterprise SOCs and security teams. Having a data engine in place will also ensure compliance with the latest industry standards and regulations. With better data management, healthcare organizations can confidently chart a path forward towards quick and useful insights, faster threat detection, and significant cost savings.

Cribl Stream™

A vendor-neutral collection, reduction, enrichment, and routing system for IT and security data.

Cribl Edge™

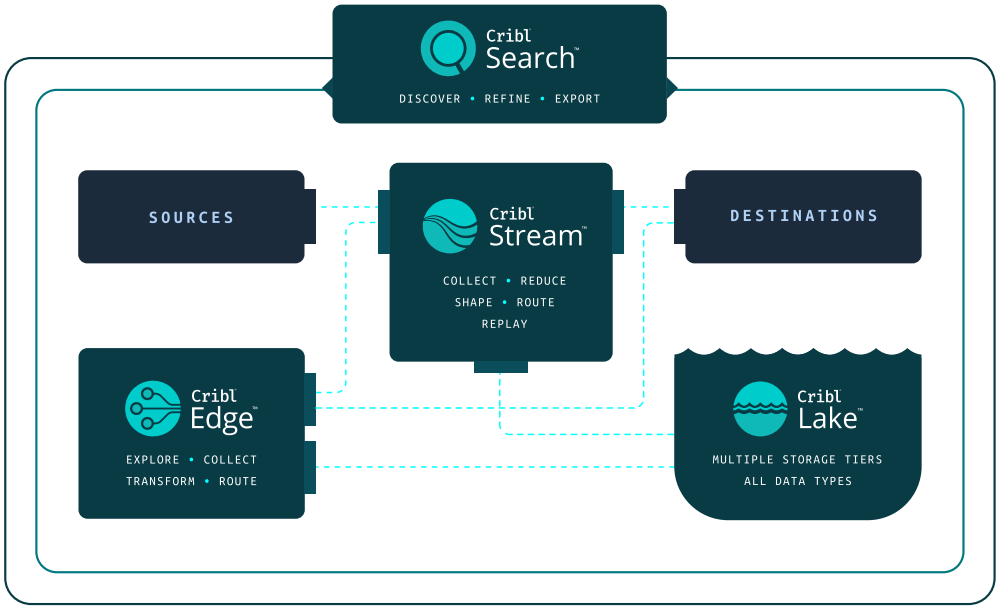
An intelligent, scalable, edge-based data collection system for logs, metrics, and application data.

Cribl Search™

Perform federated “search-in-place” queries on any data, in any form.

Cribl Lake™

A simplified data lake solution to easily store, manage, and access data.



Use cases:

Enable supercharged security insights for faster TDIR.

When managed security service providers use Cribl, their customers gain the ability to normalize and enrich events in flight with valuable context for greater accuracy and faster threat detection, investigation, and response.

Onboard new customers with ease.

Get security data from any source to multiple destinations, streamlining log ingestion and data onboarding for each new customer or tenant. Use Cribl Packs to apply the same logic across multiple customers.

Make the most of existing security investments.

Once MSSPs set up the SOC, Cribl’s top-tier collection, routing, processing, search, and storage capabilities enable each customer to make the most of low-cost storage and maximize security tooling.

Cribl for Managed Security Services.

The Cribl suite of products is the best way for MSSPs to implement a unified data engine, enabling them to meet evolving data management complexities and requirements — for multiple customers and tenants. Cribl Packs add the ability to build and reuse data pipelines securely across different SOCs, so MSSPs can bring on new clients fast. With Cribl, managed security service providers can effectively collect and route data, onboard new sources, and reduce risk without sacrificing customer experience.

BlueVoyant

"Stream allows us to offer our customers significantly more insight into the cybersecurity implications of their data, well beyond compliance. Our clients are getting substantially greater security value out of the data they have, with our use of Cribl's technology."

Chris White,
Chief Security Officer

Capabilities:

- Route data from any source to any destination for quick GDI.
- Normalize data formats in flight, regardless of tooling.
- Enrich telemetry data for a quicker response to cyber attacks.
- Encrypt, mask, and control access to PII.
- Maintain full-fidelity data in inexpensive object storage. Replay it at any time for future analysis.
- Build and reuse data pipelines with Cribl Packs.
- Search data in place to explore and discover data where it lives.
- Store and easily access data in open formats.
- Store data from various sources such as electronic health records, medical imaging, clinical trials, wearable devices, and more, in a single, scalable repository.

Benefits:

- Spend less time managing tools and onboarding data
- Increase accuracy and context of telemetry data in customer SIEMs and analytics systems
- Protect sensitive customer data across many customer and tenants
- Maximize existing customer investments in their security tooling
- Increase data visibility and boost signal to noise ratio for faster threat response
- Bring on new customers fast by leveraging proven workflow.

Cribl helps MSSPs scale operations, spend less time managing tools and data, and more time detecting, analyzing, and remediating issues to better protect customers.

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-0038-EN-1-0524