Zero Trust Security

Tim Morrow

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM22-0484

Agenda

Foundations

Architecture

Implementation

Guidance

Assessment Considerations

Acronyms

References

Zero Trust Security

Foundations

Overview

Security model developed by John Kindervag and team at Forrester approximately 2009.

Goals

- Remove implicit trust.
- Move security from the network to users, applications, and workloads.

Principles

Ensure all resources are accessed securely, regardless of location.

Adopt a least privilege strategy and strictly enforce access control.

Inspect and log all traffic.

Ensure all components support application programming interface (API)s for event and data exchange.

Automate actions across environments and systems, driven by context and events.

Deliver tactical and strategic value.

[Zero Trust Security 2021]

Working Definition

A zero trust system is an *integrated security platform* that uses *contextual information* from identity, security and IT infrastructure, and risk analytics tools to inform and enable the *dynamic enforcement of security policies uniformly across the enterprise*.

Zero trust shifts security from an ineffective perimeter-centric model to a *resource- and identity-centric model*. As a result, organizations can continuously adapt access controls to a changing environment, obtaining improved security, reduced risk, simplified and resilient operations, and increased business agility.

[Zero Trust Security 2021]

Platform Requirements –1

1. Data plane communications must be encrypted. Any exceptions must be deliberate (e.g., domain name system (DNS)).
2. The system must be able to enforce access controls for all types of resources. Access control mechanisms must be driven by identity-centric and contextual policies.
3. Data resource protections should be able to use identity and contextual policies to control access.
4. The system and policy model must support securing all users in all locations. The policy model and controls must be consistent for remote and on-premise users.
5. Devices must be able to be inspected for their security posture and configuration prior to being granted access, and periodically thereafter.

[Zero Trust Security 2021]

Platform Requirements –2

6. It must be possible to distinguish BYOD* from corporate-managed devices and control the level of access accordingly.
7. Access to any network resource must be explicitly granted by policy. No user or device should inherently have broad network access.
8. Access controls must be able to distinguish between different services on the same network resource. For example, access to HTTPS must be granted separately from access to SSH.
9. Access to specific data elements contained within the applications or containers that have different classifications must be enforced based on business policy.
10. Network traffic metadata must be logged and enriched with identity context.

* bring your own device

[Zero Trust Security 2021]

Platform Requirements –3

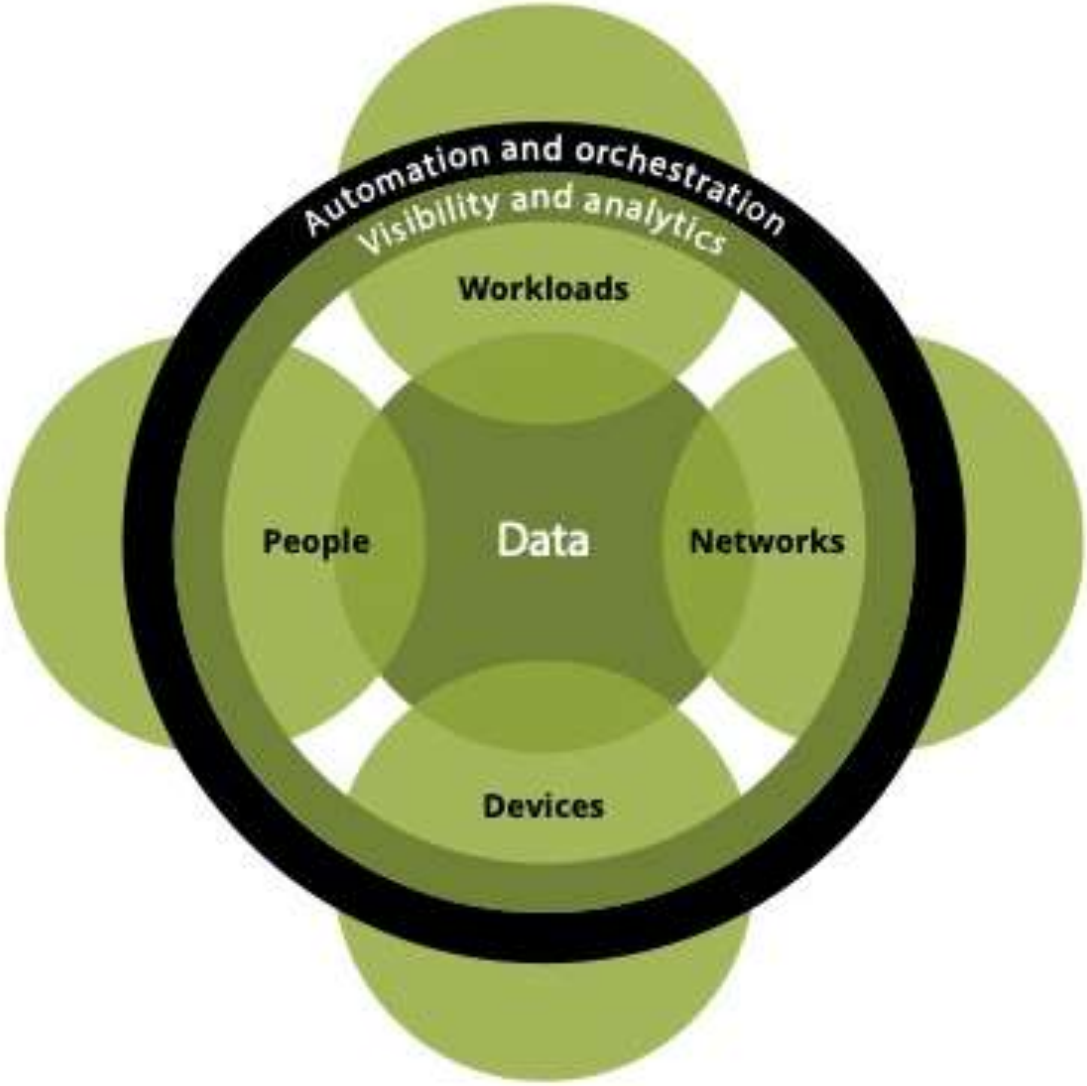
11. Network traffic must be able to be examined for security and data loss purposes.
12. Workloads transferred into the cloud should include the same access control policies as defined by on-premises solutions.
13. Automation must include identity-centric details to provide efficient and effective incident response.
14. Logs must be included in analytics tools for effective and dynamic enforcement of policies.

[Zero Trust Security 2021]

Zero Trust Security

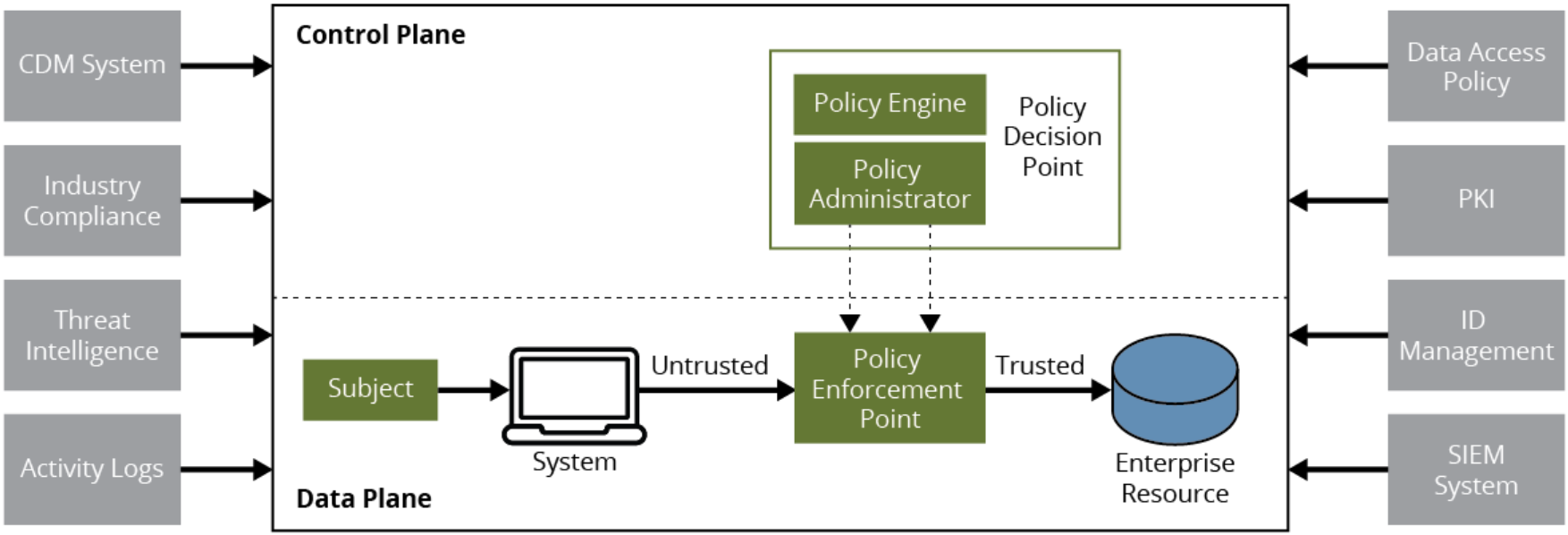
Architecture

Forrester Zero Trust eXtended (ZTX) Model



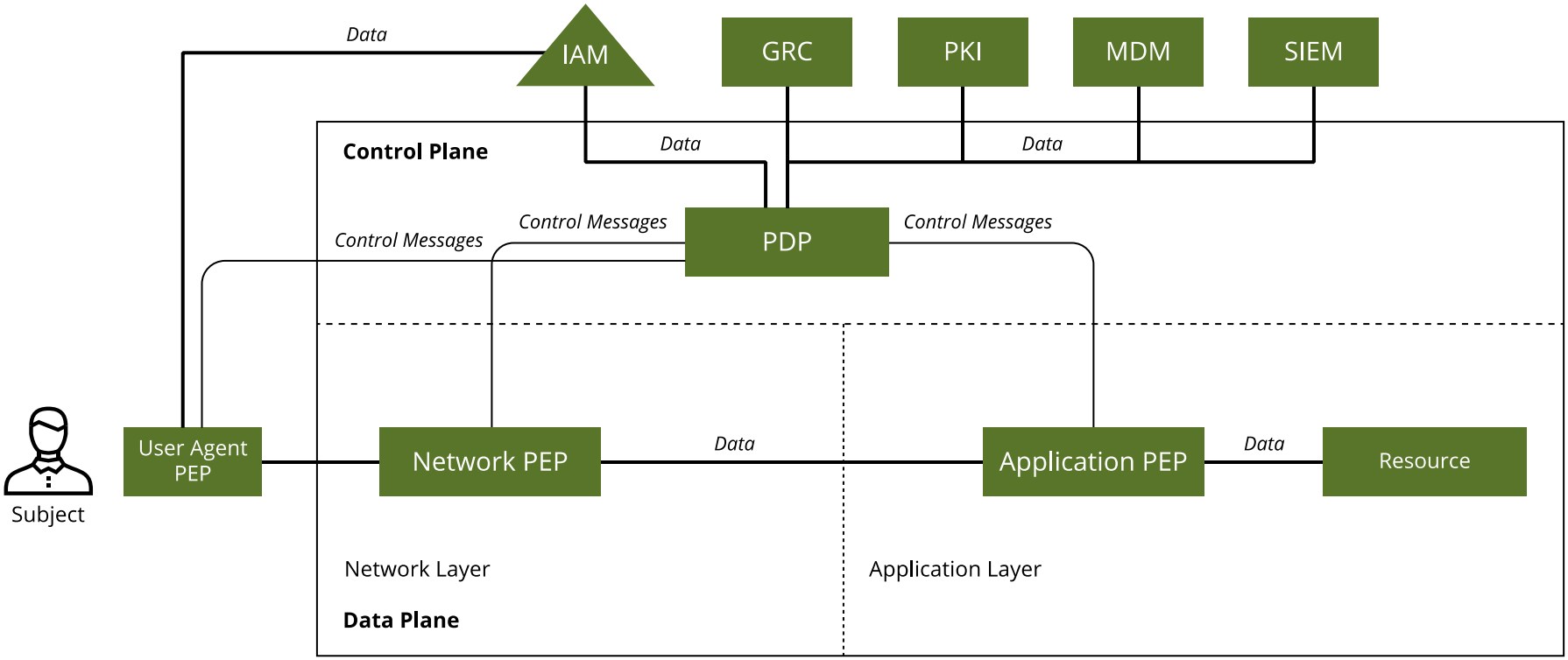
[ZTX 2019]

NIST Zero Trust Architecture Components



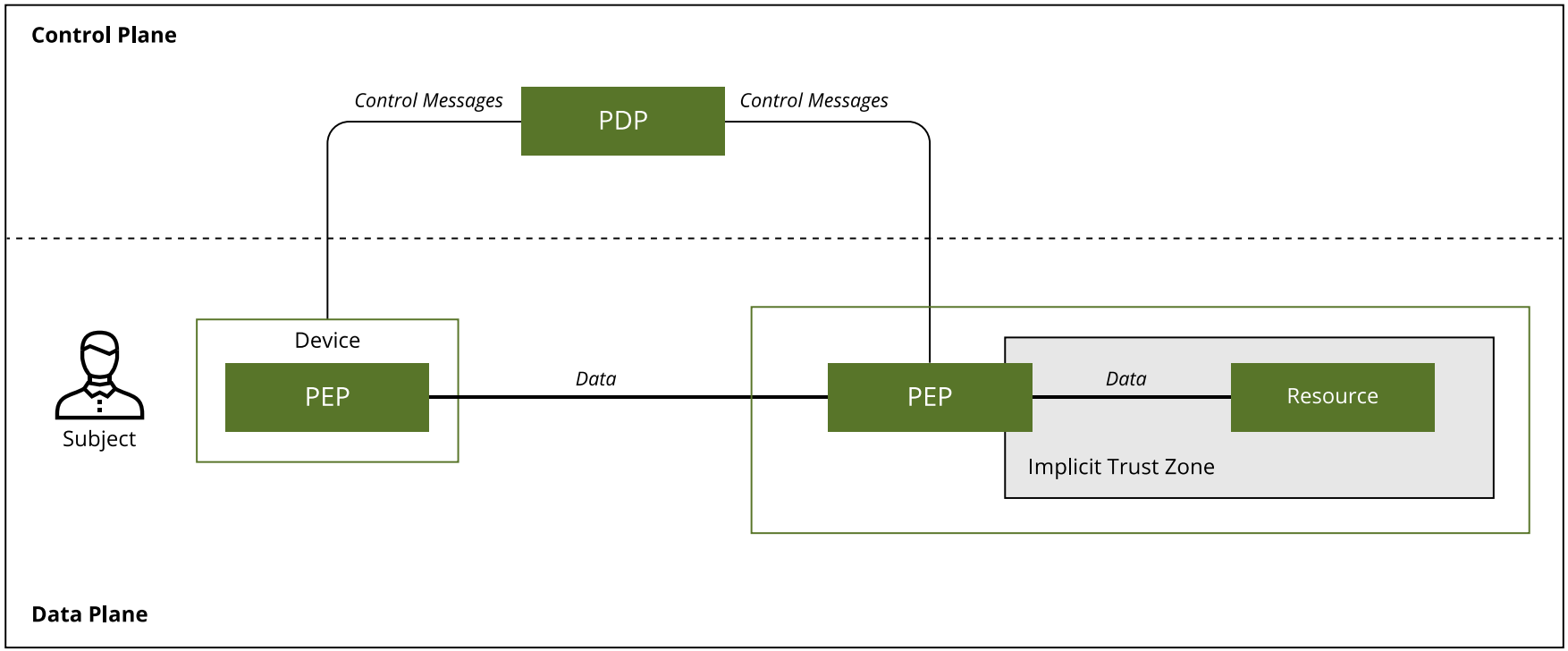
[NIST 800-207 2020]

Policy Enforcement Point Types



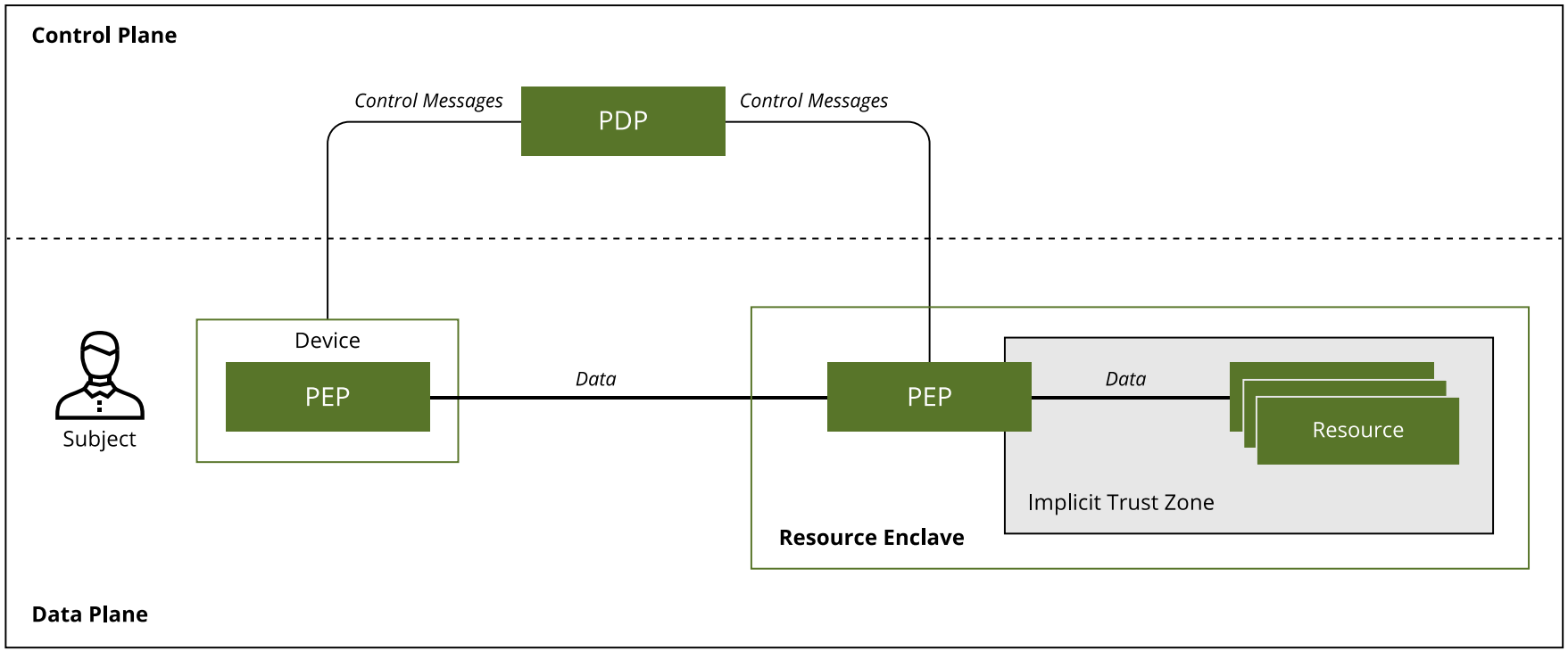
[Zero Trust Security 2021]

Resource-Based Deployment Model



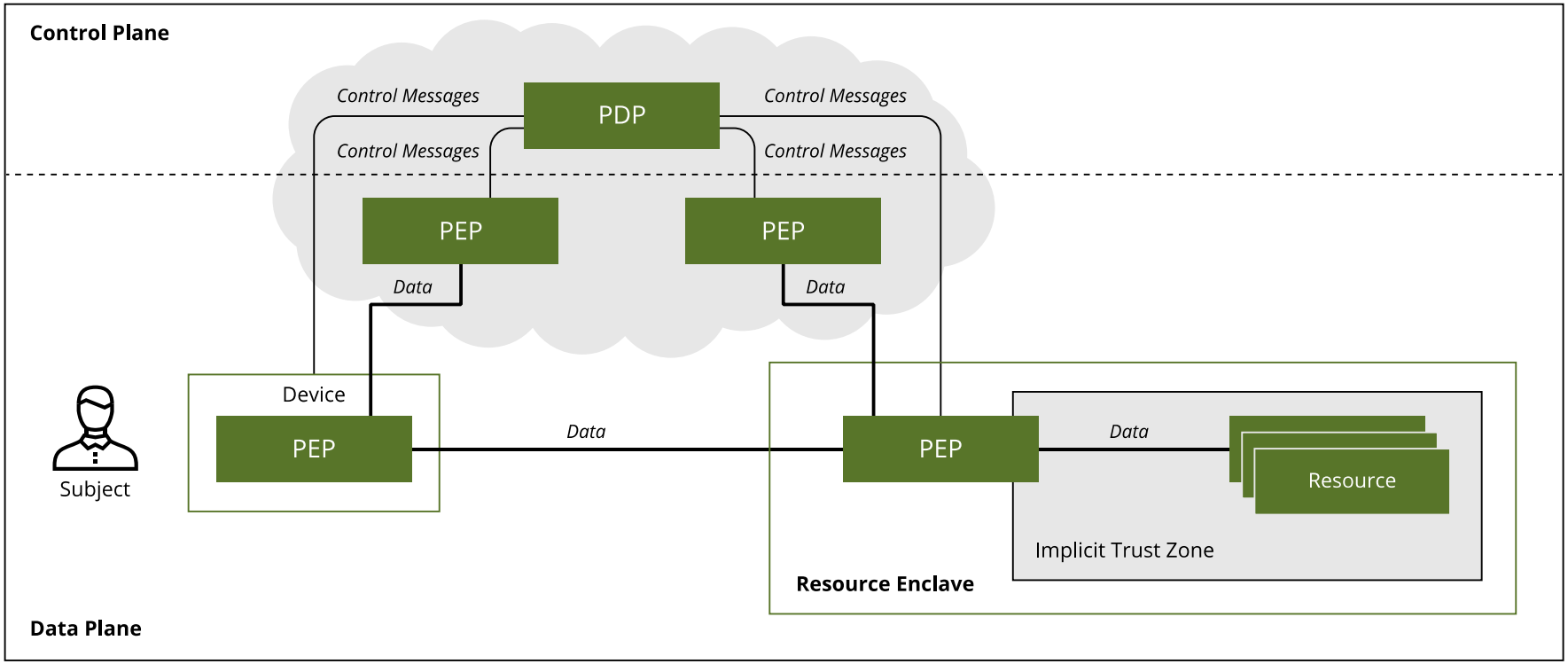
[Zero Trust Security 2021]

Enclave-Based Deployment Model



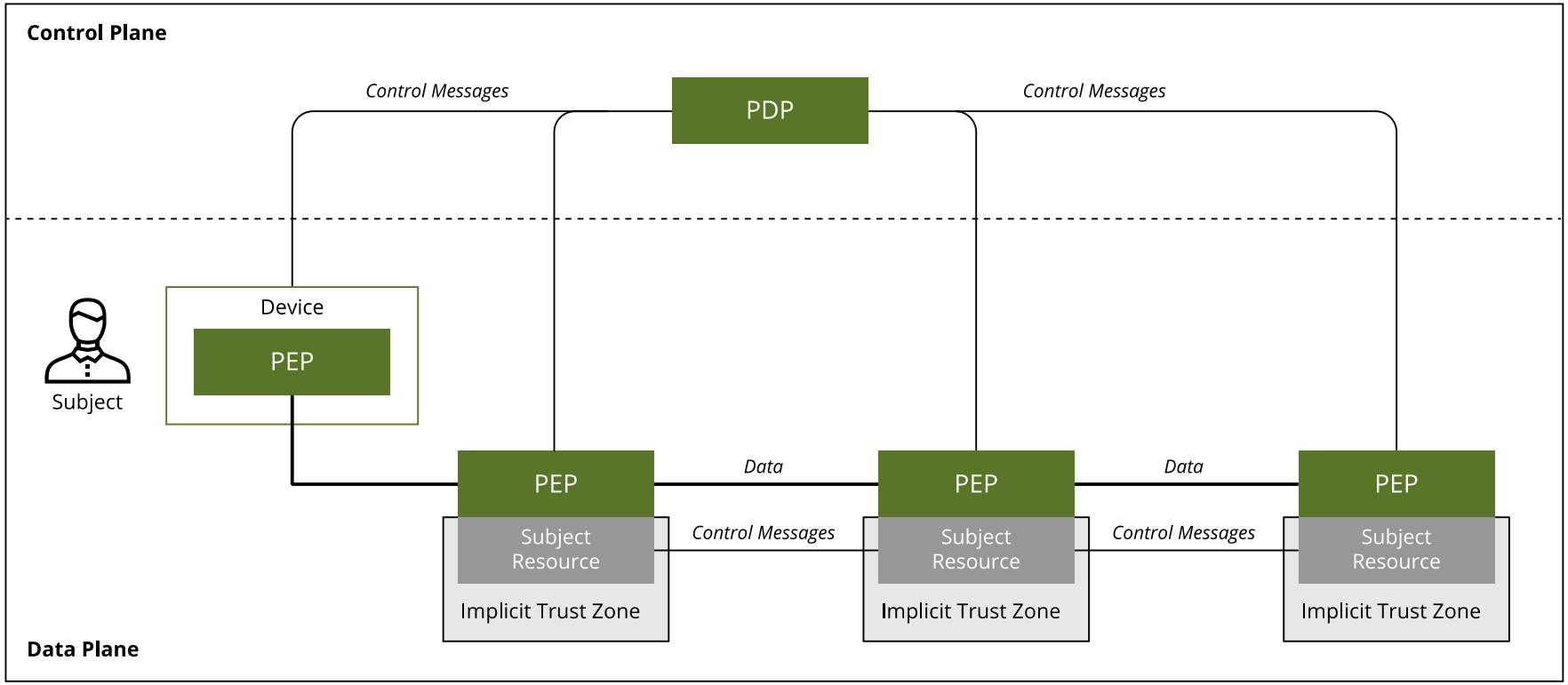
[Zero Trust Security 2021]

Cloud-Routed Deployment Model



[Zero Trust Security 2021]

Microsegmentation Deployment Model



[Zero Trust Security 2021]

Threats

1. Subversion of zero trust architecture (ZTA) decision process
2. Denial-of-service or network disruption
3. Stolen credentials/insider threat
4. Visibility on the network
5. Storage of system and network information
6. Reliance on proprietary data formats or solutions
7. Use of non-person entities (NPEs) in zero trust architecture administration

[NIST 800-207 2020]

NIST 800-207 Threat Mapping - 1

Zero Trust Architecture Threat	Components and Inputs	Proposed Mitigation
Subversion of ZTA Decision Process	Policy Engine Policy Administrator	Configuration Management Monitoring Detection
Denial-of-Service or Network Disruption	Policy Enforcement Point Policy Engine Policy Administrator	Resilience
Stolen Credentials/Insider Threat	ID Management Data Access Policy	Architecture Contextual Trust Algorithm
Visibility on the Network	Activity Logs SIEM	Network Traffic Inspection Network Traffic Logging Metadata Machine Learning

[Zero Trust Adoption 2021]

NIST 800-207 Threat Mapping - 2

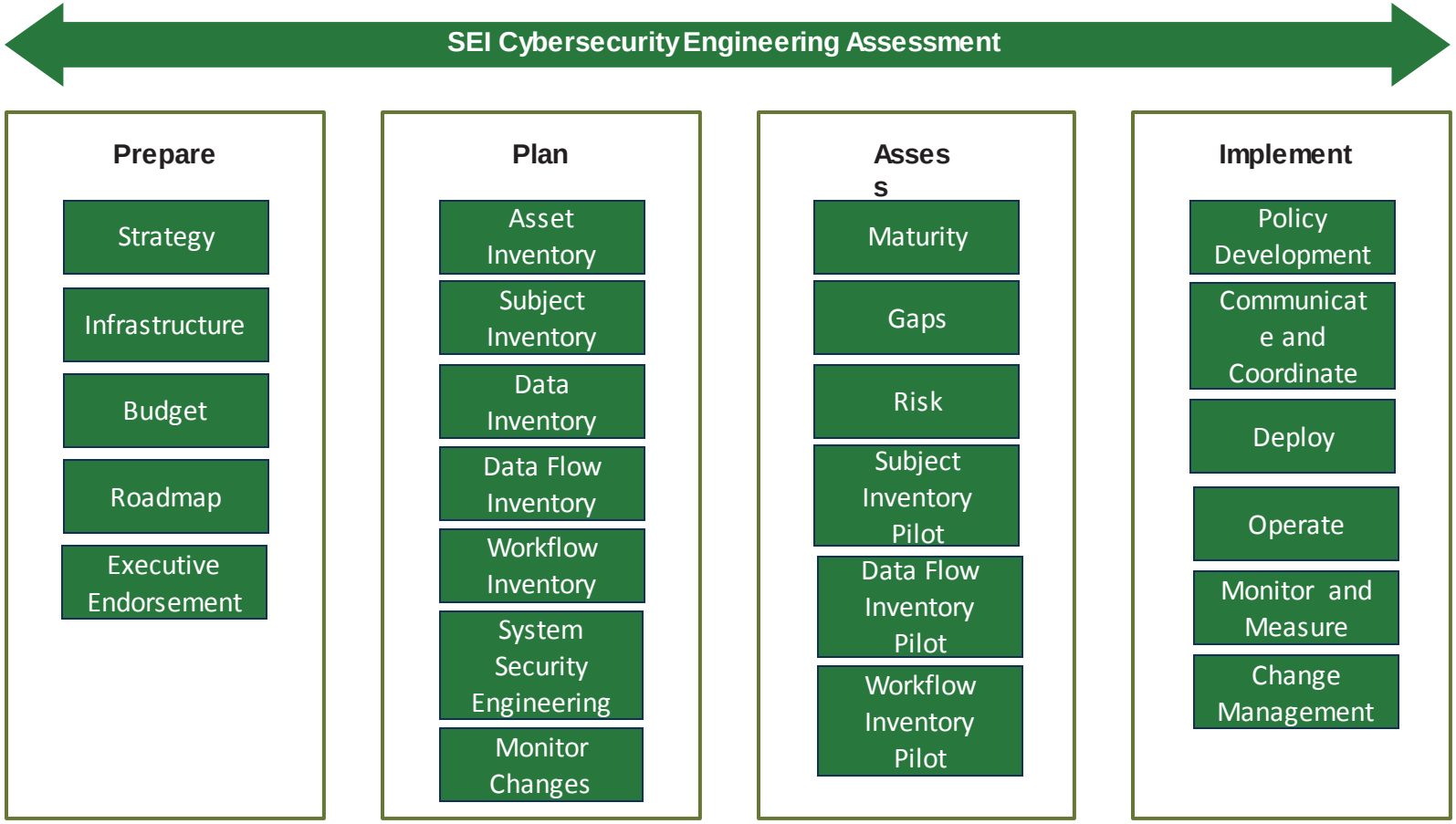
Zero Trust Architecture Threat	Components and Inputs	Proposed Mitigation
Storage of System and Network Information	Activity Logs CDM System Industry Compliance Data Access Policy PKI ID Management SIEM Information Policy Administrator Policy Engine	Restrictive Data Access Policies
Reliance on Proprietary Data Formats or Solutions	Activity Logs CDM System Industry Compliance Data Access Policy PKI ID Management SIEM Information Policy Administrator Policy Engine	Service Provider Evaluation Vendor Security Controls Enterprise Switching Costs Supply Chain Risk Management Performance Stability
Use of Non-person Entities (NPE) in ZTA Administration	Policy Engine Policy Administrator	Regular Retuning Analysis

[Zero Trust Adoption 2021]

Zero Trust Security

Implementation

SEI Zero Trust Journey



Implementation Technologies

Identity and access management (IAM)

Privileged access management (PAM)

Next generation firewalls (NGFW)

Security information and event management (SIEM)

Security orchestration automation and response (SOAR)

Software defined perimeter (SDP) (SDP is also called *zero trust network access* [ZTNA].)

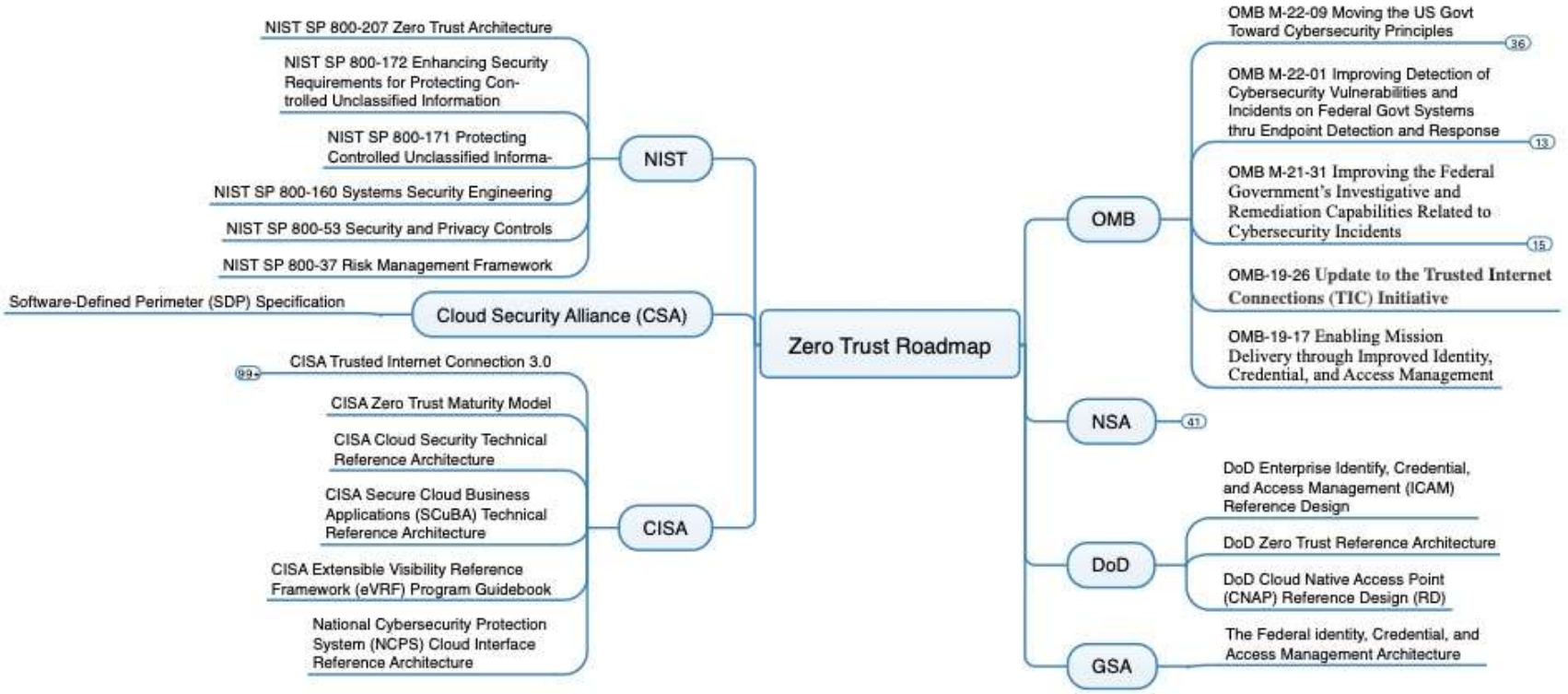
Cloud access security broker (CASB)

Microsegmentation

Zero Trust Security

Guidance

Zero Trust Guidance/Associated Documents



Zero Trust Security

Assessment Considerations

Resources

CISA

- Zero Trust Maturity Model
- High Value Asset Control Overlay

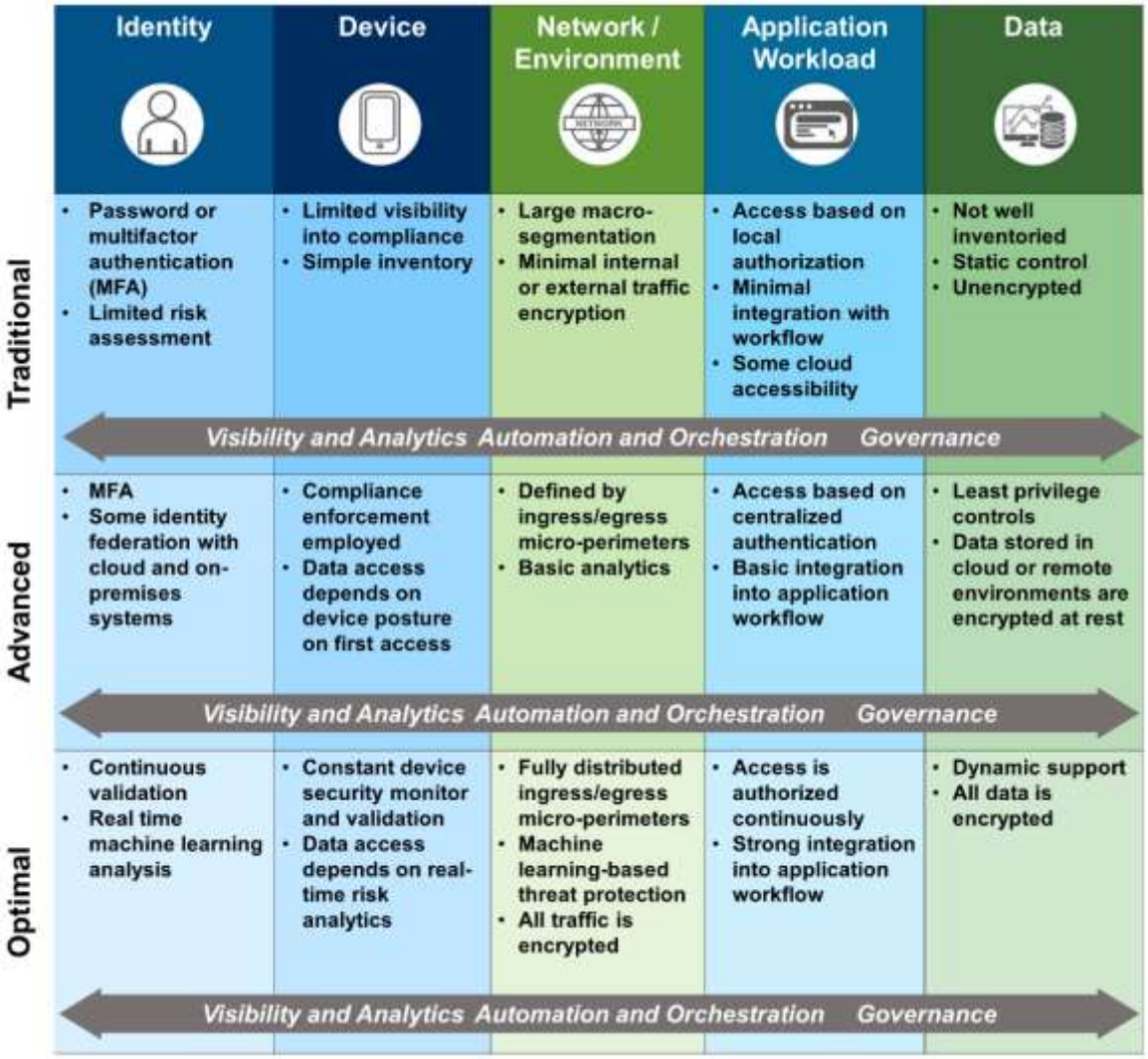
NSA

- Zero Trust Maturity Model

DoD

- Zero Trust Reference Architecture

CISA Zero Trust Maturity Model



[CISA ZTMM 2021]

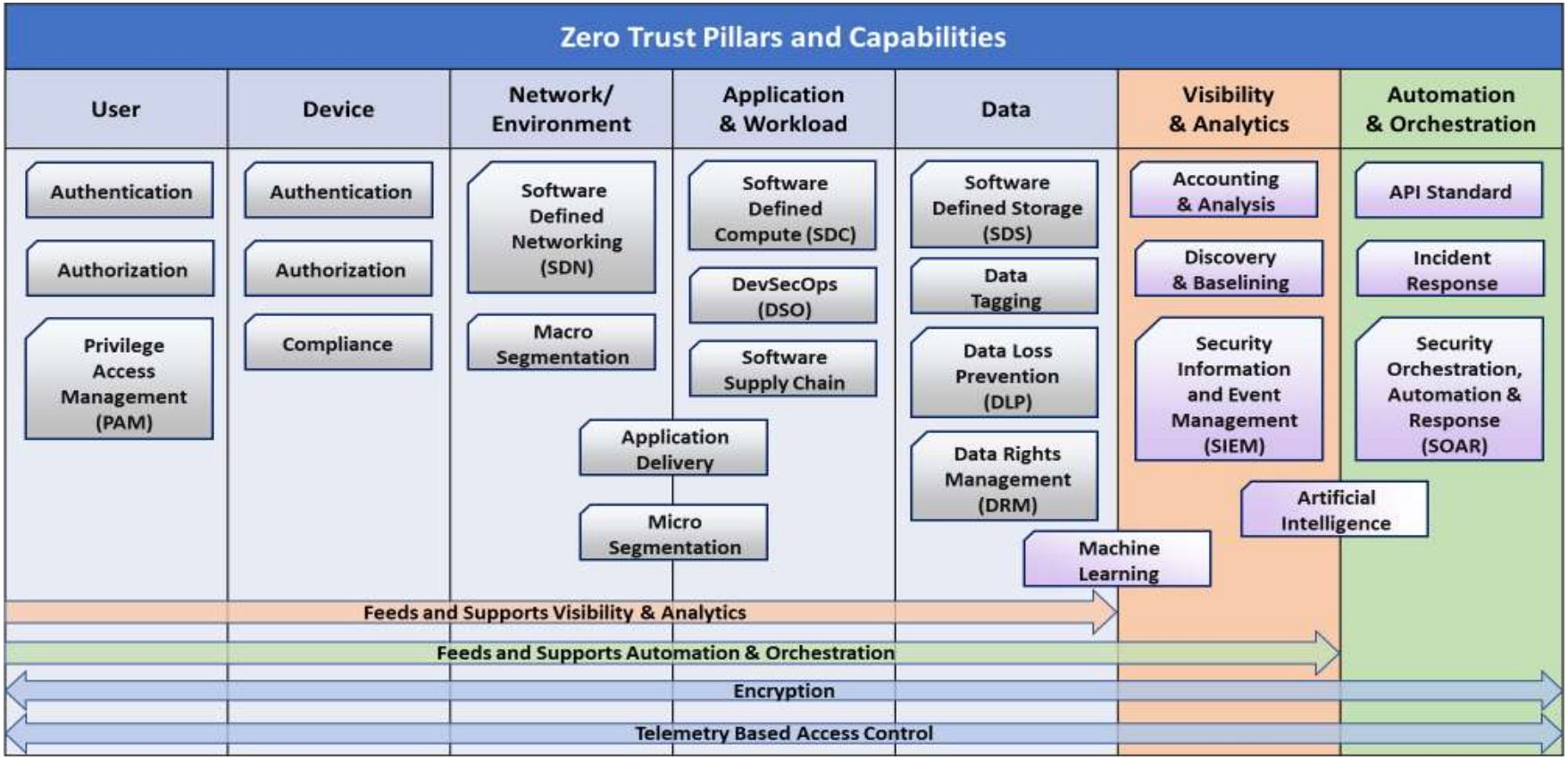
CISA ZT Maturity Model Function Tables

Function	Traditional	Advanced	Optimal
Authentication	Agency authenticates identity using either passwords or multi-factor authentication (MFA).	Agency authenticates identity using MFA.	Agency continuously validates identity, not just when access is initially granted.
Identity Stores	Agency only uses on-premises identity providers.	Agency federates some identity with cloud and on-premises systems.	Agency has global identity awareness across cloud and on-premises environments.
Risk Assessment	Agency makes limited determinations for identity risk.	Agency determines identity risk based on simple analytics and static rules.	Agency analyzes user behavior in real time with machine learning algorithms to determine risk and deliver ongoing protection.
Visibility and Analytics Capability	Agency segments user activity visibility with basic and static attributes.	Agency aggregates user activity visibility with basic attributes and then analyzes and reports for manual refinement.	Agency centralizes user visibility with high fidelity attributes and user and entity behavior analytics (UEBA).

Example: CISA Zero Trust Maturity Model Identity Pillar Functions

[CISA ZTMM 2021]

DoD ZTRA Pillars and Capabilities



[DOD ZTRA 2021]

DoD Zero Trust Maturity Model

Discovery

- Identify DAAS
- Map data flows
- Inventory User and Devices
- Identify privilege accounts
- Log network traffic

Assessment

- Determine compliance state leveraging existing hardening standards
- Determine proper account privilege levels
- Identify, if existing network/environment security policies as implemented in least privilege manner

Baseline

- Access to DAAS is determined by cybersecurity policy
- Networks are segmented with deny all/permit by exception
- Devices are managed and compliant to IT security policies
- Implement least privileged access
- MFA technologies are in use
- Begin data classification and tagging of critical data
- Meet encryption requirements

Intermediate

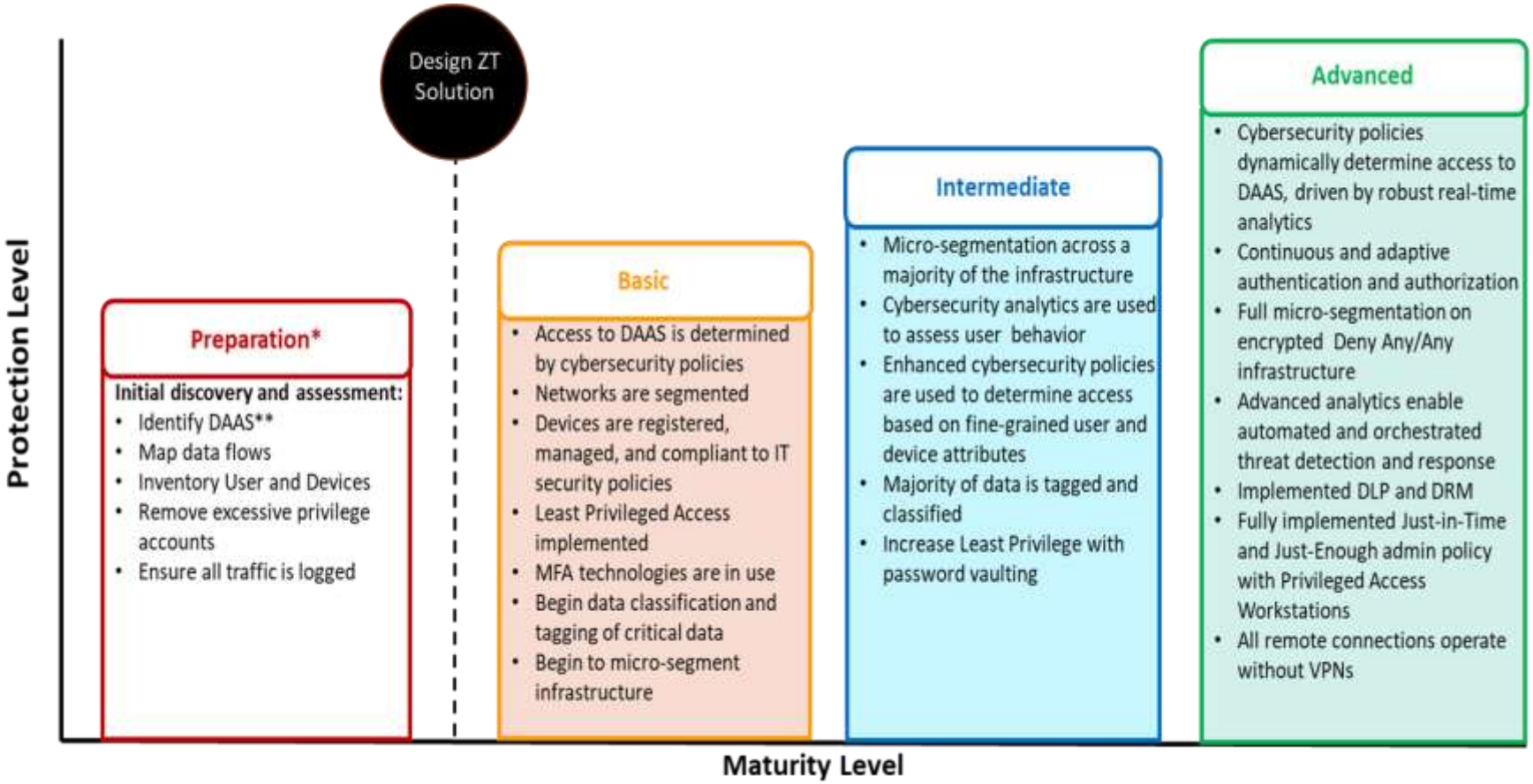
- Enhanced cybersecurity policies are used to determine access based on fine-grained user and device attributes
- Micro-segmentation across majority of network
- User identity based on Enterprise Federated Identity Service
- Enhance LPA with privileged access mgmt. solution
- Initial DLP and DRM implementations
- Data is tagged and classified via flow analysis and simple automation
- User and Entity Behavior Analytics (UEBA) to develop baseline

Advanced

- Cybersecurity policies dynamically determine access to DAAS, driven by robust real-time analytics
- Full micro-segmentation
- Continuous and adaptive authentication and authorization
- User and device identity based on Enterprise Federated Identity Service
- Fully implemented Just-in-Time and Just-Enough access policy
- Majority of data is tagged and classified through machine learning
- Full DLP and DRM implementation incorporating data tags
- Advanced analytics enable automated and orchestrated threat detection

[DOD ZTRA 2021]

NSA Zero Trust Maturity Model



[NMM-2022-01A1]

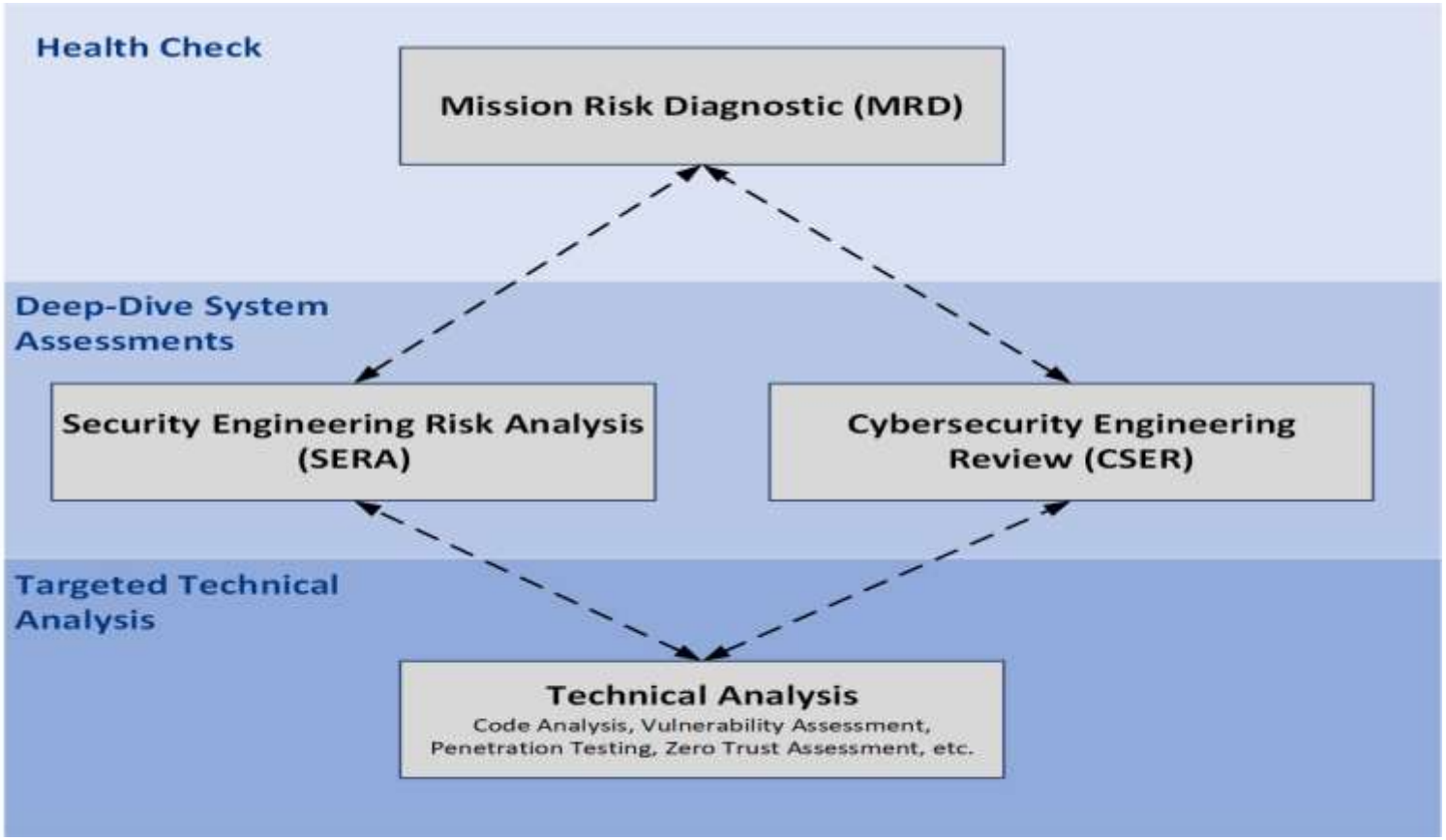
CISA High Value Asset Overlay

CISA High Value Asset Overlay Appendix 3 provides a NIST CSF function crosswalk with HVA controls.

Control	NIST Cybersecurity Framework Function				
	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
AC-2		X	X		
AC-2 (2)		X	X		
AC-3		X			
AC-3 (9)		X			
AC-4	X	X			
AC-5		X			
AC-6		X			
AC-6 (5)		X			
AC-6 (7)		X			
AC-17		X			
AC-17 (2)		X			
AC-20	X	X			
AU-2	X				
AU-6			X	X	

Example: CISA HVA Asset Overlay Controls Crosswalk

Cybersecurity Engineering Assessments



Zero Trust Security

Acronyms

Common Acronyms –1

API – Application Programming Interface

CASB – Cloud Access Security Broker

DNS – Domain Name System

DRM – Data Rights Management

FedRAMP – Federal Risk and Authorization Management Program

HVA – High Value Asset

IAM – Identity and Access Management

MFA – Multi-Factor Authentication

NGFW – Next-Generation Firewall

Common Acronyms –2

PA – Policy Administrator

PAM – Privileged Access Management

PDP – Policy Decision Point

PE – Policy Engine

PEP – Policy Enforcement Point

PKI – Public Key Infrastructure

SDN – Software Defined Networking

SDP – Software Defined Perimeter

Common Acronyms –3

SIEM – Security Information and Event Management

SOAR – Security Orchestration Automation and Response

SPA – Single Packet Authorization

ZTA – Zero Trust Architecture

ZTNA – Zero Trust Network Access

ZTRA – Zero Trust Reference Architecture

ZTX – Zero Trust eXtended

References

References –1

[CISA HVAO 2021]
Cybersecurity Infrastructure Security Agency. *High Value Asset Control Overlay, Version 2.0*. Washington, DC: CISA. 2021. https://www.cisa.gov/sites/default/files/publications/HVA%20Control%20Overlay%20v2.0_0.pdf

[CISA ZTMM 2021]
Cybersecurity Infrastructure Security Agency, Cybersecurity Division. *Zero Trust Maturity Model, Version 1.0*. Washington, DC: CISA. 2021. https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

[DOD ZTRA 2021]
U.S. Department of Defense. *Department of Defense Zero Trust Reference Architecture, Version 1.0*. Washington, DC: DOD CIO. 2021. https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf

[NIST 800-207 2020]
Rose, S.; Borchert, O.; Mitchell, S.; & Connelly, S. *NIST Special Publication 800-207: Zero Trust Architecture*. Gaithersburg, MD: NIST. 2020. https://csrc.nist.gov/publications/detail/sp/800-207/final

References –2

[NMM-2022-01A1]
National Security Agency. *National Manager Zero Trust Security Reporting Guidance and Cloud Migration Security Reporting Guidance*. 2022.

[Zero Trust Adoption 2021]
Sanders, G. "Zero Trust Adoption: Managing Risk with Cybersecurity Engineering and Adaptive Risk Assessment." *SEI Blog.* March 2021. https://insights.sei.cmu.edu/blog/zero-trust-adoption-managing-risk-with-cybersecurity-engineering-and-adaptive-risk-assessment

[Zero Trust Security 2021]
Garbis, J. & Chapman, J. *Zero Trust Security: An Enterprise Guide*. Berkeley, CA: Apress. 2021. https://link.springer.com/book/10.1007/978-1-4842-6702-8

[ZTX 2019]
Cunningham, C. *The Zero Trust eXtended (ZTX) Ecosystem*. Cambridge, MA: Forrester. (Subscription Only). 2019.