Solution Brief

SYMMETRY SYSTEMS

California Consumer Privacy Act (CCPA)

Key Challenge

The California Consumer Privacy Act of 2018 (CCPA) gave consumers more control than ever before over the personal information that organizations collect about them; but organizations are still struggling to accurately and reliably identify whatconsumer data they have.

Solution

Symmetry System's Data SecurityPosture Management (DSPM) solution, DataGuard, provides privacy, security, and compliance teams with the data security tools to discover inventory, classify, and enforce compliance with CCPA requirements across all organizational datastores with precision and accuracy.

Businesses struggle to properly inventory, classify, control, and protect personal information that they collect. As organizations grow and operate, data sprawl can make identifying personal information harderto identify and control.

Modern privacy laws like the California Consumer Privacy Act provide consumers the right to request that an organization:

- Provide details on what information is held about them.
- Describe how that data is used and who it is shared with.
- Delete personal information.
- Provide them a copy of their personal information in a "readily usable format" that enables its transfer to third parties easily.

It also allows consumers to opt out of the sale of personal information.

These rights are impossible to respond to with precision and accuracy without comprehensive visibility of the data with an organization's data stores.

Key Benefits

- Assists businesses in understanding where the **personal information** of California residents is located.
- Reduces **data sprawl.**
- Aids privacy, security, and compliance teams in identifying personal information of California residents within data stores and associate it with the owner of the personal data.
- **Reduces response time** to DataSubject Access Requests.
- Facilitates **audit and compliance** capabilities.
- **Continuously monitors** data stores and data flows for **non-compliance** with deletion, opt-out, and do-not sell requests.

Solution Overview

Data security posture management (DSPM) provides the precision and accuracy that every business needs to ensure compliance with modern privacy laws like CCPA. It allows organizations to determine with precision and accuracy:

- **What information about California consumers they hold and how it is used and shared?**
- **Have they complied with consumer requests regarding their personal information?**

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 insights, help quickly respond to consumer requests, prioritize remediation, and alert security teams on any non-compliance.

About Symmetry Systems DataGuard

DataGuard arms privacy, security, and compliance 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 Outcomes

- Minimize the time and cost in notifying impacted individuals.
- Reduce the time and cost associated with responding to Data Subject Access Requests.
- Understand the extent of recipients or categories of recipients to an individual's data and quickly take corrective or preemptive action.
- Provide executive visibility to cloud data sprawl, identity lifecycle, zero-trust violations, and personal information 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 personal information and cloud data stores.

Identify Your Data

DataGuard enables compliance and cloud migration teams to identify where personal information resides without having the data leave their cloud environment.

Gain Full Visibility

DataGuard surfaces inactive accounts, dormant data stores, anomalous data flows, and cross-account permissions.

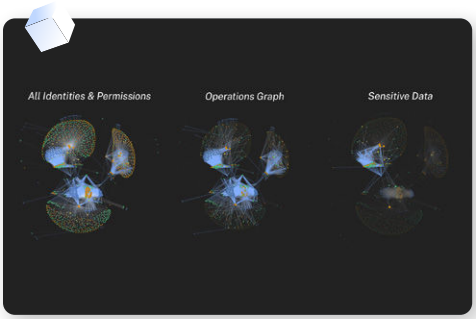
Detect and Respond

Uncover unsafe data access practices and risky operations detected by DataGuard's built in data firewalls.

Protect Your Data

DataGuard makes it easy to deploy least privilege permissions on IAM, cloud accounts, and data store access.

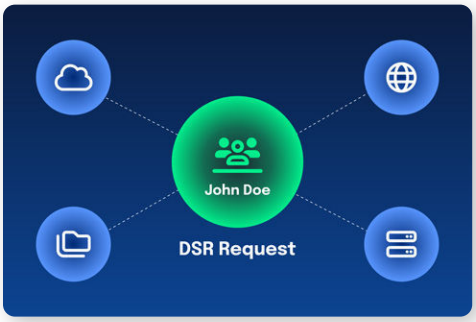
DataGuard DSPM Capabilities



Visualizing and Securing Data and Data Flow Across Environments

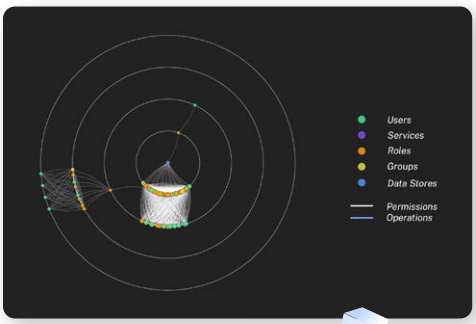
DataGuard is a DSPM solution that arms security operations teams with a complete understanding of their data, the identities that have access, and the operations performed against that data.

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



Streamline and Automate Data Subject Access Requests

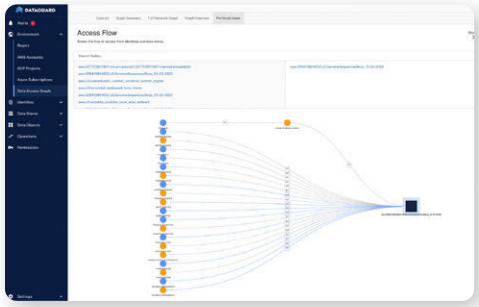
DataGuard helps quickly identify information in response to Data Subject Access Requests and validate that information is not being stored or shared unwittingly.



Leading with Effective Data Breach Investigation and Response

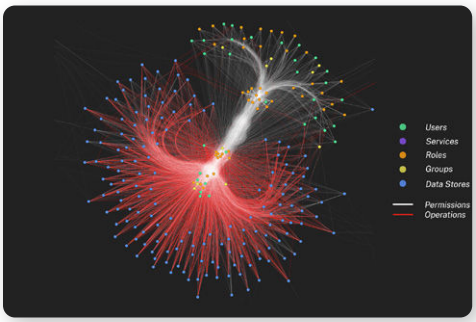
DataGuard helps security teams quickly understand the blast radius and potential root causes during investigations of data security events. With DataGuard, security teams can prioritize steps to contain and to reduce the blast radius of the data security incident. Security teams can quickly:

- **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 wereable to move laterally throughout the environment to cut down forensic time and ability to spread.**



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.



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**