Solution Brief

SYMMETRY SYSTEMS

Zero Trust and Data Security Posture Management (DSPM)

Key Challenge

The adoption of cloud-based technology and the greater mobility that comes with it means today's organizations are faced with additional challenges, such as securing data at scale, maintaining compliance, and managing complex permissions and identities. Organizations also need to monitor and understand the attack surface of countless individual data objects and maintain the right level of privileges for all identities that access data, whether directly or through applications. In the cloud, perimeter-based defense solutions no longer suffice to secure sensitive and mission-critical data.

Solution

Businesses are adopting Zero Trust strategies and architecture to secure their data and systems. Data Security Posture Management (DSPM) helps businesses adopt the Zero Trust philosophy at the data object layer across the enterprise by effectively managing both the complexity and scale associated with protecting sensitive and mission-critical data.

Zero Trust at a Glance

The goal is to prevent unauthorized access to data and services and make access control enforcement as granular as possible. Zero Trust presents a shift from a location-centric model to a more data-centric approach for fine-grained security controls between users, systems, data, and assets that change over time.

Source https://www.cisa.gov/zero-trust-maturity-model

Adapting to numerous disparate cloud environments creates challenges for businesses trying to manage identities and permissions to data. Businesses find themselves having to oversee the complexity and scale of applications, the countless identities in use, and the petabytes of data–much of which may be highly sensitive– being processed and stored daily. Security misconfigurations and non-configured controls are inevitable when operating at this scale. Increased authentication is meaningless, if access to data is unauthenticated.

And even when organizations can reliably enforce cloud infrastructure security, the issue of "excessive privileges" remains, challenging the best efforts to implement and maintain Zero Trust. The traditional approach of assigning data access rights based on ease and impact avoidance is incompatible with a Zero Trust architecture, particularly when focused on single data objects. Actively restricting data access to specific identities requires an understanding of not only whether a specific identity has access to a given datastore, but also the specific operation that identity can and is taking against a single data object within that datastore.

Why Zero Trust?

Zero Trust is based on the principle of "Never trust. Always verify." Zero Trust is most often applied as a security framework for securing data, systems, and infrastructure within an organization. It involves strict identity authentication, permissions, and continuous validation requirements for all users, devices, systems, and data. Symmetry Systems aligns its Zero Trust solutions to NIST guidelines, with specific focus on continuous verification, minimizing the blast area, and reducing the number of over-privileged users.

Key Benefits of DSPM & Zero Trust

- Achieve granular Zero Trust at the data object-level, including continuous identification and reduction of overprivileged users, excessive site reliability engineering (SRE) or top-level admin access rights with tighter controls and crossaccount or cross-cloud operations against data.
- Know the identity of every given account and device on a continuous basis, including the location and flow of sensitive and critical data. Confirm all user permissions are at the appropriate and correct level.
- Understand the specific operation an identity is taking against a single data object within a given datastore, and maintain records of how data items have changed over time.
- Obtain an accurate assessment and configuration of cloud native bi-directional permissions and achieve full visibility into all operations against data, not just “access” or “permissions” to that data.
- Alert and take action on precise operational evidence, through integrations within a given ecosystem of tools and solutions.
- Maintain full data asset inventory & data flow analysis, including detecting the presence of sensitive and confidential data and identification of dormant data.
- Reduce supply chain risk by managing over-privileged vendors, partners, contractors, and third-parties to ensure that only necessary access permissions have been granted. Ensure contractors, vendors, and third-parties are properly off-boarded.
- Pinpoint gaps in micro-segmentation policies that create vulnerabilities.
- Analyze derived permissions to understand how secondary user permissions or toxic permission combinations might increase cyber risk exposure.
- Ensure data operations are no longer being executed after remediation.

Solution Overview

Data Security Posture Management allows security teams to ensure their data is protected following Zero Trust principles. Using a DSPM solution, like Symmetry Systems' DataGuard, security teams can continuously monitor and adjust identity access management (IAM) policies on individual data objects at scale. This way organizations can make sure that only the right users and technologies have the right access to the right data, and that all user authentication is in line with Zero Trust requirements.

Symmetry Systems' DataGuard is a data security posture management (DSPM) solution designed to support and integrate within a fully operational Zero Trust architecture, including complete, data object-level understanding of:

What data do we have?

Where can the data be found?

Who has access?

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.

DSPM is critical to the successful adoption of a Zero Trust security model by continuously reducing the implicit trust before granting access to mission-critical data. DSPM allows organizations to determine whether a user needs access to data, with insights into each data object's sensitivity, permissions and operations.

Most businesses attempt to restrict access to sensitive data by focusing first on the identities and looking at what those identities have access to from the outside in. The problem with this approach is that permissions can be set both on the data object and the identity level–and unraveling data access manually is too complex for any organization to manage. DPSM extends the Zero Trust philosophy to hybrid cloud data stores by securing organizations from the data–or inside out."

About Symmetry Systems DataGuard

DataGuard arms security operations teams with a single source of truth about their data security posture and associated data risks across AWS, GCP, Azure, and on-premise environments–without having data ever leave their environment.

DataGuard allows security operations teams to build 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:

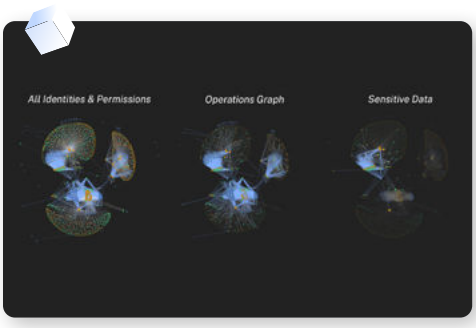
- **Where is sensitive data?**
- **Who has access to it?**
- **What operations have they performed against it?**

With DataGuard, security operations teams can improve their data security posture and outpace ever-growing data security risks and threats.

DataGuard and Zero Trust

- Reduce implicit trust and least privilege continuously to only the amount of access needed to the applications and data.
- Identify and lock down excessive data access permissions and privileges, to reduce threat actor ability to move laterally through your network.
- Understand the data blast radius of compromised identities and other insider threats quickly to take corrective or preemptive action.
- Provide executive visibility to cloud data sprawl, identity life cycle, Zero Trust violations, and sensitive data access to build security programs from the data-out.
- Accelerate Zero Trust adoption by continuously monitoring authorized access to data.
- Improve the security posture of sensitive data and cloud data stores.

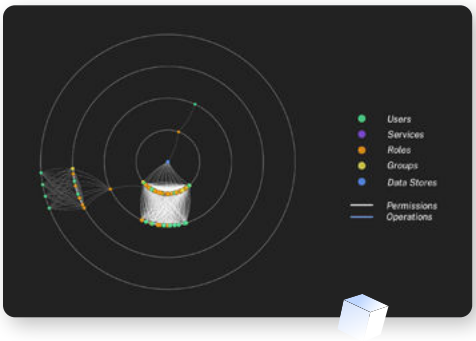
DataGuard Zero Trust DSPM Capabilities



Visualizing and Securing Data and Data Flow Across Environments

DataGuard is a DSPM solution that arms security operations teams with a complete understanding of their data, the identities that have access, and the operations performed against that data.

For each data object, DataGuard combines each of these elements to provide unique insights to help prioritize data security risks and aid security teams in remediating their impact.

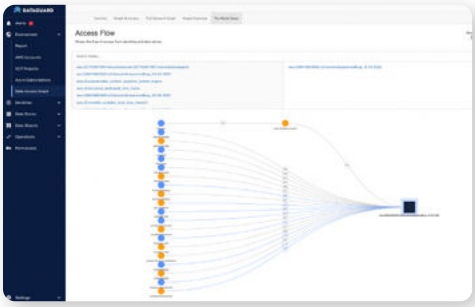


Reducing the Data Blast Radius from Insider Threats, Vendors, and Third Parties

DataGuard is able to enumerate all users and technologies who are able to access each data object, how they may use it, and have used it. Using machine learning DataGuard:

- **Identifies excessive, unused, or anomalous data.**
- **Enumerates paths to sensitive data.**
- **Determines data access and usage.**
- **Quantifies the potential data blast radius of accounts.**

Security teams use DataGuard to inform and control least privilege IAM permissions, reduce data sprawl, and proactively get alerted to anomalous data behaviors. With DataGuard, security teams can stay ahead of threats and reduce the data blast radius through Zero Trust principles.



Anomalous Data Behavior Monitoring and Alerting

DataGuard detects current and historic anomalous data access and usage, alerting security teams in a timely manner with precision. Security teams can use DataGuard to investigate Zero Trust policy violations, potential data breaches, ransomware attacks, and other cyber threats as quickly as possible.

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**