SYMMETRY SYSTEMS

Industry Solution Brief

Federal Government

With the largest, most complex, and decentralized networks comprising over 100 agencies, the US Federal government has more data systems than any organization in the world. It accounts for a larger percentage of domestic data breaches each year, in part due to a shortage of skilled cybersecurity professionals and manual efforts prone to delay and errors. In 2021, Thales reported that 47% of federal government respondents experienced a breach in the prior 12 months. Major data breaches, such as the Solarwinds Breach in 2020, surfaced the urgent need for better cyber threat visibility.

Breaches are increasing in number, strength of impact, and attack effectiveness against federal, state and local governments, military organizations, and educational institutions. Traditional network defenses have focused on preventing intrusions, but attackers continue to evade them. Federal government cybersecurity teams need to establish data security practices to protect their data, their most critical asset.

Federal Government Data Security Challenge: Protecting Classified Data

Transition to the Cloud

The move to the cloud continues to compound this challenge. Federal agencies must satisfy the requirement of moving data from unclassified, sensitive, and classified enclaves while ensuring that secure access to sensitive data can be maintained. The Data Center and Cloud Optimization Initiative (DCCOI) sets aggressive targets for IT transformation projects, which also apply to 300,000 Defense Industrial Base organizations assisting the modernization of cybersecurity.

Attack Volume and Velocity

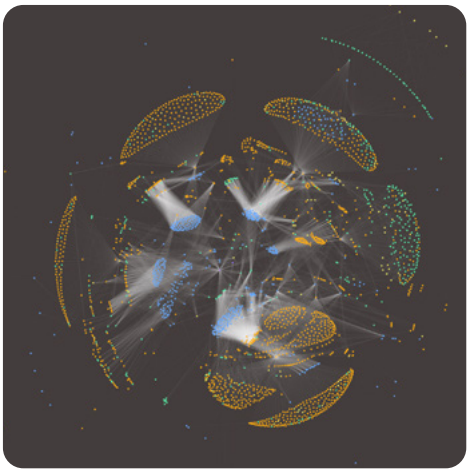
Ransomware attacks have been growing in volume and in effectiveness over the past few years. In 2020, 44% of global ransomware attacks targeted municipalities alone. Over the past 3 years 246 ransomware attacks have been on the U.S. government, costing taxpayers around $51 billion. Ransomware by nature seeks to take control of data and a lot of times organizations aren't able to evaluate if the data is sensitive, protected, or mission critical. In order to properly evaluate the risk or or impact of ransomware attacks, federal government organizations need to classify their data. They also need to have data security measures in place to make sure that ransomware actors cannot move laterally across cloud data stores, picking and choosing the data they consider worth holding for ransom.

Data Security Best Practices with Cloud Adoption

- Execute the Cloud First directive per Federal and DoD Data Strategy while satisfying the regulatory requirements by DCCOI, Cybersecurity Maturity Model Certification (CMMC), FedRAMP, FISMA, CSA STAR, CIS Standards, NIST 800-53, NIST 800-171, etc.
- Fill the growing cybersecurity skill gap with automation and enable security teams to effectively identify and respond to data anomalies.
- Gain better visibility into the security posture of government data spanning across data stores, databases, and data lakes in hybrid cloud environments.

Symmetry Systems DataGuard

DataGuard is a **data security posture management (DSPM)** solution that extends the Zero Trust philosophy to hybrid cloud data stores. Federal government cybersecurity teams use DataGuard to develop a complete understanding of what data they have, where it is located, who has access to it, how it is secured and in what manner it has been used. DataGuard enables businesses with a single source of truth about their data security posture and associated data risks across AWS, GCP, Azure, and on-premise environments – **without having data ever leaving their environment.**



DataGuard produced Environment Graph

The cybersecurity industry is saturated with security solutions that focus on peripheral security and protection within the environment. DataGuard directly addresses data objects and examines the cross-section of identity, data store, and data flow to answer important questions:

- **Where is our sensitive data?**
- **Who has access to it?**
- **What operations have they performed against it?**

With DataGuard, cross-functional teams such as security operations, cloud security, compliance, and identity & access management, can enforce least privilege, sustain regulatory compliance, improve their data security posture, and outpace ever-growing data security risks and threats.

Identify Your Data

Perform agentless scans of all data living across AWS, Azure, GCP and on-premise cloud for a real-time snapshot or historical comparisons. DataGuard enables compliance and cloud migration teams to identify where sensitive data resides without having the data leave their cloud environment. With DataGuard, security teams can easily maintain compliance with challenging industry regulations such as DCCOI, Cybersecurity Maturity Model Certification (CMMC), FedRAMP, FISMA, CSA STAR, CIS Standards, NIST 800-53, NIST 800-171, and others.

Gain Full Visibility

Gain visibility into the entire data landscape with a complete, read-only data security posture map. DataGuard surfaces inactive accounts, dormant data stores, anomalous data flows, and cross-account permissions. It simplifies risk, event detection, incident remediation, and forensics for cloud engineering, security operations teams, and incident response teams.

Detect and Respond

Uncover unsafe data access practices and risky operations detected by DataGuard's built in data firewalls. Alert on violations and potential data breaches to minimize cyber risk exposure. DataGuard provides meaningful, evidence-based insights so that security operations teams can shorten the mean-time-to-recovery (MTTR) while reducing the attack surface for malicious acts, such as ransomware.

Protect Your Data

Deploy least privilege permissions on IAM, cloud accounts, and data store access. Cloud security teams can adopt DataGuard provided data firewall recommendations to tighten access control and minimize blast radius. DataGuard bakes data security into your data ecosystem versus adding peripheral protection.

SYMMETRY SYSTEMS

symmetry-systems.com | hello@symmetry-systems.com

LinkedIn / symmetry-systems-inc

Twitter / @SymmetrySystems