SYMMETRYSYSTEMS

# Healthcare

Healthcare is one of the most targeted industries by cybercriminals. With patient data at stake, a cyberattack places healthcare providers and related companies at significant risk since care cannot be interrupted. Industry regulations such as HIPAA and HITECH demand information security around many elements, including access control. Increasing cloud adoption, as well as widely adopted telemedicine spurred by COVID, increased vulnerabilities, making compliance efforts even more painstaking.

With continued migration to the cloud, the healthcare industry is experiencing the associated challenges of exploding data volumes and inevitable data sprawl. Security operations teams are often forced to find a needle in a haystack using solutions not purpose-built for data security that often require manual tasks. The healthcare industry had the worst per-data-breach cost of $9.23M in 2021, a 30% increase from $7.13M in 2020*. Pharmaceuticals was $5.04M*.

## Data Security Best Practices with Cloud Adoption

**Conform to HIPAA and other regulatory compliance while moving into hybrid cloud operations.**

**Minimize potential data risks and exposure with visibility into the enterprise data across cloud environments.**

**Automate data management and security tasks on a single console for the hybrid cloud.**

## 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

*IBM Security, Cost of Data Breach Report 2021.

### 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

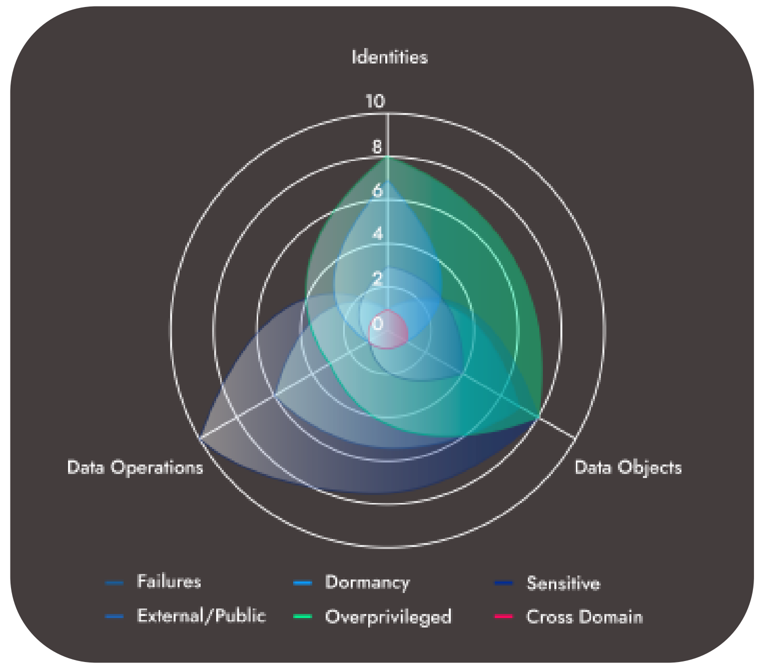
Gain visibility into your entire data landscape with a complete, read-only data security posture map. DataGuard surfaces inactive accounts, dormant data stores, anomalous data flows, and cross-account permissions simplifying risk and incident detection, remediation, and forensics for Cloud Engineering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

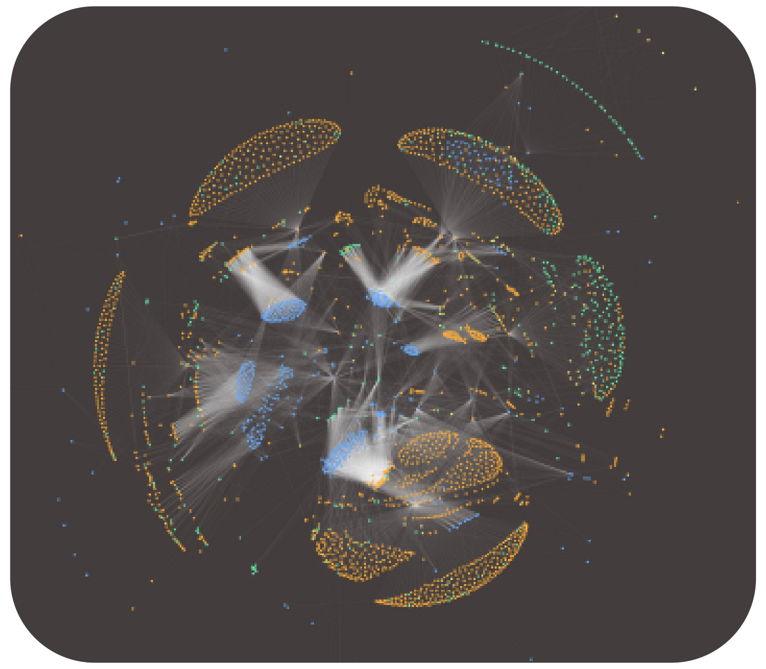
### Detect and Respond

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