Cribl

_INDUSTRY SOLUTION BRIEF

Cribl for the Defense Information Systems Agency: Streamlining Data Management and Operations

THE CHALLENGE

DISA faces challenges in data volume, transformation, migration, routing, and scaling to achieve efficient, secure, and compliant data management.

THE SOLUTION

Cribl streamlines data management by enhancing visibility, security, and compliance while controlling costs through efficient data routing and normalization, making it the ideal solution for DISA's data management challenges.

THE BENEFITS

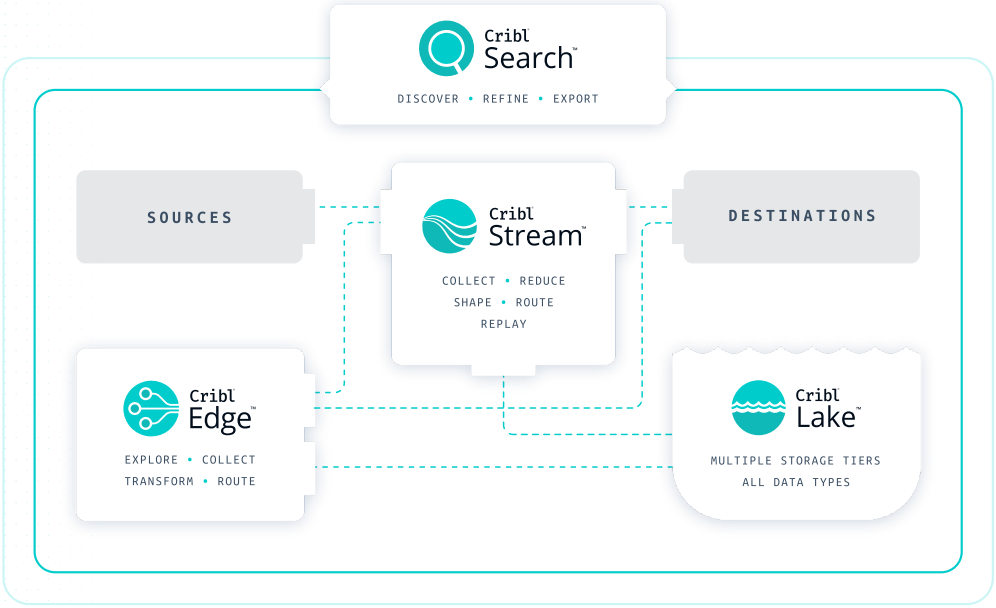
- Shape data in flight prior to indexing
- Efficiently migrate DISA workloads to the cloud
- Share data seamlessly in multi-cloud environments
- Route OCONUS data with precision
- Simplify PCAP metadata management for investigations
- Effortlessly capture and route Windows Events to any SIEM

The challenge.

The Defense Information Systems Agency (DISA) faces significant challenges in managing its complex data ecosystem. These include handling massive data volumes from distributed sources, difficulties in data transformation and cloud migration, high costs in multi-cloud environments, special routing needs for data originating outside of the United States (OCONUS), expensive packet capture (PCAP) metadata collection, and scaling issues with Windows Event Collectors. Addressing these challenges is crucial for DISA to achieve efficient, secure, and compliant data management across its operations. Overcoming these challenges is critical for DISA to achieve efficient, secure, and compliant data management.

The Cribl solution.

Cribl, the Data Engine for IT and Security, streamlines data management by empowering you to efficiently route, shape, restructure, and enrich data from any source to any destination without requiring new agents. This allows you to enhance visibility, security, and compliance while controlling costs by eliminating noise and retaining valuable data for longer periods, optimizing existing infrastructure and tooling investments. Customers can route a full-fidelity copy of raw data to cost-effective storage for long-term retention, ensuring compliance and audit readiness. Need that data analyzed for an investigation or recalled for an audit? Replay the data to any analytics tools, facilitating the insights needed to remediate incidents and support compliance. With its robust routing and processing capabilities, Cribl is uniquely positioned to effectively address the data management challenges faced by DISA and streamline operations.



CRIBL FACILITATES PROPER ROUTING OF DATA ORIGINATING OCONUS BY ALLOWING TEAMS TO LOCALLY TAG IT AT ITS SOURCE BASED ON LOCATION, DATA TYPE, OR OWNERSHIP GROUP.

Use cases.

Shape data in flight prior to indexing

Easily integrate with existing Kafka brokers, including those from Confluent. Once the data is ingested, administrators can create pipelines effortlessly using Cribl's low-code solutions. This allows them to efficiently normalize, transform, optimize, enrich, and route data to multiple destinations simultaneously.

Streamline migration of DISA workloads to the cloud

Route data from on-premises systems to the cloud, and perform data normalization in flight to ensure that data is in the correct format as soon as it reaches the cloud. Keep visibility and parity intact as workloads move to the cloud.

Share data seamlessly in multi-cloud environments

Share data across cloud tenants without breaking the bank. With Cribl Stream's powerful 8:1 data compression, you can drastically reduce multi-cloud egress costs while maintaining performance. Beyond cost savings, Cribl's flexible processing unlocks even more value—letting teams optimize logs and data flows with ease.

Route OCONUS data with precision

Tag data that originates outside the continental United States (OCONUS) based on its location, type, or ownership group, and classify this as a metadata event to facilitate informed routing decisions. Ensure that data with specific tags remains local, while other data is sent to your SIEM.

Simplify PCAP metadata management for investigations

Route high-volume PCAP metadata to cost-effective object storage to preserve fidelity. When investigations arise, replay relevant data from storage to your SIEM for enhanced scalability.

Effortlessly capture and route Windows events

Capturing and routing Windows events no longer requires complex configurations or extensive policies. With scalable event collection and direct integration with existing tools like Splunk Universal Forwarders, data can be seamlessly optimized and routed to destinations like Splunk, Elastic, or Microsoft Sentinel—all while simplifying deployment and management.

CRIBL PROVIDES THE FLEXIBILITY TO ROUTE DATA TO THE MOST SUITABLE TOOLS FOR SECURITY AND OPERATIONAL MONITORING, GIVING YOU A CLEARER PICTURE OF YOUR ENVIRONMENT AND EFFECTIVELY STREAMLINING OPERATIONS.

Get started today.

Cribl empowers DISA to overcome its most pressing data management challenges by delivering a flexible, scalable, and cost-effective solution. By enabling seamless data routing, transformation, and enrichment across distributed and multi-cloud environments, Cribl optimizes operations while ensuring compliance and security. Whether simplifying Windows event collection, reducing multi-cloud egress costs, or streamlining PCAP metadata management, Cribl helps DISA unlock the full potential of its data ecosystem. With Cribl, DISA can confidently modernize its data infrastructure, drive operational efficiency, and maintain mission-critical visibility and control across all environments.

With Cribl, DISA organizations can:

- Shape data in flight prior to indexing
- Streamline migration of workloads to the cloud
- Share data seamlessly in multi-cloud environments
- Appropriately route data originating outside of the continental United States
- Simplify PCAP metadata management for investigations
- Capture Windows Events with ease and route them to any SIEM

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-0002-EN-3-0125