SYMMETRY SYSTEMS

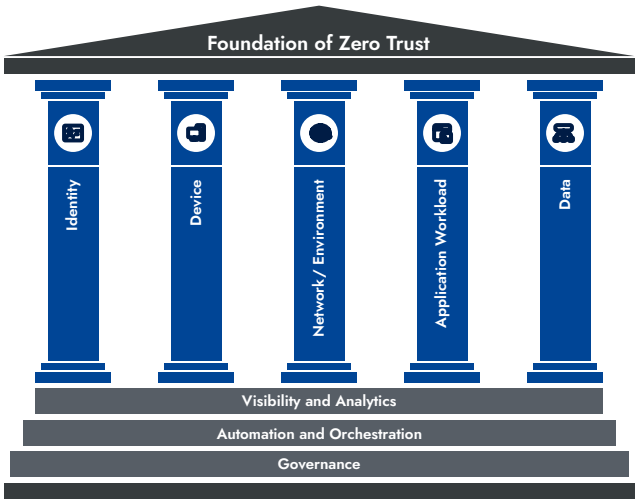
White Paper

How Symmetry Dataguard Accelerates Your Zero Trust Maturity

What Is CISA's Zero Trust Maturity Model?

CISA's Zero Trust Maturity Model is a roadmap for federal agencies to reference as they transition towards adhering to Executive Order M-22-09 and work to optimize their Zero Trust architecture. The maturity model, which includes five pillars and three cross-cutting capabilities, is based on the foundations of Zero Trust.

The five distinct pillars identified by CISA for Zero Trust implementation in their Zero Trust Maturity Model are:



Source: CISA Zero Trust Maturity Model

Identity: An attribute or set of attributes that uniquely describe an agency user or entity.

Device: Any hardware asset that can connect to a network, including internet of things (IoT) devices, mobile phones, laptops, servers, and others.

Network/Environment: An open communications medium, including agency internal networks, wireless networks, and the Internet, used to transport messages.

Application workload: Applications and workloads include agency systems, computer programs, and services that execute on premise, as well as in a cloud environment.

Data: Agency data should be protected on devices, in applications, and networks.

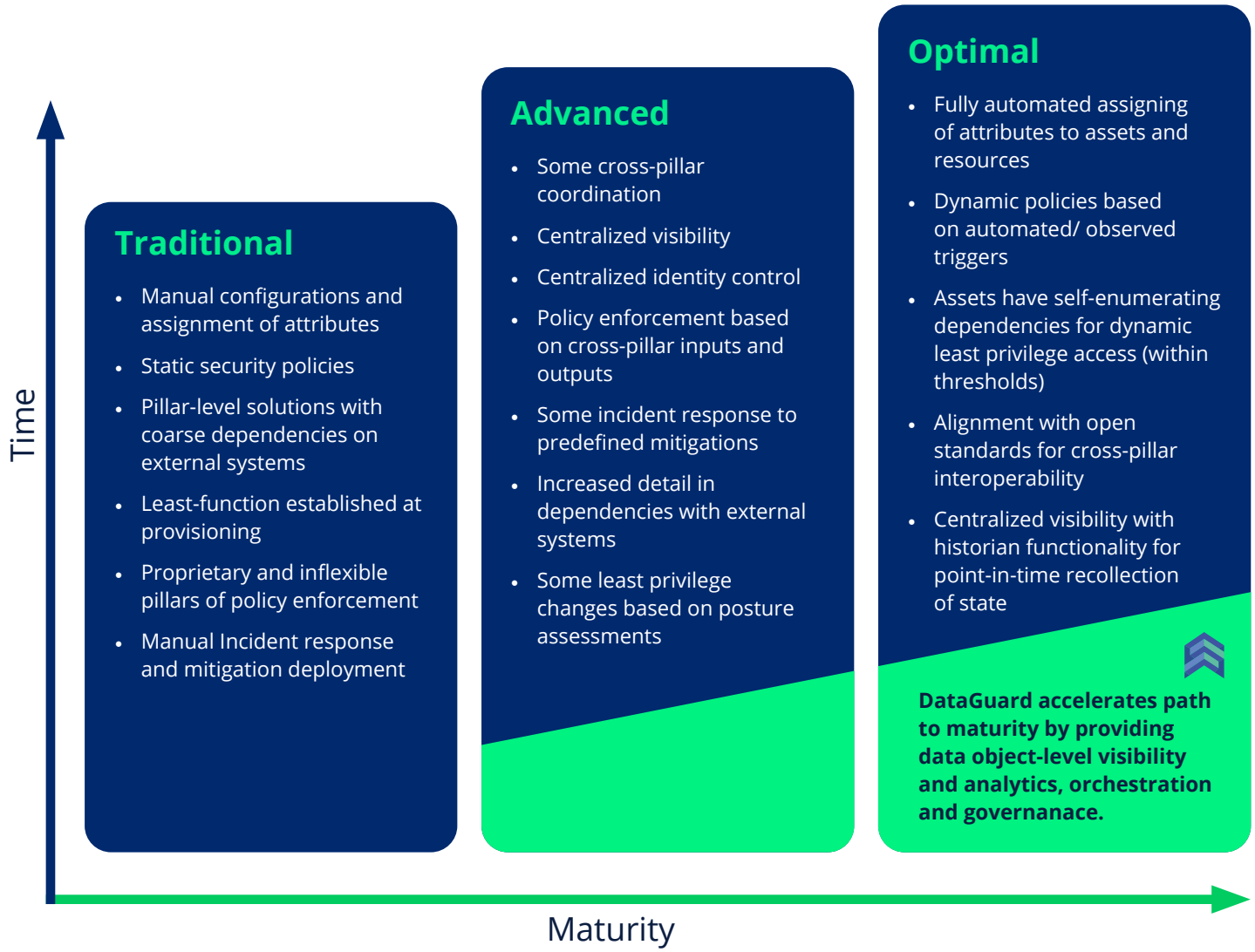
Zero Trust at a Glance

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*

How Is Zero Trust Maturity Measured?

With the understanding that Zero Trust is an incremental process that will take years to implement, CISA has outlined three maturity stages for each pillar:



How DataGuard Accelerates Your Zero Trust Maturity

Symmetry Systems' DataGuard allows agencies to accelerate their path to maturity and adopt optimal Zero Trust implementations sooner. This acceleration is possible by providing:

- **Visibility and analytics into data and data flows at a granular object level, in a way that had not been possible before.**
- **Automation, orchestration, and governance of identities and data access.**

This allows agencies to increase reliance upon automated processes and systems, providing a stable platform to integrate into other pillars of Zero Trust and become more dynamic in their policy enforcement decisions. Within each pillar, the maturity model further provides agencies with specific examples of a traditional, advanced, and optimal Zero Trust architecture.

DataGuard Alignment to the Identity Pillar

Symmetry Systems DataGuard allows security teams to identify identities with access to their data and continuously validate that the identities with access are following Zero Trust principles. Least privilege access, which underpins Zero Trust, depends both on the ability to assure the identity of the entity receiving access and guarantee that the right granularity of access is considered when assigning access. With DataGuard security teams can continuously monitor and adjust identity access management (IAM) policies on individual data objects, at scale, based on actual user behavior. This way they can make sure that only the right users and technologies have the right access to the right data, and that authentication for those users are in line with CISA Maturity Model requirements, as well as identify anomalous user behavior.

Identity	Traditional	Advanced	Optimal	SYMMETRY SYSTEMS
Authentication				Agencies can use DataGuard to continuously monitor identities that have permissions to data to ensure they are compliant with authentication policies.
Identity Stores				Agencies can use DataGuard to assess cloud and on-premise identities that have access to data.
Risk Assessment				Agencies can use DataGuard and its machine learning capabilities to identify anomalous behavior at the data object layer.
Visibility and Analytics Capability				Agencies can use DataGuard to provide centralized visibility into users, permissions, and the data operations they perform.
Automation and Orchestration Capability				Agencies can use DataGuard to proactively and dynamically adjust data access policies based on group memberships.
Governance Capability				Agencies can use DataGuard to implement and monitor access policies on data based on agency defined rules.

DataGuard Alignment to the Device Pillar

Symmetry Systems' DataGuard allows security teams to identify identities accessing data without routing through traditional access points or changes in devices being used by authorized users to access data. In addition, DataGuard provides granular information to determine what access may require differing trust levels and therefore device posture, based on the sensitivity or mission critical nature of the data being accessed.

Device	Traditional	Advanced	Optimal	SYMMETRY SYSTEMS
Data Access				Agencies can use DataGuard to monitor access to data and utilize machine learning to identify anomalous access patterns, including devices and IP addresses used.

DataGuard Alignment to the Network Pillar

Symmetry Systems DataGuard helps agencies gain a precise and accurate understanding of their assets, users and data flows, and the protections that they have applied or may need to apply. As agencies look to migrate toward a Zero Trust posture, they will need to align their network segmentation and protections according to the needs of their application workflows and **resultant data flows,** instead of the implicit trust inherent in traditional network segmentation. In addition, DataGuard provides visibility and analytics capabilities to allow security teams to proactively discover anomalous behavior and automate alerts and triggers based on out-of-the-box data firewall policies and custom rules.

Network	Traditional	Advanced	Optimal	SYMMETRY SYSTEMS
Network Segmentation				Agencies can use DataGuard to identify and monitor ingress/egress at the most granular data object level based on the data operations and data flows within their environments.
Threat Protection				Agencies can monitor access to data and utilize machine learning to identify anomalous access patterns, including geolocations and IP addresses used.
Visibility and Analytics Capability				Agencies can use DataGuard to create and monitor data object-level telemetry, create alerts, and integrate into existing network and security monitoring systems
Automation and Orchestration Capability				Agencies can use DataGuard to proactively and dynamically adjust data access policies based on data classification and other data attributes.
Governance Capability				Agencies can use DataGuard to automate discovery and remediation of unauthorized entities with access to sensitive data.

DataGuard Alignment to the Application Workload Pillar

Symmetry Systems' DataGuard allows security teams to create and monitor data object-level telemetry without requiring application code changes.

Application — Traditional — Advanced — Optimal	SYMMETRY SYSTEMS
Access Authorization	Agencies can use DataGuard to enable security teams to create and monitor data object-level telemetry and integrate into existing threat protection processes and technologies without requiring application code changes.
Application Security	Agencies can use DataGuard to prioritize which applications should be subject to application security testing based on the sensitivity and volume of data being accessed through the application.
Visibility and Analytics Capability	Agencies can use DataGuard to create and monitor data object-level telemetry and integrate into existing security monitoring systems.
Automation and Orchestration Capability	DataGuard does not require application code changes to adapt to environmental changes as it maintains data object-level visibility.
Governance Capability	Agencies can use DataGuard to implement data protection policies on data based on agency defined rules, regardless of application controls.

DataGuard Alignment to the Data Pillar

DataGuard enables agencies to rapidly shift to a "data-centric" cybersecurity approach. With DataGuard, organizations can identify, categorize, and inventory data assets with precision and accuracy; ensuring that data protections and least privilege is enforced for their most critical data assets (e.g., high value assets (HVAs)) are configured and continually enforced.

Data — Traditional — Advanced — Optimal	SYMMETRY SYSTEMS
Inventory Management	Agencies can continuously inventory their data and monitor data flow across their environments using DataGuard.
Access Determination	Agencies can use DataGuard to dynamically adjust data access policies based on continual risk based determinations based on data classification, identity posture, and permissions and operations.
Encryption	Agencies can use DataGuard to monitor the encryption state of data objects in the cloud or on premise.
Visibility and Analytics Capability	Agencies can use DataGuard to maintain complete visibility of the agency's data, access events, and other suspicious behavior.
Automation and Orchestration Capability	Agencies can use DataGuard to implement access, manage backups, and administer other security requirements on data based on sensitivity.
Governance Capability	Agencies can use DataGuard to fulfill data protection policies on data based on agency defined rules, regardless of data source.

Conclusion

With DataGuard, organizations now have the visibility, analytics, and governance tools needed to accelerate their **Zero Trust network architecture and maturity.** Organizations can identify with precision and accuracy the right amount of access required by authenticated users and continuously monitor the effectiveness of their Zero Trust architectures based on the flow of data within their environment.

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 is 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.

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