SYMMETRY SYSTEMS

Industry Solution Brief

Healthcare

Healthcare organizations are a primary target for hackers, nation-state sponsored threat actors and cyber criminals. With patient data at stake, a cyberattack places healthcare providers, hospitals, medical centers, their vendors, and their partner organizations at significant risk for cyber attacks. Obtaining private identifiable information (PII) is a lucrative goal for threat actors, as the data can be sold on the dark web, or otherwise utilized for nefarious purposes. Legacy cybersecurity technologies and processes are designed to defend the perimeter and endpoints, not the data the threat actors want to attain. Healthcare industry cybersecurity teams need to establish data security practices to protect their most critical asset, their data.

The Healthcare Data Security Challenge: Protecting Patient Data

Compliance and Data Privacy

Industry regulations such as HIPAA and HITECH demand information security around many elements, including data security, data visibility, and access control. Increasing cloud adoption, as well as widely adopted telemedicine spurred by the COVID pandemic, has increased vulnerabilities and threats to healthcare organizations. This has increased cyber risk exposure for healthcare organizations and has made security and compliance efforts even more painstaking.

Transition to Hybrid Cloud

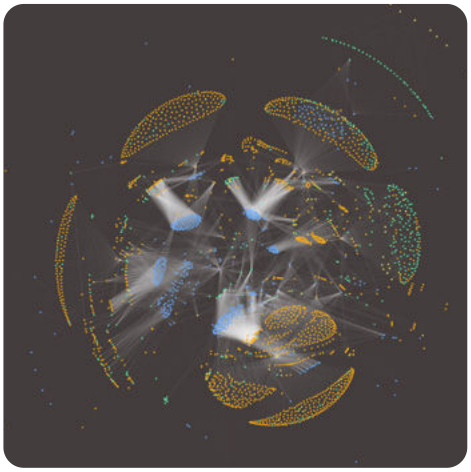
With continued data migration to the cloud, the healthcare industry is experiencing the associated challenges of exploding data volumes and inevitable data sprawl. Healthcare security operations teams are often forced to find a needle in a haystack using solutions not purpose-built for data security 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, French HDS, ISO 27799, HITRUST and other health data regulatory compliance/ standards 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.

Symmetry Systems DataGuard

DataGuard is a **data security posture management (DSPM)** solution that extends the zero trust philosophy to hybrid cloud data stores. Healthcare 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 healthcare organizations 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 **HIPAA, French HDS, ISO 27799, HITRUST,** 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