>SOLUTION BRIEF_

Augment your SIEM with Microsoft Sentinel, Azure Data Explorer, and Cribl

THE CHALLENGE

Growing data volumes, fragmented tools, and extended retention requirements strain budgets, weaken security, and increase compliance and operational risks across cloud environments.

THE SOLUTION

Cribl and Microsoft work together to help teams gain control of their data, no matter where it resides or what format it takes. Collect, transform, and route data from legacy systems and third-party sources directly into Microsoft Sentinel and Azure Data Explorer in required formats.

THE BENEFITS

- Enhanced management and visibility.
- Improved security posture.
- Streamlined data ingestion and transformation.
- Optimized security operations.
- Cross-cloud consolidation.

Seamlessly collect, transform, and route data security from legacy systems and third-party sources into Microsoft Sentinel and Azure Data Explorer without complex configurations.

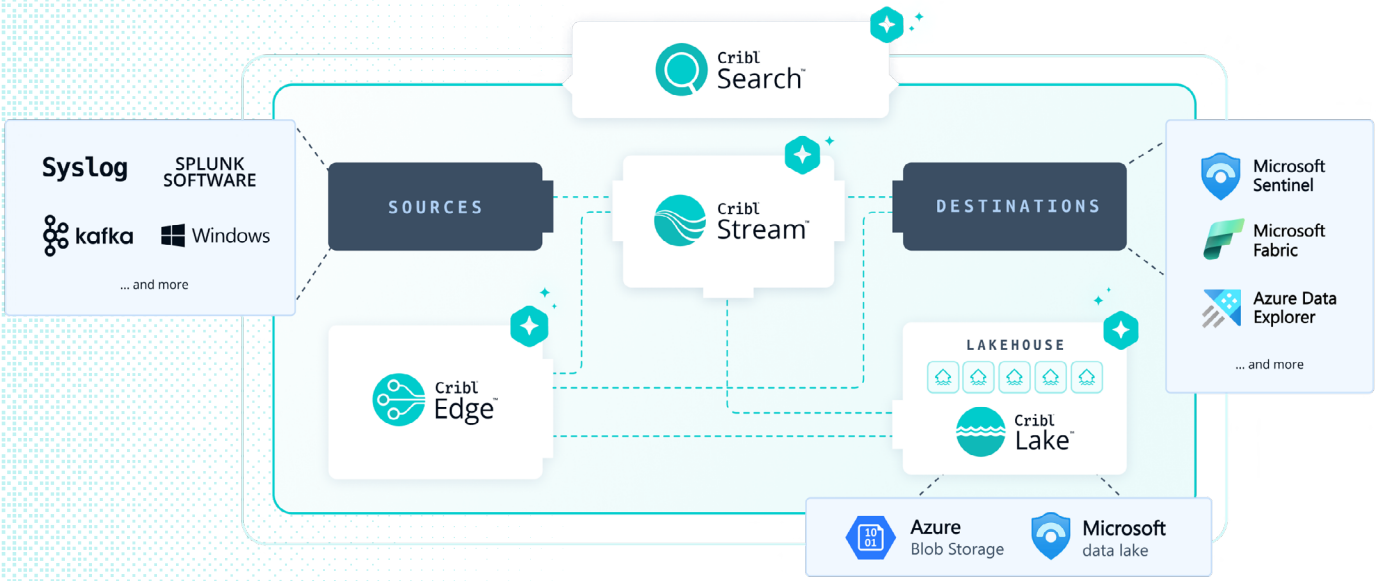
The challenge

Organizations are struggling to balance budgets, flexibility, and data visibility as they manage growing data volumes across complex systems and applications. Fragmented tools, inconsistent visibility, and a lack of end-to-end integration across Microsoft and third-party stacks increase configuration risks, weaken security posture, hinder AI-assisted detection, and complicate compliance across distributed environments. At the same time, teams are trying to minimize disruptions, maintain operational integrity and security posture, and meet stringent compliance requirements. Without effective solutions, organizations risk security vulnerabilities, compliance failures, and operational disruptions in their cloud environments.

The solution

Cribl and Microsoft work together to help teams gain control of their data, no matter where it resides or what format it takes. By collecting, transforming, and routing data from legacy systems and third-party sources directly into Microsoft Sentinel and Azure Data Explorer in required formats like CommonSecurityLog and WindowsEvents. Organizations can modernize their security infrastructure without complex configurations, streamlining cross-cloud consolidation and enhancing AI-powered threat detection and response.

Acting as the essential plumbing between legacy systems and modern cloud architectures, Cribl bridges the gap to a more agile, digitally transformed security environment. Teams can selectively route data based on its value—sending high-value data to Sentinel for real-time analysis and directing lower-value data to cost-efficient storage such as Azure Blob Storage. This approach supports compliance, optimizes costs, and preserves access to full-fidelity data, giving organizations the flexibility to manage data strategically, strengthen detection capabilities, and improve overall security posture.



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:

Accelerate SIEM migrations

Transform and selectively route data from legacy SIEM platforms to Microsoft Sentinel, streamlining the transition while maintaining operational parity, without requiring licensing changes or new agents.

Simplify data onboarding at scale

Rapidly onboard third-party data into Sentinel, transform it into the required format, and enrich it with additional context for a complete story without complex reconfigurations.

Optimize threat detection and resources with flexible data routing

Send enriched, high-value data to Sentinel for real-time threat detection while routing low-value datasets to Sentinel data lake, Azure Blob Storage, or other cost-effective storage. Maintain a full-fidelity copy for historical analysis if needed, without overburdening active detection systems, ensuring security teams focus on the most relevant and actionable information.

Improve security posture with efficient analysis

Avoid SIEM downtime or outages and meet compliance requirements by eliminating duplicative data. Replay historical data to Sentinel as needed for threat hunting and investigations.

Cross-cloud consolidation

Simplify data integrations from multiple clouds into ADX and Sentinel with Cribl. A smoother migration into security data warehouses gives enhanced visibility, cost-effectiveness, and a more flexible data analytics framework.

USE CASES

Vendor-neutral routing

- Onboard and route data from any on-premises, cloud platforms, or open-source tools to Microsoft Azure with the flexibility to move that data wherever it needs to go in the future.

SIEM augmentation

- Enhance threat detection and incident response by routing specific data to dedicated tools and workflows including Microsoft Sentinel.

Storage and compliance

- Fork a copy of your data to ADX to meet compliance requirements, with the ability to replay data ad hoc to any destination.

Summary

Organizations are under constant pressure to manage expanding data volumes, stay compliant, and protect against evolving threats while working within tight budgets. Cribl enhances Microsoft Sentinel with a flexible data pipeline that simplifies the migration and integration of diverse security data sources. With Cribl Stream, you can ingest, transform, and route data into Sentinel's required formats. By selectively routing data based on its value, teams can send high-impact workloads for real-time analysis, while storing lower-value data in accessible, cost-efficient storage. Cribl serves as the essential infrastructure that bridges the gap between legacy systems and modernized, digitally transformed organizations.

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-4-1125