Implementing Zero Trust Strategy

Introduction to securing data with Zero Trust principles in cloud environments.

Introduction to Zero Trust Data

Zero trust data is a security model that requires all data to be encrypted and secured, regardless of where it resides.

It assumes that all data is untrusted by default.

One of the basic tenets of zero trust is to remove the implicit trust in users, services, and devices based only on their network location, affiliation, and ownership.

.

Introduction to Zero Trust Strategy

1.

Defining Zero Trust

- Every user, device, and app treated as untrusted.
- Evolves from traditional perimeter defenses to proactive security.

2.

Key Principles of Zero Trust

- Verify identity and least privilege access.
- Implement micro-segmentation and continuous monitoring.

3.

Evolution of Cybersecurity Models

- Shift from perimeter-based to Zero Trust approach.
- Adapts to dynamic cyber threats for enhanced resilience.

Key Principles of Zero Trust Data

Data encryption

All data at rest and in transit should be encrypted

Least privilege access

Only authorized users should have access to sensitive data

Data provenance

Know where your data comes from and where it goes

Continuous validation

Validate user access and data integrity continuously

Following these principles ensures your data is secure even in cloud environments.

Zero Trust Domains

1. User Identity
2. Device
3. Application
4. Data
5. Networks
6. Workloads

Zero Trust Data

Zero Trust Data Component	Mayhem Shield Message Implementation
4.1 Data Catalog Risk Assessment Multi-mission capability	Fully decentralized architecture enables policies to be matched to risk/clearance of project
4.2 DoD Enterprise Data Governance Simplified operations	Real time monitoring of creation-movement-access of protected data
4.3 Data Labeling & Tagging Easier application support	Every block of encrypted data is identified by the unique label which is generated using quantum entropy
4.4 Data Monitoring & Sensing Data exfiltration monitor	Agents track location of data as it is moved and report back to policy server
4.5 Data Encryption & Management Improved system performance	Crypto agile encryption enables different algorithms based on risk (post quantum) or data type (voice, video, data)
4.6 Data Loss Prevention (DLP) Reduced data leakage	Content is scanned during encryption process to reduce risk of data leakage
4.7 Data Access Control Coalition data sharing	Access to protected data is only allowed after policy verification: identity, location, token, time, server type

Implementation Framework

Data Integrity in Zero Trust Architecture

Zero Trust is a process more than a product. Therefore it helps to have a framework so that progress can be tracked and goals appointed. The Nist Framework and by extension, the CMMC Level 2 controls list, provide an excellent guide to mature a Zero Trust Posture.

NIST as an implementation Framework

NIST Special Publication 800-207 has laid out a comprehensive set of zero trust principles and referenced zero trust architectures (ZTA) for turning those concepts into reality.

NIST SP 800-171

“Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations."

The NIST SP 800-171 publication outlines requirements for protecting Controlled Unclassified Information (CUI) in non-federal systems and organizations. It is often referenced in contracts with the U.S. government.

.

NIST

NIST Recommends a 7-step Process to Establish a Cybersecurity Program:

- Prioritize and Scope.
- Orient.
- Create a Current Profile.
- Conduct a Risk Assessment.
- Create a Target Profile.
- Determine, Analyze and Prioritize Gaps.
- Implement Action Plan.

Getting Started with Zero Trust

Determine the key goals and outcomes you want to achieve from adopting zero trust, such as improving security, reducing risk, or enabling remote access.

Take an inventory of all assets, users, devices, and data flows across your IT environment to understand gaps and priorities.

Define granular access policies based on least privilege principles and multi-factor authentication for all users and devices.

Architect network & data segmentation, microperimeters and private access to limit lateral movement and isolate critical assets.

Implement continuous monitoring across all assets and users to maintain visibility and quickly detect threats.

NIST CheckList

Nist has 110 Controls

Use this controls checklist.

Nist has 110 Controls

1. Access controls 2. Awareness and training 3. Auditing and accountability 4. Configuration management 5. Identification and authentication 6. Incident response 7. Maintenance

8. Media protection

9. Personnel security

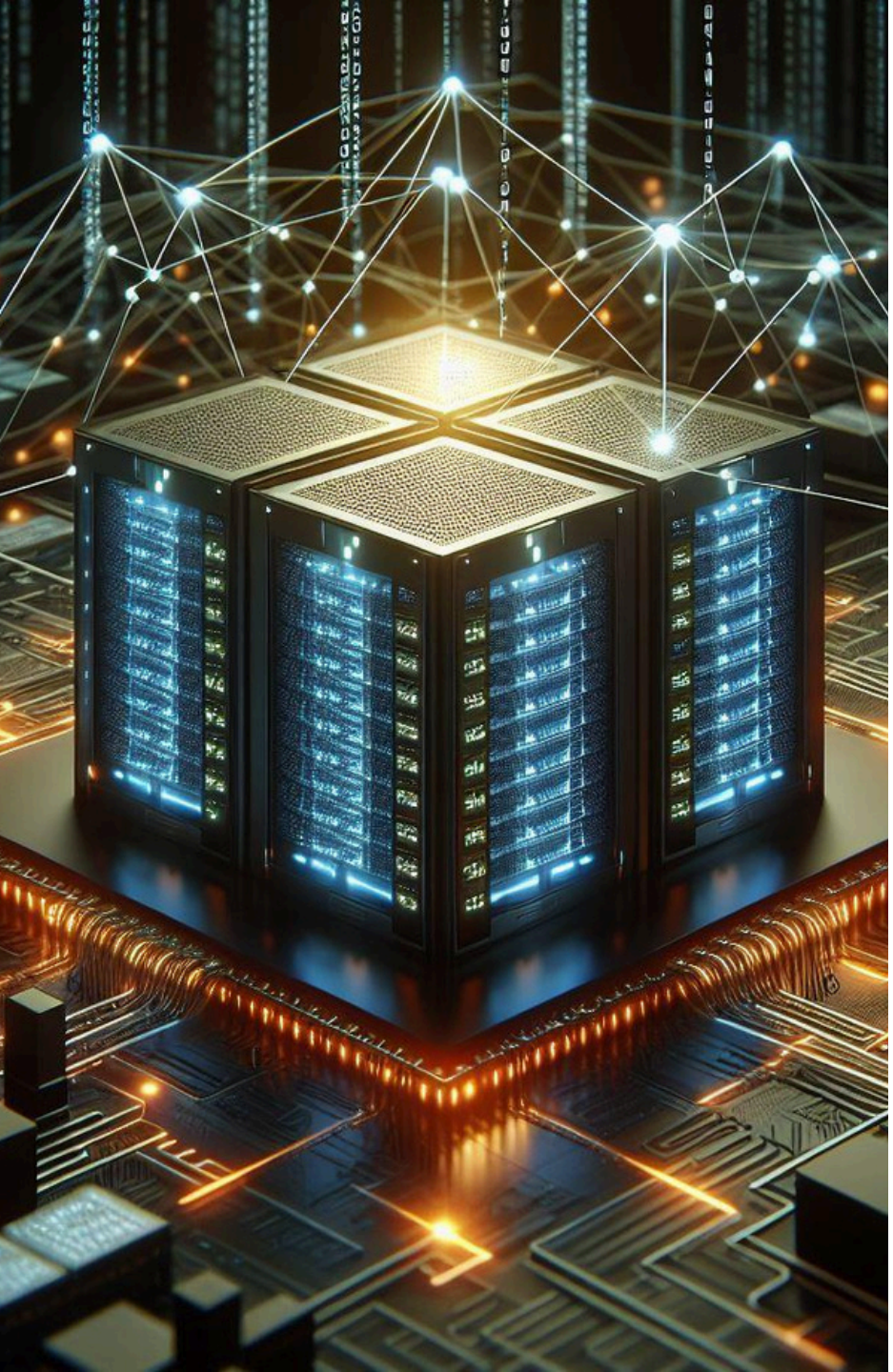
10. Physical protection

11. Risk assessment

12. Security assessment

13. System and communications protection

14. System and information integrity



Zero Trust Domains

Identify Domain Solutions

- For each domain, identify a key partner

Prioritize

- Data, network, identity are good places to start

Automated Governance and Continuous Monitoring

- Regularly monitor network activity
- Quickly detect and respond to security incidents

NIST Best Practices

1. Define and Classify CUI (Controlled Unclassified Information)
2. Implement a Least Privilege Model
3. Audits and Alerts for Changes in CUI
4. Verification of Access Changes

Next Steps

1. Define goals
    a. Zero Trust Data
    b Zero Trust Network
    · Zero Trust Identity
    c
2. Internal Assessment
    a. Download the 110 controls and see how they map to Mayhem Shield capabilities. Use this document to build your compliance profile.
3. Strategy Plan