



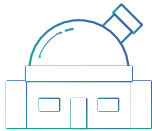
WHAT IS DATAGUARD?

DATAGUARD is a logically isolated security visibility suite that plugs into your cloud environment to provide valuable insight into identities, data stores, accesses, operations, objects and assesses your risk vulnerability.

WHY IS IT IMPORTANT?

Currently, security teams work with network-centric tools that allow only limited visibility into their environment, making accurate monitoring and risk measurement non-trivial in compromised applications.

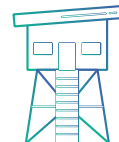
BENEFITS TO CUSTOMERS



Granular security monitoring on your accounts, data stores, operations and access



Object-level access to records, simplifying HIPAA, SOC2, ISO, GDPR, and CCPA audits/compliance



Detection-response alerting performing comprehensive reporting on the flag trigger

DATAGUARD offers an easy solution to maintaining tight identity access and management policies by supplying exhaustive risk maps, customizable firewall alerts, and granular data monitoring.

OUR SOLUTION



Provides visibility of data objects, identities, and behaviors via its graph analytics engine



Automated responses at scale for DevOps



Takes less than 1 hour to set up and run org-wide



Enables customers to filter by critical data, anomalous behaviors, and compliance requirements



Runs inside a customer's AWS, GCP, and private cloud in an isolated account

DATAGUARD

THE DATAGUARD JOURNEY

INSTALLATION IN
THE CLOUD ENVIRONMENT



FINDINGS PRESENTED
AND DISCUSSED



REMEDiations WITH
CLOUD SECURITY TEAM



ONGOING EVALUATIONS AND ALERTS
FOR CLOUD ENVIRONMENT



THE BREAKDOWN

DataGuard connects to your cloud environment without breaching or damaging your data

The service runs in a separate account in your organization. It is limited to the virtual machines it is assigned to and can be removed from the cloud provider dashboard at any time.

DataGuard also utilizes Bastion servers both on the customer security side (to investigate DataGuard output) and on the Symmetry side (to diagnose customer provided issues and logs) in order further isolate its own operations.

DataGuard outputs highly sanitized graphs and charts with filtering capabilities

Using a highly restricted IAM role and VPC, DataGuard combs through data stores to provide only necessary data attributes for monitoring and visibility.

DataGuard can be tailored to your use

Based on your preferences, you can set up highly configurable firewalls, install APM services, perform health and stack monitoring, schedule investigations, and even expose sanitized data to endpoints for your own service and automation development.

Accommodate regulatory compliance suited to your business i.e., HIPAA, SOC2, ISO, GDPR, CCPA, etc.

