Solution Brief

SYMMETRY SYSTEMS

Cloud Data Activity Monitoring (Cloud DAM)

Key Challenge

Modern organizations are accelerating their growth with data, but legacy **Database Activity Monitoring (DAM)** tools haven't kept pace, lacking the capability to monitor data cost effectively where it is being used the most.

Solution

Symmetry Systems' **Data Security Posture Management (DSPM)** solution, DataGuard, provides security teams with **cloud data activity monitoring capabilities** that offer visibility into activity across all organizational datastores with precision and accuracy.

Database Activity Monitoring (DAM) solutions have been commercially available for decades and are used to provide an audit trail of user activity on data within monitored databases. Their adoption has been minimal outside of regulated industries as they are generally perceived as expensive database logging and database auditing tools. As organizations have migrated to the cloud and adopted more modern cloud data platforms (AWS Redshift, Google BigQuery, PostgreSQL, Azure SQL, AWS DaaS) and other new forms of persistent data repositories like Kafka, Spark, or NoSQL, existing DAM tools have struggled to adapt. Their biggest challenge has been connecting the user to the activity, providing no traceability due to session pooling or use of shared service accounts.

Key Benefits

- Assists businesses in understanding **how data is being used** without any overhead.
- Ensures logs are being written to existing **tamper-proof log stores**, creating an immutable audit trail of all access to all data in their data stores.
- Aids security teams in **understanding** and **remediating** data breach and attack impact.
- Addresses **insider threats** and vendor, supplier, and third-party risk by providing insight into which identities have accessed which data.
- Facilitates **audit and compliance** capabilities.

Solution Overview

Data Security Posture Management (DSPM) provides data activity monitoring at scale across all organizational data stores. It answers the questions: “How is my data being used?”, and “Who is using it?” with precision and accuracy, creating an immutable and searchable audit trail of data operations being performed.

Symmetry Systems’ DataGuard is a Data Security Posture Management solution designed to support a complete, data object-level understanding of:

What data do we have?

Where can the data be found?

Who has access?

For each data object, DataGuard uses machine learning and near real-time alerting to combine knowledge of the data, the identities, and the operations to provide unique and searchable insights into the activity being performed and the identity that performed it.

About Symmetry Systems DataGuard

DataGuard arms security operations teams 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 their environment.

DataGuard allows security operations teams to build 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:

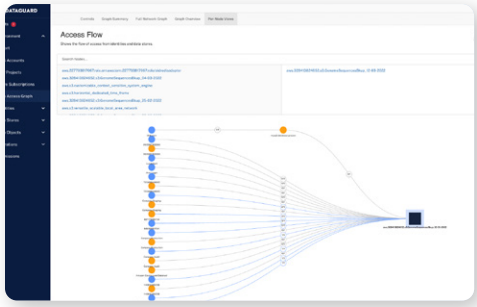
- **Where is sensitive data?**
- **Who has access to it?**
- **What operations have they performed against it?**

With DataGuard, security operations teams can improve their data security posture and outpace ever-growing data security risks and threats.

DataGuard Cloud Data Activity Monitoring Outcomes

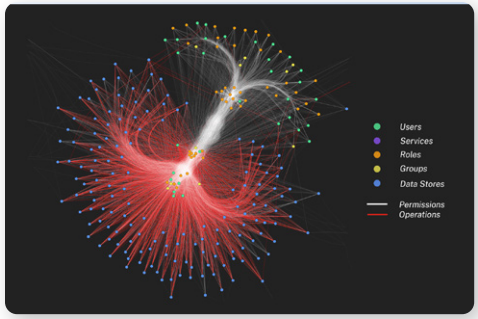
- Reduce meantime to detect and mean time to respond to data security issues and breaches to minimize data breach cost.
- Identify and lock down excessive data access permissions and privileges, to reduce threat actor ability to move laterally through your network.
- Understand the data blast radius of compromised identities and other insider threats quickly to take corrective or preemptive action.
- Provide executive visibility to cloud data sprawl, identity life cycle, Zero Trust violations, and sensitive data access to build security programs from the data-out.
- Minimize the cost and risk of data exposure associated with cloud data stores.
- Improve the security posture of sensitive data and cloud data stores.

DataGuard Data Activity Monitoring Capabilities



Anomalous Data Behavior Monitoring and Alerting

DataGuard detects current and historic anomalous data access and usage, alerting security teams in a timely manner with precision. Security teams can use DataGuard to investigate potential data breaches, ransomware attacks, and other cyber threats as quickly as possible.

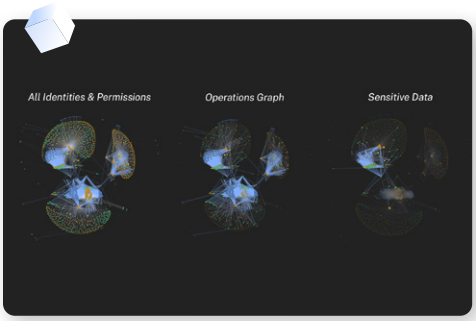


Leading with Effective Data Breach Investigation and Response

DataGuard helps security teams quickly understand the blast radius and potential root causes during investigations of data security events. With DataGuard security teams can prioritize steps to contain and reduce the blast radius of the data security incident. Security teams can quickly:

- **Uncover potential malicious data access within hybridcloud environments and initiate steps quickly contain the attack.**
- **Collect information on what data threat actors have accessed and obtained, and what can be done to lock down further access.**
- **Review data flow maps on how far threat actors were able to move laterally throughout the environment to cut down forensic time and ability to spread.**

DataGuard helps security teams to reduce the blast radius of a potential data security event and quickly understand the blast radius during a data security incident.

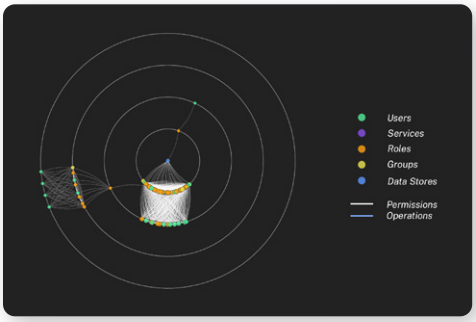


Visualizing and Securing Data and Data Flow Across Environments

DataGuard is a DSPM solution that arms security operations teams with a complete understanding of:.

- **The data (from sensitivity to location).**
- **The identities that have access (permissions).**
- **Operations performed on the data by those identities(flows).**

For each data object, DataGuard combines each of these elements to provide unique insights to help prioritize data security risks, and aids security teams in remediating their impact.



Reducing the Data Blast Radius from Insider Threats, Vendors, and Third Parties

DataGuard is able to enumerate all users and technologies who are able to access each data object, how they may use it, and have used it. Using machine learning DataGuard:

- **Identifies excessive, unused, or anomalous data.**
- **Determines data access and usage.**
- **Enumerates paths to sensitive data.**
- **Quantifies the potential data blast radius of accounts.**

Security teams use DataGuard to inform and control least privilege IAM permissions, reduce data sprawl, and proactively get alerted to anomalous data behaviors. With DataGuard, security teams can stay ahead of threats and reduce the data blast radius.

Ready to secure your mission-critical data with precision and scale?

Stop chasing threats at your perimeter. Know your data security posture and protect your sensitive data.

For more information, visit us at **www.symmetry-systems.com**