SYMMETRY SYSTEMS

Industry Solution Brief

Financial Services and Insurance

Financial services and insurance organizations and the data they manage have been high value targets for threat actors for decades. Tremendous efforts have been made by financial services cybersecurity teams and insurance cyber security teams to fortify their defenses to protect their business and their customers from sophisticated cyber attacks. However, legacy cybersecurity technologies and processes are designed to defend the perimeter and end-points, not the sensitive data the threat actors want to attain. All financial services and insurance industry cybersecurity teams need to establish new data security tools and practices to protect their most critical asset, their data.

The Financial Services & Insurance Data Security Challenge: Protecting Customer and Financial Data

Compliance and Data Privacy

Most financial services and insurance organizations operate across multiple jurisdictions and borders, and are challenged to maintain applicable compliance programs such as PCI DSS, FFIEC, FINRA, NCUA-CAP, GLBA, SOX, SOC 1, etc.

They also need to be in pace and compliance with various evolving privacy law requirements – GDPR, CCPA, LGDP and more.

Transition to Hybrid Cloud

While these organizations transition to a hybrid cloud environment, the dormant data accumulated from legacy systems create massive risk. This risk is continuously exploited by threat actors and is reflected in the 36% increased average cost per breach of $5.85M that the industry experienced in 2021.

FinTech Competition

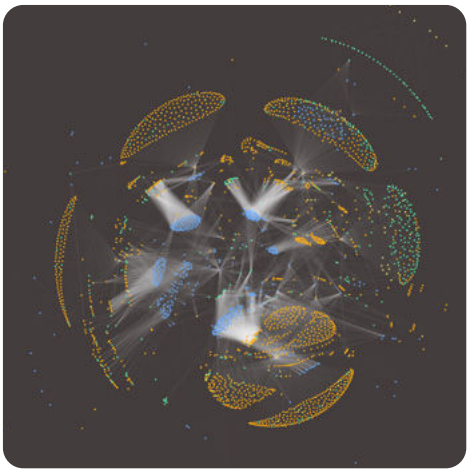
Additionally, a new wave of competition from small, nimble, FinTech competitors is forcing financial services organizations to accelerate the adoption of differentiated digital banking experiences while maintaining compliance and security.

Data Security Best Practices with Cloud Adoption

- Sustain and maintain pace with evolving regulatory requirements while differentiating services from competition.
- Mitigate insider threats and third-party vendor risks through the detection and rapid response to anomalies.
- Gain visibility and effectively manage data security posture, e.g., detecting dormant data, while transitioning to hybrid cloud operations.

Symmetry Systems DataGuard

DataGuard is a **data security posture management (DSPM)** solution that extends the zero trust philosophy to hybrid cloud data stores. Modern security teams use DataGuard to develop a complete understanding of what data they have, where it is located, who and what is entitled to it, how it is secured and in what manner it has been accessed. 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 leave the environment.**



DataGuard produced Environment Graph

The cybersecurity industry is saturated with security solutions that focus on building defense in depth beginning at the perimeter and working toward the data. DataGuard builds security from the data out, directly addresses data objects and examines the cross-section of identity, data store, and data flow to answer important questions like:

- **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, insurance and financial services security teams can easily maintain compliance with challenging industry regulations such as **PCI, SOX, ISO, CSA STAR, GDPR, HIPAA, etc.**

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