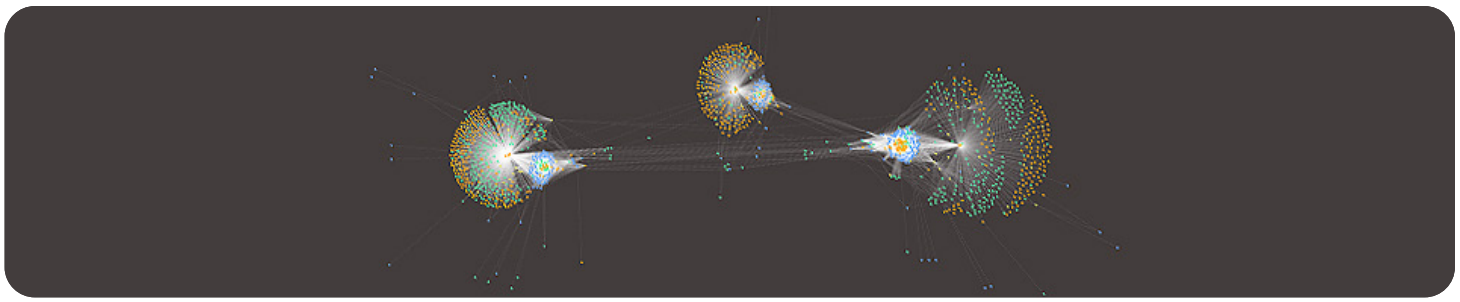
SYMMETRY SYSTEMS

Whitepaper

Forensics

Can you minimize organizational impact by pinpointing if and which data has been compromised within minutes?

As business and regulatory impacts are defined by the time and precision it takes to identify, respond to, and mitigate an incident, how is your organization positioned to respond?



Technical Requirements to Achieve Future State

Preparation

- Visibility across all your cloud environments (AWS, Azure, GCP)
- Proactively visualize how identities are accessing data, and with what roles or permissions over time

Detection & Analysis

- Ability to set Data Firewall Rules allowing alerting on anomalous behavior or access to sensitive data
- ML-based risk scoring based on identity behavior and cloud configurations

Containment, Eradication, & Recovery

- Identify what sensitive data has been accessed, by whom, and what operations have been taken against it
- Visualize identity's operations against data and implement auto-generated IAM policies for containment

Post Event Activity

- Gather precise, reportable evidence based on identity behavior, and implement mitigation strategies to reduce future blast radius

Driving to Future State Requirements

Current Operations	Future Operations
Preparation	
• Combining multiple sources to construct full visibility • Vendors potentially introduce attack vectors into organization	• Using a single platform for complete data flow visibility and controls • Hosted solution within your cloud perimeter
Detection & Analysis	
• Sifting through multiple alerting tools to find out where sensitive data lives and how it's been accessed	• Single workflow for detecting and alerting when sensitive data is accessed outside set policy
Containment, Eradication, & Recovery	
• Responding to an incident by analyzing and mitigating the estimated blast radius	• Taking precise actions based on accurate evidence • ML-based evidence allows for rapid identification and containment of an incident
Post Event Activity	
• Collecting and combining evidence from multiple sources to reconstruct events and report	• Ability to gather precise, accurate, and actionable evidence from a single workflow

Why Symmetry Systems DataGuard?

- No Vendor Risk due to 'In your Cloud' deployment model
- Supporting Multi cloud and On-premise deployments
- Precision and Accuracy due to operations and activity log information ingestion
- Out of band information collection ensuring no business process interruptions

Gain rapid understanding through classification of sensitive data

- Mapping out the full blast radius of compromised credentials including derived permissions
- Ability to analyze historic events, behaviours, and operations through correlating cloud natively available logs

Gain clear visibility into attack vectors

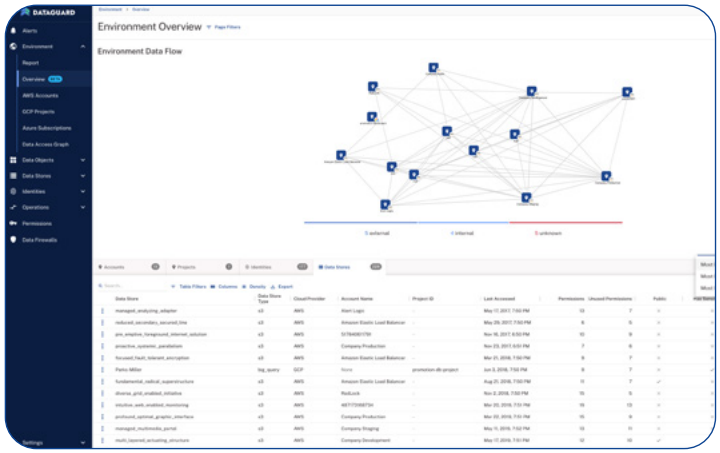
- Understanding and learning how the incident occured allows organizations to better protect, mitigate, and prevent future security incidents and breaches.
- Analyst investigation and response man-hours drastically reduced by using advanced data science behind Identities, permissions, operations and data to correlate risky and anomalous behavior

About Symmetry Systems DataGuard

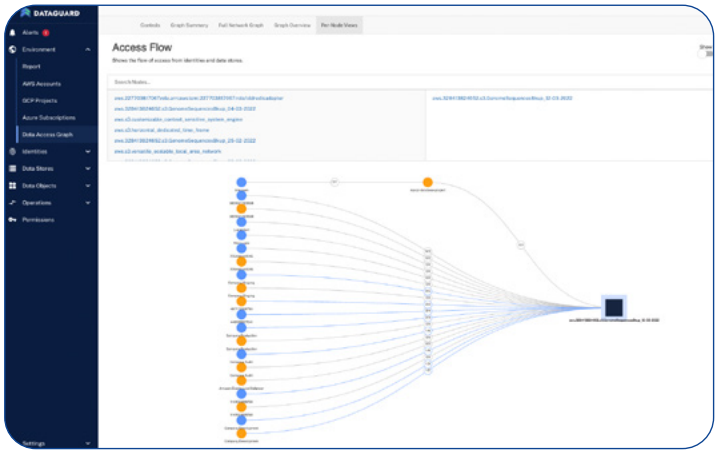
Symmetry's DataGuard is a hybrid cloud data security solution that provides a data-centric approach to enable organizations to map, secure and track identity, permissions, and data flows – **at scale in multi-cloud environments** while providing unified visibility across these environments for cloud- and information security teams.

DataGuard provides a cloud **Data Security Posture Management (DSPM)** solution that unifies visibility into data objects across all data stores, answering data security and compliance questions that **traditional cloud security tools cannot.** For example, what data is affected by a compromised credential, or an exploited web-service, or an off-boarded analyst?

DataGuard enables cloud and security operations to understand and systematically control data risk -- **defining the path to zero trust for data** -- while baking in compliance and incident response. DataGuard provides actionable insights into your data flow, unlike the traditional, static views offered by legacy technologies.



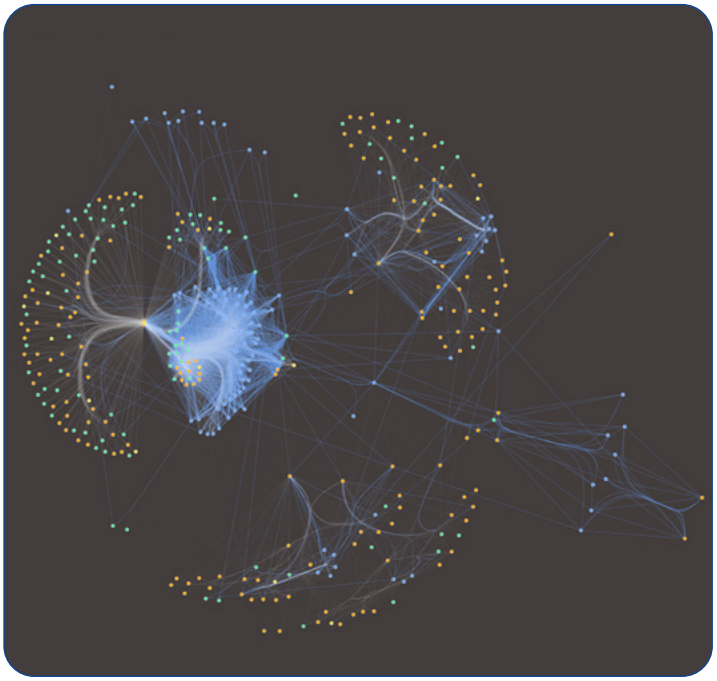
Top-down view into your data environments: filter by **most Data Stores, Permissions or Identities**

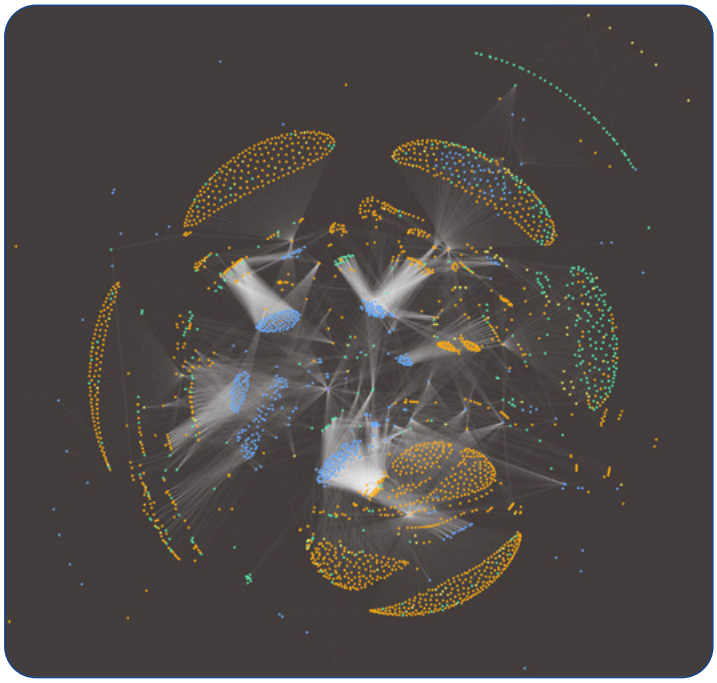


Easily track data flows: both in and out of your environments with high accuracy

Supports a variety of integrations out of the box, so you can track IAM, Alerts and Evidence

Vast cloud provider support: Amazon Web Services, Microsoft Azure, Google Cloud, on-premise environments





Cutting-edge visualizations produced by DataGuard to help you visualise your entire environment, blast radius and more

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

SYMMETRY SYSTEMS

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

LinkedIn / symmetry-systems-inc

Twitter / @SymmetrySystems