White paper Cisco public

Framework Mapping: Cisco Identity Services Engine+ CISA Zero Trust Model

Background

U.S. Public Sector organizations are embarking on a Zero Trust roadmap—a structured and phased approach to transition its cybersecurity framework toward a more mature and resilient Zero Trust Architecture (ZTA). This roadmap aligns with best practices outlined in the National Institute of Standards and Technology (NIST) Special Publication 800-207 and the Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model (ZTMM).

By leveraging these frameworks, U.S. Public Sector Organizations can adopt a comprehensive strategy to strengthen its security posture across all five CISA Zero Trust pillars—**Identity, Device, Network/Environment, Application Workload,** and **Data**.

1. **Identity:** Focuses on verifying and managing the identities of users, processes, and systems, ensuring access is granted only to authenticated and authorized entities based on least privilege principles.
2. **Device:** Ensures that all devices accessing the network are identified, monitored, and meet security compliance standards to reduce potential attack surfaces.
3. **Network/Environment:** Emphasizes secure network segmentation, dynamic access controls, and monitoring of traffic flows to limit lateral movement and protect resources within hybrid, cloud, and on-premises environments.
4. **Application Workload:** Protects applications and workloads by enforcing secure access, implementing runtime monitoring, and ensuring that interactions between applications are trusted and compliant.
5. **Data:** Focuses on protecting sensitive information through classification, encryption, monitoring, and policies that prevent unauthorized access or exfiltration.

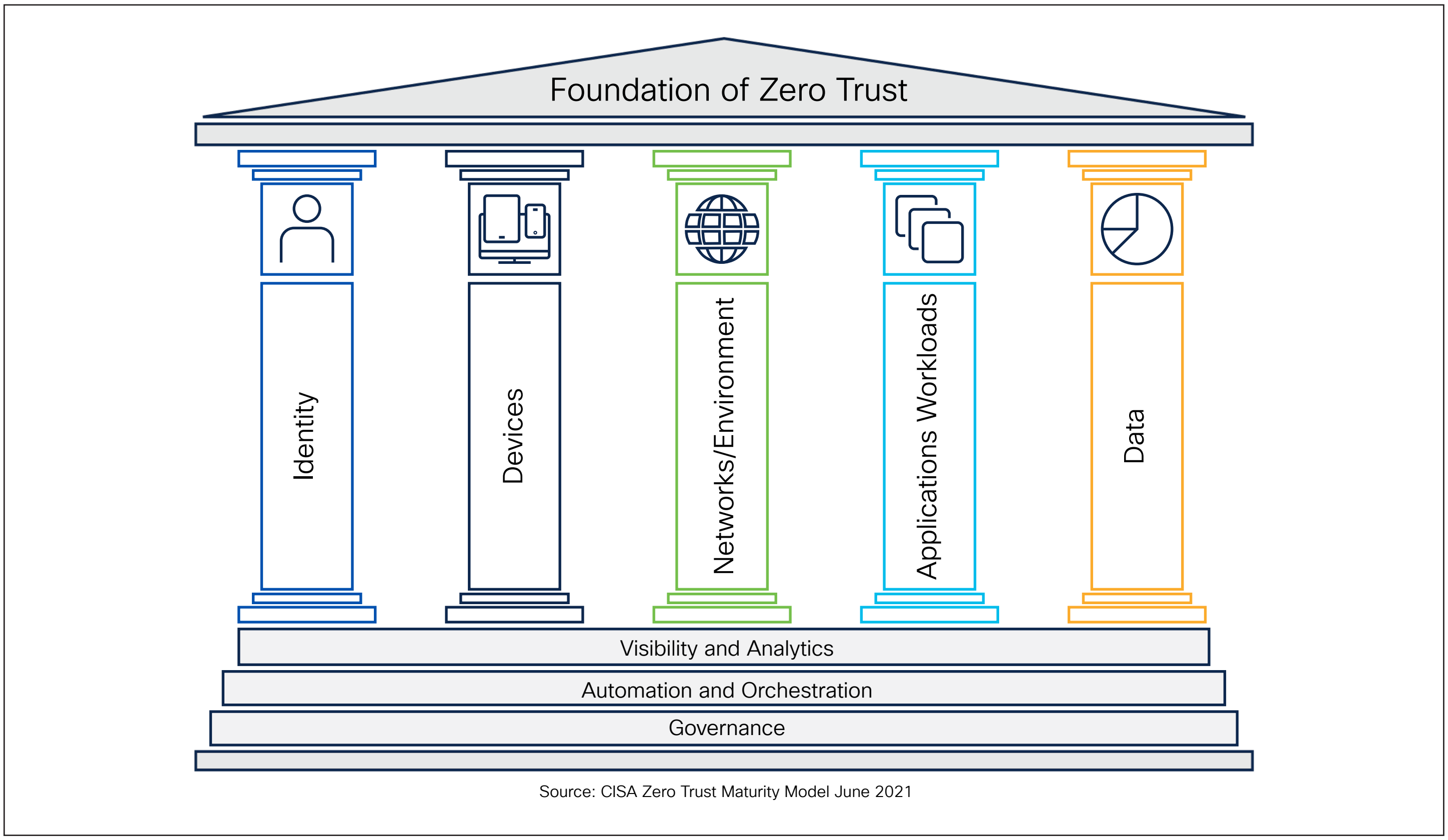
The CISA Zero Trust Model also builds on the foundational capabilities of the cross-cutting pillars with **Visibility and Analytics**,[1] **Automation and Orchestration**,[2] and **Governance**[3] which support (acts as the Pillar Base) and enhance the maturity of each core pillar.

Cisco® provides proven solutions for accelerating Zero Trust adoption. In this document we discuss how Cisco Identity Services Engine (ISE) meets the CISA ZTMM standard.

[1] **Visibility and Analytics** enable organizations to monitor and analyze behavior and events across the five pillars. This foundation capability provides the data-driven insights necessary to identify anomalies, detect threats, and enforce Zero Trust polices.

[2] **Automation and Orchestration** ensure that Zero Trust principles are implemented consistently and efficiently across the five pillars. By automating security tasks and orchestrating responses, organizations can reduce human error and improve reaction times to potential threats.

[3] **Governance** ensures that security policies, processes, and compliance requirements are well-defined and constantly applied across all pillars. It provides the overarching framework for decision-making, accountability, and adherence to organizational goals and regulatory mandates.



Source: CISA Zero Trust Maturity Model June 2021

Figure 1. CISA Zero Trust Maturity Model

Cisco ISE is a cornerstone of the U.S. Public Sector's Zero Trust strategy, excelling in the **Identity**, **Device**, and **Network** pillars of the CISA model. With its robust capabilities for identity management, device compliance enforcement, and network access control, Cisco ISE enables secure and dynamic access to critical resources. By ensuring that only authorized users and trusted devices can access the network, ISE reduces the risk of unauthorized access and lateral movement. Its ability to enforce role-based access controls (RBAC) and dynamic segmentation strengthens the alignment of Zero Trust principles to a Zero Trust security framework.

While Cisco ISE’s contributions to the **Application Workload** and **Data** pillars are indirect, it plays a vital complementary role by securing access to these resources through robust identity and device controls. ISE integrates seamlessly with other Cisco solutions to provide end-to-end visibility and enforcement, ensuring that security policies are consistently applied across the network. This comprehensive approach makes Cisco ISE an essential component of an organizations Zero Trust roadmap, helping the organization achieve a scalable and resilient security architecture that aligns with Zero Trust best practices and national standards.

Mapping to the CISA Zero Trust Five Pillars

Below is a mapping of Cisco Identity Services Engine (ISE) capabilities to the CISA 5 Pillars of Zero Trust and their corresponding functions, based on the information provided regarding its alignment with the DoD 7 Pillars of Zero Trust.

Table 1. Mapping Cisco ISE Capabilities to the CISA Zero Trust Identity Pillar

CISA Zero Trust Pillar	CISA Functions	Cisco ISE Capabilities	Notes
Identity	Enterprise Identity and Access Management	Conditional User Access	Cisco ISE ensures user authentication and access control based on dynamic conditions, contributing to enterprise identity and access management.
	Multi-Factor Authentication	Continuous Authentication	Cisco ISE supports integration with MFA solutions and continuously verifies user identity during ongoing sessions.
	Privileged Access Management	Privileged Access Management	Cisco ISE helps enforce access control policies for privileged users, ensuring they only access authorized resources.
	Least Privilege Access	Least Privilege Access	Cisco ISE enforces role-based access control (RBAC) to ensure users operate with the minimum privileges necessary.

Table 2. Mapping Cisco ISE Capabilities to the CISA Zero Trust Device Pillar

CISA Zero Trust Pillar	CISA Functions	Cisco ISE Capabilities	Notes
Device	Device Inventory	Device Inventory	Cisco ISE maintains a detailed inventory of devices connected to the network.
	Device Security Posture	Device Detection and Compliance	Cisco ISE inspects devices in real-time to ensure compliance with security policies before granting access.
	Device Trust	Device Authorization with Real-Time Inspection	Cisco ISE authorizes devices dynamically based on trust levels and compliance with security controls.
	Secure Remote Access	Remote Access	Cisco ISE secures remote access by verifying device posture and enforcing conditional access policies.

Table 3. Mapping Cisco ISE Capabilities to the CISA Zero Trust Network/Environment Pillar

CISA Zero Trust Pillar	CISA Functions	Cisco ISE Capabilities	Notes
Network / Environment	Segmentation of Network	Macro-segmentation	Cisco ISE enables macro-segmentation by defining access policies for groups of devices or users.
	Secure Network Access	Micro-segmentation	Cisco ISE supports micro-segmentation by enforcing granular access policies at the individual device/user level.
	Encrypted Network Traffic		While Cisco ISE does not itself encrypt network traffic, it complements encryption by controlling access to encrypted communication pathways.

Table 4. Mapping Cisco ISE Capabilities to the CISA Zero Trust Application Workload Pillar

CISA Zero Trust Pillar	CISA Functions	Cisco ISE Capabilities	Notes
Application Workload	Enterprise Application Inventory		Cisco ISE does not directly manage application workloads but indirectly supports secure access to applications through identity and device polices.
	Secure Application Access		Cisco ISE indirectly contributes by ensuring only authorized users and devices can access applications.

Table 5. Mapping Cisco ISE Capabilities to the CISA Zero Trust Data Pillar

CISA Zero Trust Pillar	CISA Functions	Cisco ISE Capabilities	Notes
Data	Data Classification		Cisco ISE does not directly classify data but helps secure access to data by managing use and device authorization.
	Data Discovery		Data discovery is not a primary function of Cisco ISE, but can be supported indirectly by integrating with tools that classify or tag data.
	Encrypt Data at Rest and In Transit		Cisco ISE works alongside encryption solutions by controlling access to data, ensuring only authorized users/devices can access encrypted information.
	Prevent Data Exfiltration		Cisco ISE indirectly supports this by limiting access to unauthorized endpoints or users, reducing opportunities for data exfiltration.

Key observations

1. Core Strengths in Identity and Device Pillars

- Cisco ISE aligns strongly with the **Identity** and **Device** pillars of the CISA Zero Trust model. It provides robust identity and access management, continuous authentication, and device compliance capabilities.

2. Partial Contributions to the Network Pillar:

- Cisco ISE contributes to the **Network** Pillar by enabling **macro-segmentation** and **micro-segmentation**, as well as supporting **Software-Defined Networking (SDN)** for dynamic policy enforcement.

3. Limited Role in Application Workload and Data Pillars

- While Cisco ISE does not directly address application workloads or data management, it plays a supporting role by securing access to applications and data through identity and device controls.

4. Cross-Pillar Automation:

- Cisco ISE contributes to **Automation and Orchestration** (a Department of Defense (DoD) capability) through its **Policy Decision Point (PDP)** and **Policy Orchestration**, which align with the overarching automation requirements of the CISA Zero Trust model.

Summary

This mapping demonstrates that Cisco ISE is a powerful enabler of Zero Trust principles, particularly in the areas of **Identity**, **Device**, and **Network** security. While it does not address all aspects of **Application Workload** and the **Data** pillars, it complements solutions in those areas by securing access to resources.

Resources

Cisco Identity Services Engine

Cisco Identity Services Engine At-a-Glance

Cisco ISE Aligns to Comply-2-Connect (C2C) At-a-Glance