SYMMETRYSYSTEMS

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 accounted for 5.6% of domestic data breaches in 2019*, partly due to a shortage of skilled cybersecurity professionals and manual efforts prone to delay and errors. Major data breaches, such as the Solarwinds Breach in 2020, surfaced the urgent need for better cyber threats visibility.

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.

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), 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.

Hybrid Cloud Security from the Data Out

Symmetry System's DataGuard solution provides a single source of truth of your data security across your hybrid cloud environment. It allows organizations to identify where sensitive data is, who has access to it, and how it's used. With DataGuard, cross-business teams in Security Ops, Cloud Security, Identity, and Compliance can optimize a data security posture and outpace ever-growing data breach risks and threats, all on a single platform.

Gartner
COOL VENDOR 2022™

- The only Gartner Cool Vendor providing solutions for Data Security Posture Management (DSPM)
- Full visibility into all of your data, identities, data consumption, and corresponding data flows across AWS, GCP, Azure, and on-premise environments
- Actionable intelligence and evidence-based recommendations
- Better operational continuity with agentless deployment
- SaaS deployed in your cloud environment — no data, even findings, ever leaves your environment

*Identity Theft Resource Center, ITRC 2019 End-of-Year Data Breach Report

Identify Your Data

Perform an agentless scan of all your data living across AWS, Azure, GCP and on-premise cloud for a real-time snapshot or historical comparisons. DataGuard helps Compliance and Cloud Migration teams identify where sensitive data resides without having your data leave your cloud environment. Maintaining compliance with industry regulations is simplified.

Gain Full Visibility

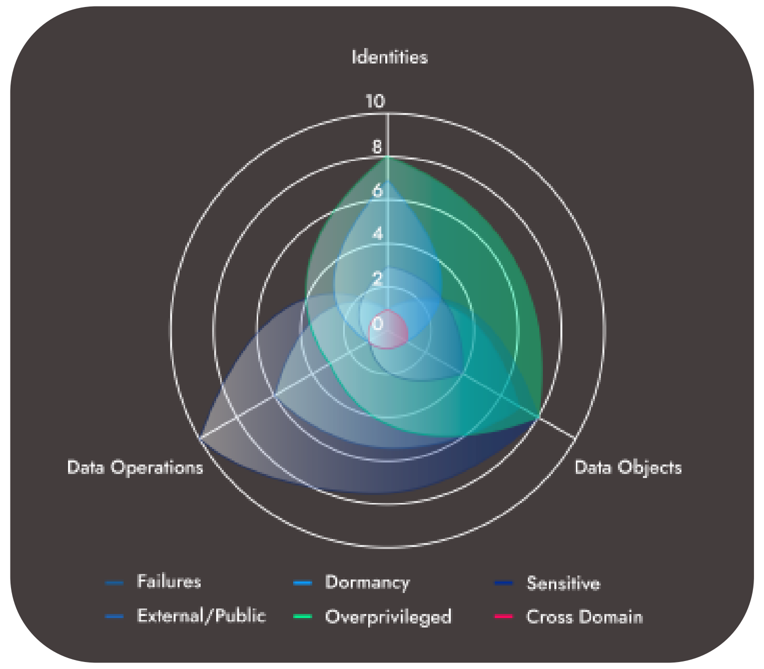
Gain visibility into your entire data landscape with a complete, read-only data security posture map. DataGuard surfaces inactive accounts, dormant data stores, anomalous data flows, and cross-account permissions simplifying risk and incident detection, remediation, and forensics for Cloud Engineering and Security Operations teams.

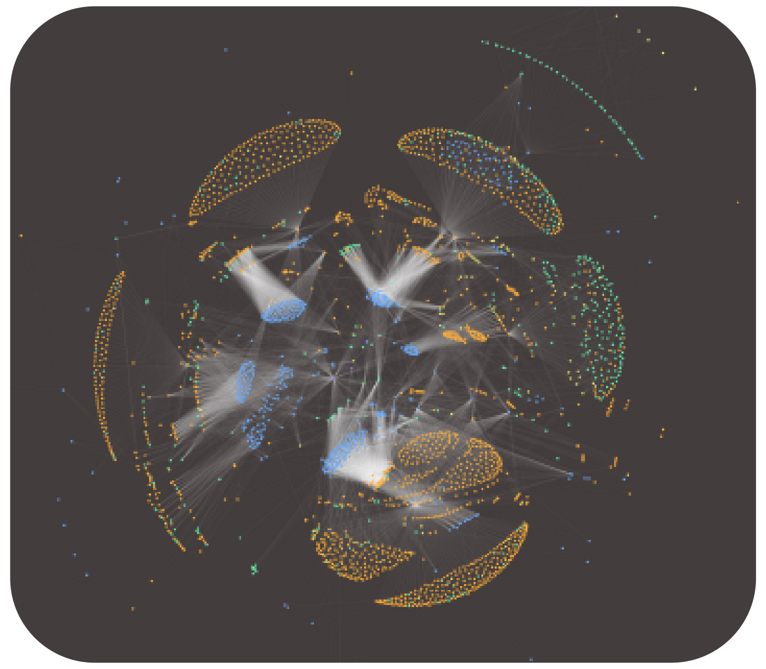
Detect and Respond

Drill down on unsafe data access and risky operations detected by Data Firewalls and alert on violations and potential data breaches. 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 Data Firewall recommendations to tighten access control and minimize blast radius. DataGuard bakes data security into your system infrastructure versus adding peripheral protection.





Get Data Security Posture Map