Solution Brief

SYMMETRY SYSTEMS

Data Visibility with Data Security Posture Management (DSPM)

Key Challenge

When it comes to data visibility, today's complex web of cloud and on-premise infrastructures means data is housed in a diverse array of locations. IT and security teams face the challenge of understanding where data resides, how sensitive it is, who has access, and how that data is being used.

Solution

Data visibility for data security purposes is a key component of an overall Data Security Posture Management (DSPM) solution. DSPM solves the complexity problems associated with protecting sensitive business data.

Challenges

Today, organizations retain different types of data across complex cloud and on-premises infrastructures. When it comes to protecting that data, IT and information security teams need to understand where data resides, how sensitive it is, who has access, and how that data is being used. Having full data visibility across the infrastructure is difficult when using a patchwork of traditional security tools like **identity access management** (IAM), data catalogs, **data loss prevention** (DLP), **data activity monitoring** (DAM), and **cloud infrastructure entitlement management** (CIEM)

To further complicate data visibility, many companies are challenged with restrictive firewall policies limiting visibility, complex IAM policies that are difficult to unravel, and the lengthy and often manual process of responding to compliance and auditing requests.

Key Benefits

Data visibility benefits in **DataGuard**, Symmetry Systems' Data Security Posture Management (DSPM) solution, include:

- ✓ **Assisting** businesses in understanding where sensitive data is located.
- ✓ **Removing** 'dormant data' (i.e., data no longer in use) and reducing both the risk of exposure and data storage costs.
- ✓ **Highlighting** locations and usage of sensitive data to improve the security audit process or identify high-risk applications.
- ✓ **Facilitating** audit and compliance capabilities.
- ✓ **Addressing** insider threats and vendor, supplier, and third-party risk by providing insight into which identities have access to which data.

Solution Overview

Businesses need both comprehensive and coherent visibility into their entire data landscape, including a complete data access graph. What businesses don't need is a mishmash of tools, alerts, and insights from IAM, DAM, DLP, and CIEM tools that require hours of manual interpretation and fixes.

Unique data visibility components in DataGuard surface sensitive, dormant, and at-risk data objects at a granular level, as well as identify anomalous data flows for cloud security and security operations teams to act on.

DataGuard resides within your environment, and the unique data visibility insight DataGuard offers helps you understand your overall security posture and protect sensitive data. DataGuard provides:

- ✓ **Automated auditing and compliance reports.**
- ✓ **Integration with SIEM solutions.**
- ✓ **High-quality, actionable security alerts.**
- ✓ **Recommendations for streamlining IAM and security policies.**
- ✓ **Ability to see how identities connect to various data stores.**

For each data object, **DataGuard** combines knowledge and classification of the data, the identities, and the operations performed on it to protect sensitive data by providing unique insights, helping to prioritize an organizations' data security risks, and supporting any impact remediation.

About DataGuard

DataGuard arms security operations teams with accurate and precise insights into their data security posture and associated data risks across AWS, GCP, Azure, and on-premises environments–**without having data ever leave their environment.**

DataGuard improves data visibility by allowing security operations teams to build security from the data out by directly addressing data objects and examining the cross-section of identity, data stores, and data flows to answer important questions like:

What data do we have?

Where can the data be found?

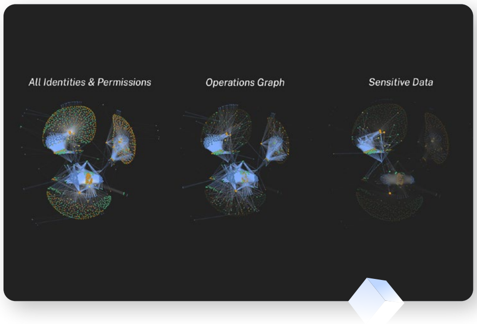
Who has access?

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

DataGuard Data Visibility Outcomes

- Provide unmatched visibility to data and data flows within hybrid-cloud data repositories.
- Quantify and minimize the cost and risk of data exposure associated with cloud data stores.
- Provide deep visibility to cloud data sprawl, identity lifecycle, zero-trust violations, and sensitive data access to build security programs from the data out.
- Understand the potential data blast radius of compromised identities and other insider threats quickly to take corrective or preemptive action.
- Improve the security posture of sensitive data and cloud data stores.
- Reduce mean time to detect (MTTD) and mean time to respond (MTTR) to data security issues and breaches to minimize data breach cost.

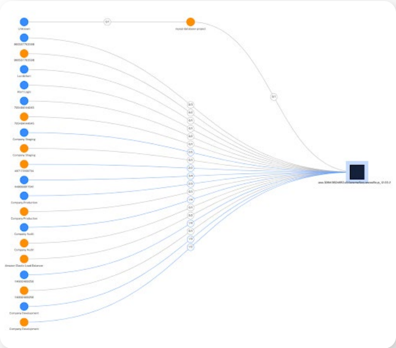
DataGuard Data Visibility Outcomes



Visualizing and Securing Data and Data Flow Across Environments

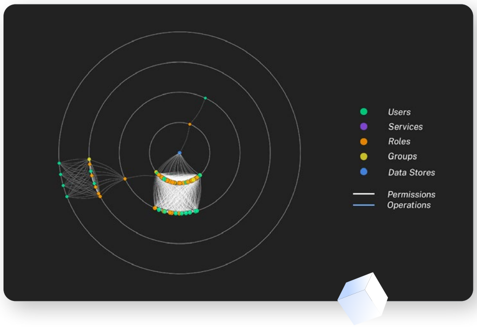
DataGuard is a DSPM solution that arms security operations teams with a complete understanding of their data, the identities that have access, and the operations performed against that data.

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



Data Activity Monitoring and Alerting

DataGuard ensures current and historic data access and usage is logged and searchable, providing security teams with insights into what is happening to individual data objects with precision. Security teams can use DataGuard to investigate potential data breaches, ransomware attacks, and other cyber threats as quickly as possible.

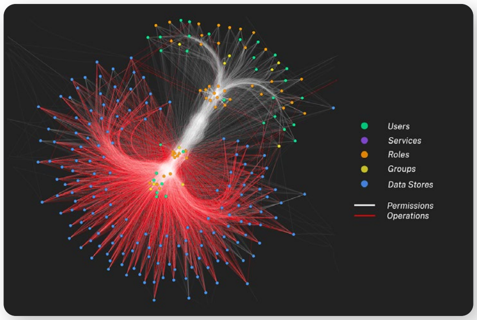


Quantify and Reduce the Data Blast Radius from Insider Threats, Vendors, and Third Parties

DataGuard is able to enumerate all users and technologies who can access each data object, as well as clarify 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.



Respond effectively to Data Breach and other data loss events

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 to reduce the blast radius of the data security incident. Security teams can quickly:

- **Uncover potential malicious data access within hybrid-cloud environments and understand the steps to take to 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.**

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**

symmetry-systems.com | sales@symmetry-systems.com symmetry-systems-inc @SymmetrySystems