SYMMETRY SYSTEMS

Industry Solution Brief

Communications and Media

Threat actors love to target communications & media companies. The business model for these organizations relies heavily on collecting customer data, payment processing data, advertising data, and more. If a threat actor is able to breach a communication & media organization, they will likely be able to collect data that can be used to conduct sophisticated attack reconnaissance or develop spear phishing campaigns against their customers. They could also collect personally identifiable information (PII) and payment card data that they can use for financial gain immediately. With millions of users, thousands of clients, dozens of interconnected technologies and applications, and a vast infrastructure that is challenging to protect, these companies have numerous entry points for third-party attacks. The impact of successful attacks can be significant and far reaching. Business reputations can be ruined, stock prices can drop and the organization's ability to grow and succeed can be impeded. Legacy cybersecurity technologies were designed to defend the perimeter and endpoints, not the data the threat actors want to attain. Communications & media security teams need to establish data security practices to protect their most critical asset, their data. They must protect their reputations, revenue, and trustworthiness by defending their data.

The Communication & Media Industry Data Security Challenge: Protecting Customer and Proprietary Business Information

Third-party Risk

Media & communication companies and their products combine mobile, network, hardware, software, and data storage capabilities. These create dependencies and a massive volume of data that needs to be stored and protected. Businesses, vendors, and customers are interconnected via APIs, portals, and, most importantly, data. If one customer or vendor experiences a breach, this might create a domino effect in which customer, business, vendor, and mission critical data is exposed or stolen.

Compliance and Data Privacy

Communication & media companies collect massive volumes of data and operate across multiple jurisdictions and borders. It is a tremendous challenge for them to maintain pace and compliance with various evolving privacy law requirements – GDPR, CCPA, and more.

Customer Data Protection

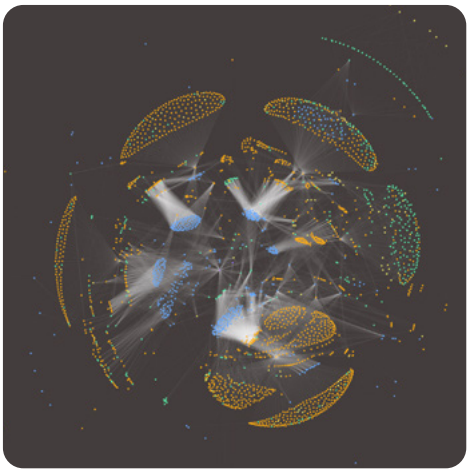
It has been reported 69% of consumers would be less inclined to do business with a breached organization. Communication & media companies, business-to-business and business-to-consumer, collect customer data in droves. The sheer volume of customer data that is collected in the sales and marketing process, as well as user data that is generated throughout the life of the technology is tremendous. In order to protect customer data, technology companies 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

- Understand where customer data is stored, how it is accessed, and how it is used, so that proper access permissions can be enforced.
- Gain visibility and effectively manage data security posture, e.g., detecting dormant data, while transitioning to hybrid cloud operations.
- Sustain and maintain pace with evolving regulatory requirements (such as GDPR and CCPA) while differentiating services from competition.

Symmetry Systems DataGuard

DataGuard is a **data security posture management (DSPM)** solution that extends the Zero Trust philosophy to hybrid cloud data stores. Communication & media 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 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 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**, 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