INDUSTRY SOLUTION BRIEF

Cribl LogStream™

for Managed Security Services
INDUSTRY SOLUTION BRIEF

Cribl LogStream™ for Managed Security Services

Managed security service providers need a vendor-agnostic observability tool that centralizes their customers’ growing amounts of data and continues to prioritize cybersecurity, with a focus on pure threat detection and response.

Changes Across the Industry

Data volumes are growing year over year in nearly every industry, and organizations supplying managed security services often feel these effects many times over. Because managed security service providers (MSSPs) offer outsourced monitoring and management of security systems, these providers may be working with data from a myriad of companies daily. Those companies could span several industries and be using a variety of tools. The COVID-19 pandemic has also had an outsized impact on MSSPs. Intrusion detection and prevention was always top of mind for MSSPs; however, the pandemic has led to a wave of new methods designed to defraud and attack, making cybersecurity even more of a concern. Managed security service buyers are feeling the pressure too, demonstrated by an increased focus on pure threat detection and response, versus other services MSSPs may provide.

MSSPs not only need a way to manage increasing data volumes across a large quantity of industries and companies, but they’ll also require methods to support their customers’ various tooling. Concurrently, they will need ways to better detect threats and streamline the subsequent response.

That structure must also include:

- Security throughout each customer’s environment
- Compliance with relevant industry standards and regulations
- Ability to effectively manage, encrypt, and secure each customer’s data
- Support for multiple source protocols
- Support for both cloud and local instances across customers
- Support for many destinations while having flexibility to onboard new ones
- Centralized management system that streamlines both detection, reporting, and response
Many managed service providers are looking to Cribl LogStream to support their customers regardless of tooling and streamline threat detection and response overall. Enterprises supported by MSSPs typically work with data that exists in multiple sources with different source protocols. They often have data coming in a variety of formats, and those formats may not always match the formats required by the tools they are using. The managed security service providers themselves also have to ensure compliance with the latest industry standards and regulations for each customer organization. With Cribl LogStream, MSSPs can support the continued onboarding of new buyer data sources regardless of format and get necessary insights from that data, all while saving time on threat detection and response.

An Observability Solution That Meets the Needs of MSSPs

Cribl LogStream is the best way for managed security service providers to implement an observability pipeline, enabling them to parse, restructure, and enrich data in flight – before paying to analyze it. LogStream helps these organizations slash data management costs, improve performance, and effectively route data in the formats their customers require.

With Cribl LogStream, MSSPs can now:

• Reshape, reduce, or route data from any source to any destination
• Stay compliant with the latest relevant standards and regulations, regardless of industry
• Get further visibility into data, including valuable customer insights for threat detection and response
• Control data management costs along the way

Cribl LogStream is the best way for MSSPs to implement an observability pipeline, enabling them to parse, restructure, and enrich data in flight – before paying to analyze it.
A Closer Look: Cribl LogStream™ for Managed Security Services

ROUTE DATA FROM ANY SOURCE TO ANY DESTINATION
With Cribl LogStream, managed security service providers can send data to the most effective destinations, including low-cost storage locations like S3 for long-term retention and compliance with relevant industry standards and regulations. MSSPs can quickly route data to the best tool for the job – or all the tools for the job – by translating and formatting data into the tooling schemas each customer requires.

ONBOARD ANY CUSTOMER WITH EASE
Because LogStream is a universal receiver and router, managed security providers can smoothly and securely migrate data from customers' in-house environments to the MSSP's own systems. Cribl LogStream enables MSSPs to onboard any new client quickly and easily – without worrying about dropping or losing valuable customer data.

CENTRALIZE DATA MANAGEMENT AND MONITORING
Logtream's robust and easy-to-use GUI-based configuration and testing interface reduces management overhead, making it easier to support multiple customers. MSSPs can quickly capture live data and monitor each buyer's observability pipeline in real time, giving providers further visibility into the data.

STREAMLINE THREAT DETECTION AND RESPONSE
Cribl LogStream allows managed security service providers to park full-fidelity data in low-cost storage according to each customer's unique retention policies and industry standards. When a threat is detected, MSSPs can use LogStream to efficiently collect data from object storage and replay that security data to any SIEM or UEBA system. They can put customers at ease by quickly diagnosing and resolving existing intrusions and potential cyber threats. LogStream provides MSSPs – and their customers – with an affordable way to retain more data for longer periods of time, while still making that data easily accessible for investigations.

Industry Early Adopter: BlueVoyant®

BlueVoyant is a cybersecurity service provider specializing in advanced technologies that support world-class offerings designed to protect organizations from today's agile attackers. Their team processes and cross-correlates a staggering amount of data from hundreds of different sources with Cribl LogStream – all in the aim of protecting their customers.

BlueVoyant leverages several of LogStream's features, including smart routing, data masking, and real-time detection at the edge — all manageable from a central console — when designing the architecture of their custom data processing pipeline for their managed security service offering.

“The Cribl team understands our business requirements; it's a great design partnership. They understand how a given change will impact us — how to scale it out effectively and safely for our hundreds of clients,” says Chris White, BlueVoyant's Chief Security Officer.
Summary

The managed security services industry is facing massive disruption due to a number of factors, including:

- *Increasing data volumes, amplified by the volume of customers each MSSP supports*
- *Greater concern for cybersecurity, accelerated by the COVID-19 pandemic*
- *A shift in buyer focus to pure threat detection and response, versus other services MSSPs may offer*

Managed security service providers must consider these changes when selecting an observability solution. Cribl Logstream is an observability solution that meets the needs of MSSPs, enabling them to route, reduce, or reshape data so that they and their customers remain compliant and get the insights needed in the most cost-effective way possible.

LogStream gives MSSPs the power to make choices that best serve their unique needs without limiting the vendors they can support, sacrificing customer data security, or breaking the bank.

As these organizations’ goals continue to evolve, they will have the freedom to work with new tools and destinations, perform more comprehensive investigations, and onboard new sources of data for their buyers.

Cribl LogStream™ helps MSSPs — and their customers — get the data they want, in the formats they need, to wherever they want it to go.

ABOUT CRIBL

Cribl is a company built to solve customer data challenges and enable customer choice. Our solutions deliver innovative and customizable controls to route security and machine data where it has the most value. We call this an observability pipeline, and it helps slash costs, improve performance, and get the right data, to the right destinations, in the right formats, at the right time. Join the dozens of early adopters, including market leaders such as TransUnion and Autodesk, to take control and shape your data. Founded in 2017, Cribl is headquartered in San Francisco, CA. For more information, visit [www.cribl.io](http://www.cribl.io) or our [LinkedIn](https), [Twitter](https), or [Slack](https) community.