>SOLUTION BRIEF_

Cribl for DoD: Enhancing Data Visibility for the Warfighter

THE CHALLENGE

The Department of Defense components have been tasked with developing a measurable Data Strategy Implementation Plan with the focus of data as a strategic asset to national security.

THE SOLUTION

With Cribl Stream, you'll achieve complete control of all observability data across the enterprise — on-prem, cloud, disconnected networks — empowering you to optimize cyber awareness and accelerate response.

THE BENEFITS

- Collect, transform and share data by utilizing an observability pipeline
- Data access & availability across the enterprise by routing any data to any system of analysis
- Achieve your mission throughout the entire data lifecycle with this tactical tool
- Accelerate the onboarding of new data sources to meet rapidly changing mission objectives

When federal agencies integrate Cribl Stream into their environment, they can quickly and securely optimize and share their mission critical data across the enterprise

The DoD has established seven goals to become a data-centric enterprise. These seven goals focus on making data; visible, accessible, understandable, linked, trustworthy, interoperable, and secure. It's an exciting goal to modernize the way the DoD develops and deploys secure capabilities to a modern workforce. Improving data management and data driven systems give the DoD a competitive advantage and provides the workforce with exciting ways to promote a culture of data awareness. Leveraging data at speed and scale enables operational advantages and increased efficiency.

Achieve Best In Class Data Observability and Sharing Capabilities

With Cribl Stream, the DoD can focus on making data-centric decisions and achieving the seven VAULTIS goals to transform components and the enterprise. Cribl Stream processes data in flight — meaning components can preview and transform data and then transforms it with Stream's built in pipelines and functions to remove extraneous fields, null values, mask sensitive/PII fields, and eliminate duplicate events. Previewing and transforming data ensures that data management personnel can locate the necessary data and that all data is recognized and impactful to the mission. Cribl Stream offers the ability to replay data from S3 and other object storage solutions to make all data retrievable and provide a full fidelity copy that's available in a cost effective manner.

OMB-issued memorandum M-21-31 details a maturity model for event log management. With Cribl Stream, a streamlined approach to advanced maturity is finally within reach for federal agencies.

VAULTIS DATA GOALS	HOW CRIBL STREAM CAN HELP YOU ACHIEVE THESE GOALS
VISIBLE	Robust preview and monitoring capabilities to accelerate onboarding of new data sources.
ACCESSIBLE	Route data to any destination, and ensure that data is available to all authorized parties, including other components and agencies.
UNDERSTANDABLE	Format data into a common schema and enrich it with semantic metadata for top-tier data optimization.
LINKED	Perform lookups to ensure unique identifiers are present within each data source.
TRUSTWORTHY	Tag data and route a full-fidelity copy to long-term storage in compliance with DoD standards.
INTEROPERABLE	Normalize key-value pairs and timestamps to standard compliant format and transform data to open standards on its way to downstream systems.
SECURE	Role-based access control (RBAC) capabilities and secure/encrypt data in flight.

Effectively Address the Requirements of M-21-31

The Biden Administration's Executive Order (EO) 14028: Improving the Nation's Cybersecurity emphasizes cybersecurity as a national priority and mandates each federal agency to adapt to today's continuously changing threat environment. EO 14028 directs federal agencies to take decisive action to improve cybersecurity investigative and remediation capabilities. Effective policies around logging, retention, and management are essential for improving these capabilities, and OMB-issued memorandum M-21-31 details a maturity model for event log management. With Cribl Stream, a streamlined approach to advanced maturity is finally within reach for federal agencies. These mandates provide direction for Federal agencies to reach basic logging maturity by August 2022, and achieve the highest maturity level by August 2023. Cribl Stream supports the most critical elements of each maturity level by augmenting your current logging environment.

STREAM SUPPORT ACROSS MATURITY LEVELS		
EL1	**EL2**	**EL3**
• Basic Logging Categories • Minimum Logging Data • Time Standards • Event Forwarding • Protecting & Validating Log Info • CISA & FBI Access Requirement • Basic Centralized Access	• Intermediate Logging Categories • Inspection of Encrypted Data • Intermediate Centralized Access	• Advanced Logging Categories • Advanced Centralized Access

Easily Comply with Data Enrichment and Routing Directives

A second memorandum, M-22-01, directs the federal government to adopt a robust endpoint detection and response (EDR) solution to bolster agency's abilities to respond to increasingly sophisticated threat activity on Federal networks. Real-time continuous monitoring and collection of all endpoint data is crucial to those efforts. Cribl Stream is able to perform data enrichment in order to address data attribution issues and help you answer the question, "Who performed this action?" As a universal router and receiver, Cribl Stream can bring in endpoint data from any source, and send it to any destination for consolidation, retention, and archival — making it the perfect tool to help you achieve M-22-01 compliance.

Accelerate Your ZTA Strategy for Network and Data with Respect to M-22-09

Finally, memorandum M-22-09 puts forth a zero trust architecture (ZTA) strategy for all federal agencies. The Zero Trust Model is built on the tenet that no actor, system, network, service operating outside or within the security perimeter is trusted. Data categorization, monitoring sensitive data, and information sharing are additional components of zero trust and critical to national security. Cribl Stream provides out of the box capabilities to address each of these challenges through data enrichment, masking and removing sensitive data, and allowing agencies to format data when sharing across multiple destinations. With an observability pipeline like Cribl Stream in place, federal agencies get a centralized control plane that adheres to the Zero Trust model, so they can securely manage device data and traffic flow.

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-0045-EN-1-0624