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.