SYMMETRY

SOLUTION BRIEF

Cloud Data Loss Prevention (Cloud DLP)

symmetry-systems.com | hello@symmetry-systems.com

Key Challenge

Data breaches are seemingly inevitable. Traditional enterprise data loss prevention (DLP) software is ineffective in reducing the impact from these breaches, since DLP focuses on inspecting data as it leaves your organization—a classic case of too little security after the fact.

Solution

Symmetry System's Data Security Posture Management (DSPM) solution, DataGuard, provides modern cloud data loss prevention capabilities to reduce the risk from data breaches by helping organizations properly inventory, classify, and protect their sensitive data assets long before data get exfiltrated. DataGuard secures sensitive data from unauthorized use from the data out, unlike traditional DLP that focus solely on the data loss.

In modern organizations, there are more users, devices, applications, services, and data located outside of an enterprise perimeter than ever before. Businesses struggle to properly inventory, classify, control, and protect their sensitive information from unauthorized access, resulting in an endless stream of preventable data breaches.

An increase in multi- and hybrid-cloud environments means that your organization's information is held in a multitude of fragmented locations, including structured and unstructured data. Legacy perimeter-based data loss prevention tools are simply ineffective in this distributed environment without forcing network traffic through multiple disparate security chokepoints and intercepting encrypting traffic. Relyingon the

integrated and costly DLP capabilities provided by each cloud provider quickly becomes too challenging for security teams.

Government regulations and industry mandates add further complexity, requiring near real-time notification of data breaches.

Key Benefits

- Assists businesses in understanding where sensitive data is located.
- Reduces data sprawl.
- Informs and controls least privilege IAM permissions.
- Helps organizations prioritize their data security risks.
- Reduces data blast radius.
- Aids security teams in remediating data breach and attack impact.
- Addresses insider threats and vendor, supplier, and third-party risk by providing insight into which identities have access to which data.
- Facilitates audit and compliance capabilities.

Solution Overview

Data security posture management (DSPM) addresses the key issues facing every business when it comes to protecting mission-critical data. It answers the questions:

- What data do we have?
- Where can the data be found?
- Who has access?

Most businesses implement data loss prevention by focusing first on the egress points and then trying to classify data in motion, preventing it leaving the organization's control from the "threat in". The problem with this approach is that scaling to billions of data objects directly accessible from the internet is impossible for any company to manage. DPSM extends the Zero Trust philosophy to hybrid cloud data stores by securing organizations from the "data out". Symmetry Systems' DataGuard is a data security posture management solution designed to support a complete, data object-level 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 uses machine learning and near real-time alerting to combine knowledge of the data, the identities, and the operations to provide unique insights, help prioritize an organization's potential data loss, prioritize any impact remediation, and alert security teams on any anomalous data leakage events.

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.

- Where Is Sensitive Data?
- Who Has Access To It?
- What Operations Have They Performed Against It?

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:

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

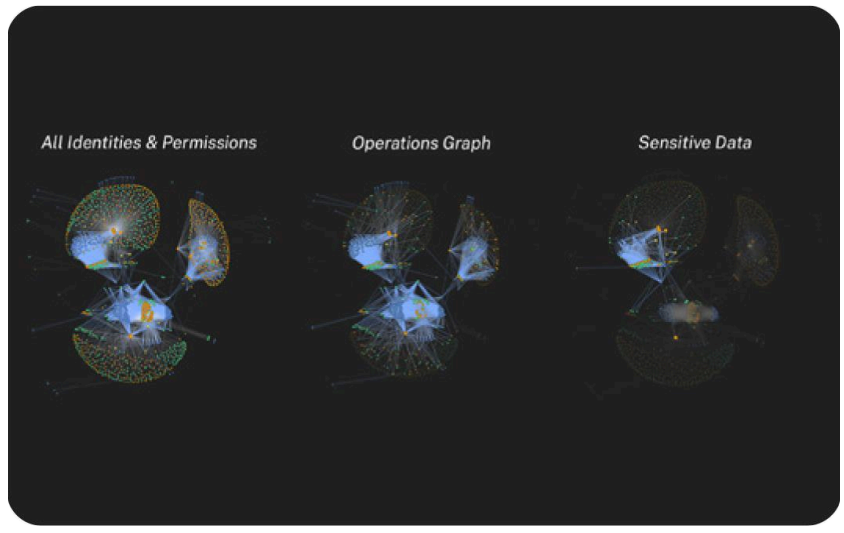
DataGuard Cloud Data Loss Prevention Outcomes

- Reduce mean time to detect (MTTD) and mean time to respond (MTTR) 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 your sensitive data and cloud data stores.

DataGuard Data Loss Prevention Capabilities

VISUALIZING AND SECURING DATA AND DATA FLOW ACROSS ENVIRONMENTS

DataGuard is a DSPM solution that supports data loss prevention by arming security 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 these elements to provide unique insights to help prioritize data security risks and aid security teams in remediating their impact.



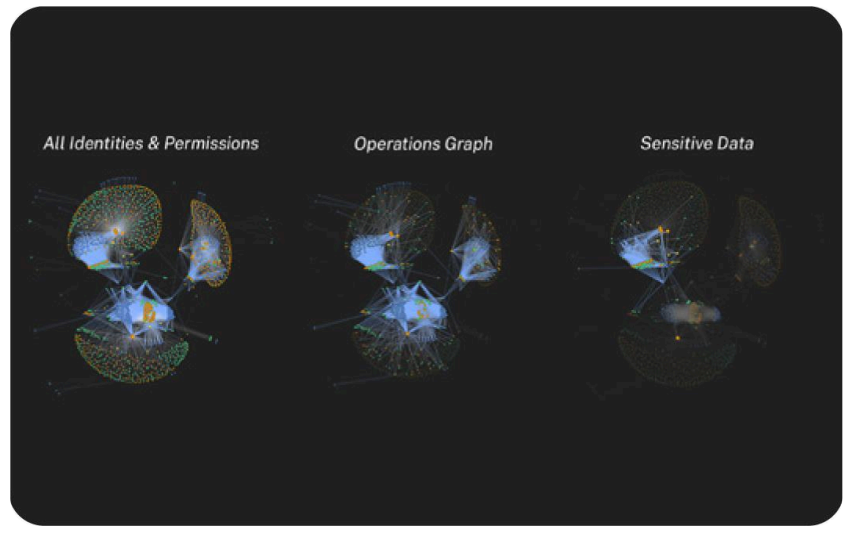
ANOMALOUS DATA BEHAVIOR MONITORING AND ALERTING

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

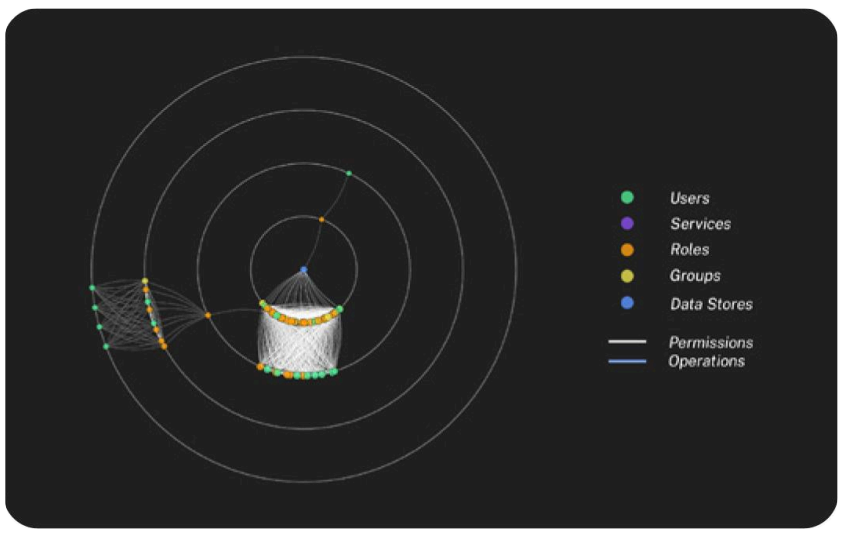
LEADING WITH EFFECTIVE DATA BREACH INVESTIGATION AND RESPONSE

DataGuard helps security teams to reduce the blast radius of a potential data loss and quickly understand the data blast radius during a data loss event. With DataGuard, security teams can prioritize steps to contain and to reduce the data loss blast radius. Security teams can quickly:

- Uncover potential malicious data access within hybridcloud environments and 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.



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