>SOLUTION BRIEF_

Optimize your SOC with Microsoft and Cribl

THE CHALLENGE

Security teams struggle to manage surging data with disparate tools, leading to visibility gaps and security vulnerabilities that threaten operational integrity.

THE SOLUTION

Cribl and Microsoft work together to help teams gain control of their data, regardless of where it resides or what format it takes, streamlining SOC workflows. Collect, transform, route, and search data from diverse sources to Microsoft Sentinel and Azure Data Explorer in required formats.

THE BENEFITS

- Simplify data onboarding at scale
- Accelerate SOC optimization and workload migrations
- Optimize threat detection and costs
- Easily explore your data in place

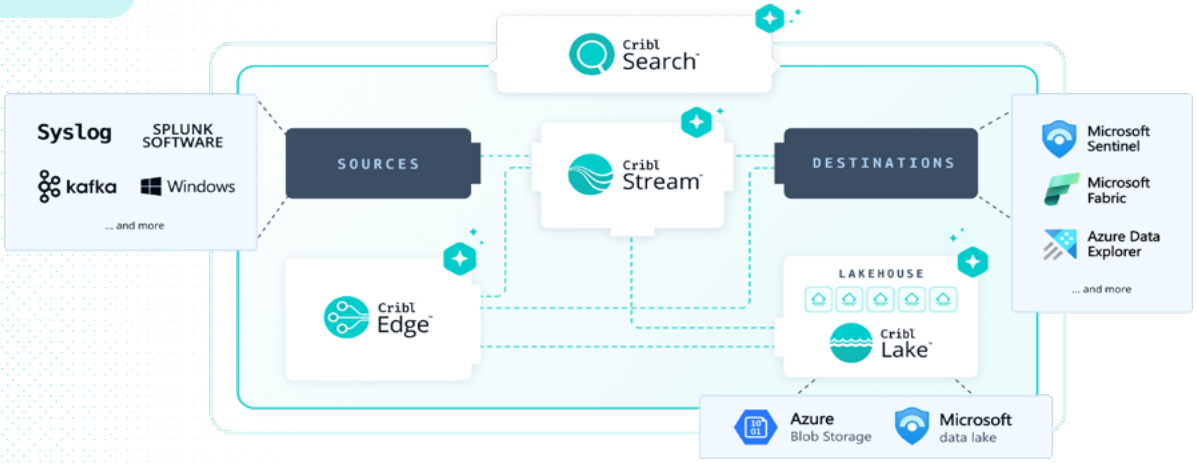
Turn fragmented telemetry into an effective security workflow by structuring security data before it enters Microsoft Sentinel, Microsoft Fabric Real-Time Intelligence, or Azure Data Explorer. With flexible routing and search in place, teams can move faster, reduce noise and costs, and modernize security operations without sacrificing visibility or control.

The challenge

As organizations manage surging data volumes across complex ecosystems, balancing budgets and visibility is difficult. Reliance on fragmented tools creates operational gaps that increase configuration risks, weaken security posture, and hinder AI-assisted detection. Teams struggle to maintain operational integrity and compliance, leaving environments exposed to security vulnerabilities and costly failures.

The solution

Cribl and Microsoft work together to help teams gain control of their data, regardless of where it resides or what format it takes, streamlining Security Operations Center (SOC) workflows. Cribl provides the essential plumbing that connects legacy systems to modern cloud architectures. Cribl Edge collects telemetry data directly from any source at the host, while Cribl Stream can also collect, shape, and route data to Microsoft Sentinel, Microsoft Fabric Real-Time Intelligence, or Azure Data Explorer in required formats, including CommonSecurityLog and WindowsEvents. Cribl Search lets teams quickly search their data in place, without centralizing it first. By bridging the gap between complex data sources and powerful analysis tools, Cribl and Microsoft enable organizations to scale their data strategy without limits.



CUSTOMER STORY:

"Cribl has significantly improved our data management, making operations smoother. As a small team with extensive responsibilities, Cribl has been an invaluable asset."

— Richard McIver,
Senior Security Engineer at the University of Pittsburgh

Read the case study ›

The benefits of using Cribl with Microsoft Sentinel and Azure Data Explorer:

Simplify data onboarding at scale

Rapidly onboard third-party data into your Microsoft environment and enrich security decision-making with additional context. Deliver data in the right format for Microsoft Sentinel, Microsoft Fabric Real-Time Intelligence, or Azure Data Explorer without complex reconfigurations, enabling faster analysis and response with AI-powered efficiency and human-in-the-loop verified accuracy.

Accelerate SOC optimization and workload migrations

Transform and selectively route data from legacy systems to your Microsoft environment, ensuring data parity without compromising security or integrity. Plus, simplify multi-cloud integrations into Azure Data Explorer and Sentinel for enhanced visibility, cost-effectiveness, and a more flexible analytics framework.

Optimize threat detection and costs with flexible data routing

Route enriched, high-value data to Sentinel, Azure Data Explorer, or Microsoft Fabric Real-Time Intelligence, and archival data to Azure Blob Storage to maximize detection efficiency and optimize costs. Offloading retention data to lower-cost storage ensures compliance and historical data is accessible, while keeping detection, analysis, and visualization systems focused on immediate threats.

Easily explore your data in place

Search data directly at its source, rest in object storage, or flows from API endpoints with Cribl Search. Forward only actionable data to your systems of analysis, like Sentinel, for further investigation, reducing data movement and bridging machine telemetry with human context to deliver faster insights.

Summary

Fragmented tools and disconnected legacy systems frequently create dangerous blind spots that compromise your security posture. By bridging these disparate sources with Cribl's intelligent routing and Microsoft's powerful analytics, organizations can ensure every piece of telemetry is formatted and sent exactly where it delivers the most value. Teams gain the freedom to modernize their security operations without fear of data loss, moving from reactive firefighting to proactive, data-driven operations.

To get started with Microsoft Azure and Cribl, visit Azure Marketplace for a free trial today! The Cribl Slack Community is also a great place to connect with leaders from other teams leveraging both Microsoft Azure and Cribl.

ABOUT CRIBL

Cribl, the Data Engine for IT and Security, empowers organizations to transform their data strategy. Powered by a data processing engine purpose-built for IT and Security, Cribl's product suite is a vendor-agnostic data management solution capable of collecting data from any source, processing billions of events per second, automatically routing data for optimized storage, and analyzing any data, at any time, in any location. With Cribl, IT and Security teams have the choice, control, and flexibility required to adapt to their ever-changing data needs. Cribl's offerings — Stream, Edge, Search, and Lake — are available either as discrete products or as a holistic solution.

Learn more: www.cribl.io | Try now: Cribl sandboxes | Join us: Slack community | Follow us: LinkedIn and X (Twitter)

SB-0012-EN-5-0226