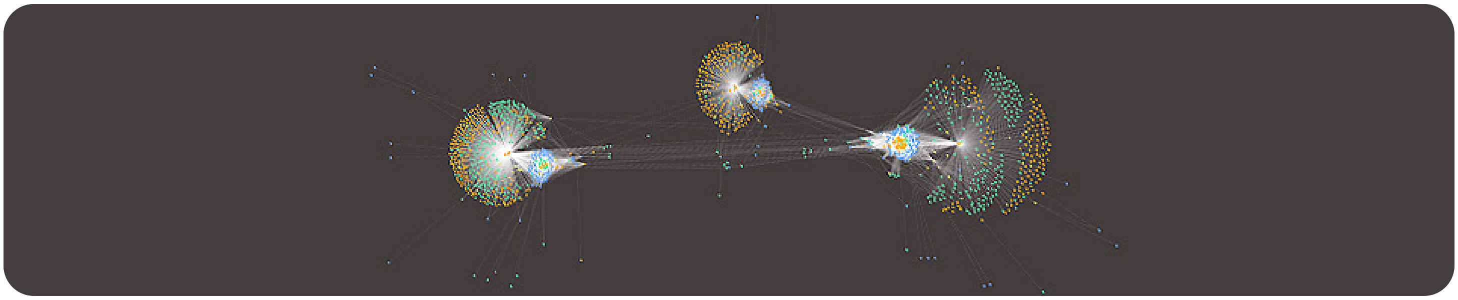
SYMMETRY SYSTEMS

Whitepaper

Digital Transformation/ Zero Trust

Are you hesitant to move workloads to the cloud due to the lack of visibility and usage of your sensitive data?

Adopting Zero Trust initiatives ensures no free flow of sensitive data is occurring, but how can you be sure?



Technical Requirements to Achieve Future State

Lift and Shift

- Ability to monitor all operations at the data object layer to ensure integrity
- Map direct and derived permissions to validate data access
- Monitor and visualize vendor permissions and operations

Continuous Visibility and Monitoring

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

Identify and Limit Blast Radius (Exposure)

- Visualize identities' operations against data and implement auto-generated IAM policies for reduction of blast radius

Automate context collection and response

- Ability to set Data Firewall Rules allowing alerting on anomalous behavior or access to sensitive data
- Utilizing Data Firewall Rules with SOAR, Ticketing systems, and Collaboration platforms via OOTB Integrations

Driving to Future State Requirements

Current Operations	Future Operations
Lift and Shift	
• Vague or no understanding if data integrity was compromised during digital transformation • On premise permission structure applied to a cloud environment creates unwanted permission impact • Workloads are assigned to third parties with unverified trust	• Comprehensive on all operations to ensure data integrity is not compromised • Clear visibility into direct and derived permissions to understand data access in cloud environment • Ability to trust, validate, and visualize third parties executing digital transformation project
Continuous Visibility and Monitoring	
• Manual process for contextualizing insights from multiple environments and vendors	• ML driven, automated process for receiving critical insights about your environment enabling Zero Trust
Identify and Limit Blast Radius (Exposure)	
• Approximation of blast radius based on combining multiple data points and vendors • Little insight into specific operations performed against sensitive data	• Clear and accurate picture of blast radius from the operations and data object layer • Tangible evidence on what operations are being taken against data to harden Zero Trust
Automate context collection and response	
• Using custom vendor integrations to construct Zero Trust detection and response	• Integrating data security alerts into SOAR, SIEM, and Collaboration platforms

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 around location and usage 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 in your applied Zero Trust architecture

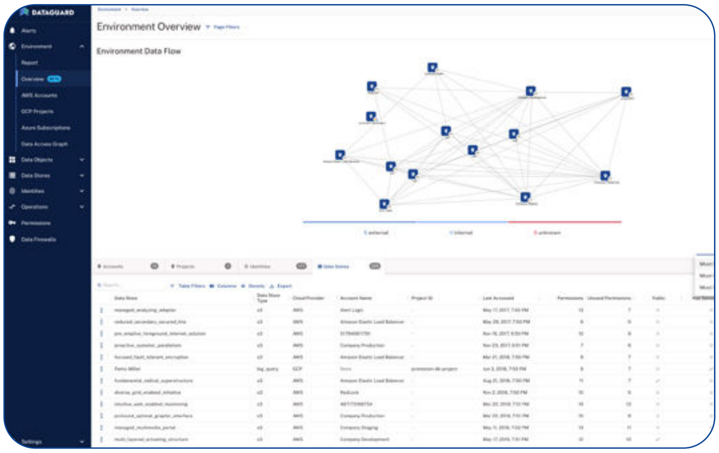
- An attacker's ultimate goal is to compromise your data. DataGuard provides security from the data out to support your Zero Trust architecture
- Implementing a Zero Trust architecture is incredibly challenging. DataGuard provides detailed visibility into what impact your Zero Trust architecture is making over time, enabling you to make informed decisions in your security posture, regardless of your Cloud Service Provider.

About Symmetry Systems DataGuard

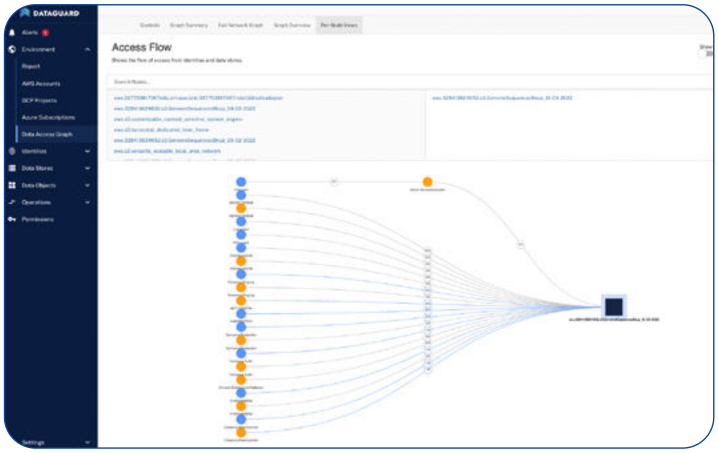
Symmetry's DataGuard is a hybrid cloud data security solution that provides a data-centric approach to enable organizations to map, secure and track identity, permissions, and data flows – **at scale in multi-cloud environments** while providing unified visibility across these environments for cloud-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

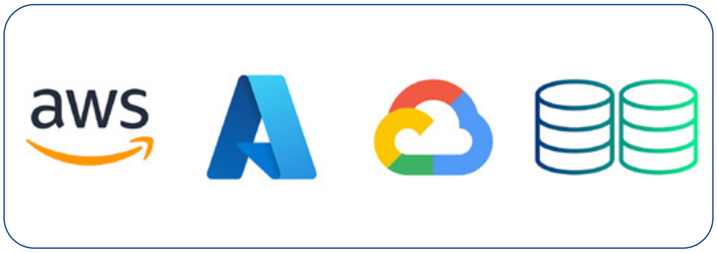
DataGuard enables cloud and security operations to understand and systematically control data risk -- **defining the path to zero trust for data** -- while baking in compliance and incident response. DataGuard provides actionable insights into your data flow, unlike the traditional, static views offered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



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

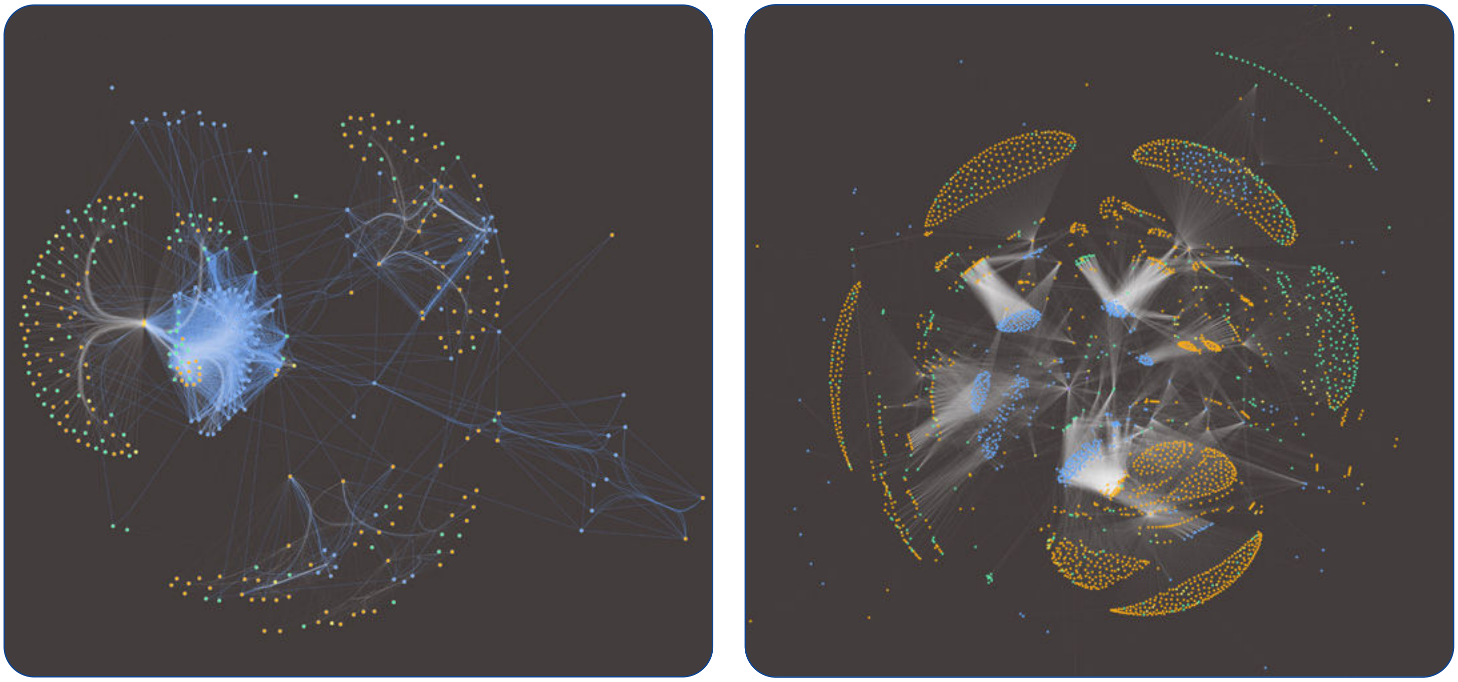


Easily track data flows: both in and out of your environments with high accuracy



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