Comparison

Amazon Macie & DataGuard

SYMMETRY SYSTEMS

Tools like Amazon Macie are designed to help businesses manage sensitive data discovery.

Macie may seem like an ideal solution. But as data stores and the amount of sensitive information contained in them grow, businesses are discovering that Macie presents challenges around cost, scalability, and actionable insight.

Limited to S3 Buckets

To start, Macie only works with S3 buckets, and the more S3 data you have, the more incredibly cost prohibitive Macie becomes. Many businesses are capping their Macie budgets because Macie just becomes too expensive to operate with large amounts of S3 data.

Little or No Actionable Insight

And when it comes to actionable insight, security professionals are finding themselves making decisions in the dark, because Macie doesn't provide adequate insight to enable meaningful action around:

- Data access monitoring (DAM) including identifying dormant data or indicators of compromise (IOC).
- Discovering sensitive data you didn't know you had.
- Identifying your lifecycle, zero-trust or least-privilege violations, and sensitive data access.
- Identifying and locking down excessive data access permissions and privileges.
- Detecting and controlling out of country data operations.
- Maintaining compliance with privacy regulations.

No Classification/Compliance Support for Other Data Stores and Cloud Services

And then there are the added complexities around data classification and compliance with your other data stores, like RDS, PostgreSQL, or MongoDB or additional cloud services like GCP and Azure–or any combination of these. Because guess what? Macie isn't going to help you with these data buckets or cloud services.

Challenge

AWS designed Macie to provide visibility and data classification for S3 buckets so organizations can address the needs associated with security, compliance, and privacy. Unfortunately, Macie is not without its drawbacks.

- Organizations often find themselves capping their Macie budget due to how cost prohibitive Macie becomes as S3 data stores grow.
- Macie lacks critical information on data access monitoring (DAM), such as whether dormant data exists and if there are any indicators of compromise (IOC).
- Macie works with limited sets of business logic for security and compliance detections and offers no actionable insight when issues are discovered.
- Macie doesn't support other data bucket types, such as RDS, PostgreSQL, MongoDB, and others or other cloud services like GCP and Azure. Few companies limit their data stores to only S3.

Solution

DataGuard DSPM

SYMMETRY SYSTEMS

Data Security Posture Management (DSPM) helps modern organizations manage the level of complexity and scale involved with protecting their most important asset–their data. **DataGuard is a Data Security Posture Management (DSPM)** solution that arms security operations teams with a single source of information about their data security posture and associated data risks across AWS, GCP, Azure, and on-premise environments.

DataGuard unifies visibility into data objects across all data stores, answering the data security and compliance questions that traditional cloud security tools cannot. With DataGuard, SecOps teams can enable 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?

DataGuard is 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 to combine knowledge of the data, the identities, and the operations to provide unique insights, help prioritize an organizations' data security risks, and support any impact remediation.

SYMMETRY SYSTEMS

DataGuard Benefits for S3

- Affordable, cost-effective scanning and licensing model; significantly less than Macie.
- Highly scalable; Supports multi-cloud, hybrid-cloud, and on-premise deployments.
- Out-of-bound information collection to ensure no business process interruptions.
- Continuous data security and compliance validation.
- Improve the security posture of sensitive data and cloud data stores.
- Audit and compliance capabilities.
- Automatic and continuous monitoring of data, with discovery of a multitude of sensitive data types in all your environments.
- Comprehensive understanding where sensitive data is located.
- Significant reduction in data sprawl by providing visibility into data dormancy and over-permissioned buckets.
- No vendor risk due to 'in-your-cloud' deployment model.
- Precision and accuracy with operations and activity log information ingestion.
- Rapid time to results–gain data security insights in hours from deployment.
- Truly actionable insights–understand the impact of compromised identities and data quickly to take corrective or preemptive action.
- Minimize the cost and risk of data exposure associated with cloud data stores.
- Ability to prioritize data security risks.
- Proactive reduction in potential blast radius by giving organizations the ability to clean dormant data and manage unused permissions.
- Insight into what data has been accessed by which identities to address concerns around insider threats and vendor, supplier, and third-party risk.
- Information, support, and alerts to ensure businesses can maintain least privilege access to S3 buckets.

SYMMETRY SYSTEMS

Product Capability/Feature Comparison	AWS Macie	Symmetry Systems DataGuard
Cost-effective classification.		●
Actionable insights based on data scans.	◐	●
Scalable beyond just S3 (e.g., RDS, PostgreSQL, or MongoDB).		●
Scalable beyond AWS. Supports GCP, Azure, and On-Premises.		●
Detects PII and PHI data stored in AWS cloud accounts.	●	●
Supports data security and privacy for S3	●	●
Shows Active and Passive Identities that have access to sensitive data.		●
Shows activities performed by identities connected to sensitive data.		●
Shows third-party identities that have access to sensitive data.		●
Shows data flow at present and activities trends.		●
Presents visualization of data.		●
Exports alerts to third-party systems.	●	●
Supports Lambda Rules execution (via Evenbridge for Macie).	●	●
Generates automated scripts to remediate findings.		●

Ready to secure your data with precision and scale?

Stop chasing threats at your perimeter.

Know your data security posture and protect your mission critical data.
For more information, visit us at www.symmetry-systems.com.