SYMMETRY SYSTEMS

Industry Solution Brief

Retail and Ecommerce

Retail and ecommerce businesses have been all over the news on account of being the victims of a plethora of cyber attacks. Ecrime is one probably the most active attack vector to date. Be it ransomware, point-of-sale system compromises, eskimming, phishing, or other attacks, ecommerce cybersecurity teams have had to fight harder than most to keep their businesses safe from threat actors.

With customer data at stake, a cyberattack places retail and e-commerce and their supply chain partners at significant risk for cyber attacks. Obtaining private identifiable information (PII), credit card data, and business data is a lucrative goal for threat actors. Credit card information, as an example, can fetch an average of $500 per card on the dark web. Most cybersecurity technologies and processes were designed to defend the businesses security perimeter, not the data the malicious hackers want to attain. Retail & ecommerce industry cybersecurity teams need to evolve from securing the perimeter and endpoints, to establishing data security practices to protect customer data and their businesses brand.

The Retail & E-commerce Data Security Challenge: Protecting Customers and Brand

Compliance and Data Privacy

In order to conduct digital business, customer information is collected by retailers in droves. Also, most retail and e-commerce organizations operate across multiple jurisdictions and borders, and are challenged to maintain pace and compliance with various evolving privacy law requirements – GDPR, CCPA, PCI, and more.

Customer Data Protection

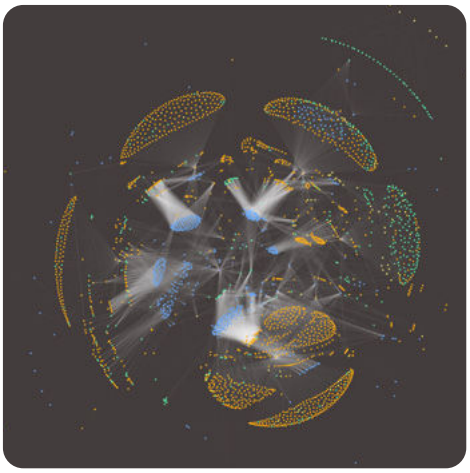
It has been reported 69% of consumers would be less inclined to do business with a breached organization. The **Verizon Data Breach Investigations Report (DBIR)** outlined that 61% of attacks targeted payment card data. Retailers must secure their environment with **Payment Card Industry Data Security Standards (PCI DSS)** compliance requirements, or they will be subject to fines. In order to protect customer data, you need to know where it is stored, who has access to it, and what is being done with that data.

Data Security Best Practices with Cloud Adoption

- Comply with PCI, GDPR, CCPA and other regulations by establishing cybersecurity practices from the data out.
- 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. Retail and ecommerce 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 ecommerce and retail 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 GDPR, CCPA, PCI, 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