# Framework Mapping: Cisco Secure Access + CISA Zero Trust Model

# Background

U.S. Public Sector organizations are embarking on a Zero Trust roadmap—a structured and phased approach to transition their 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 their 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] that support (act 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 Secure Access meets the requirements of the CISA ZTMM.

[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.

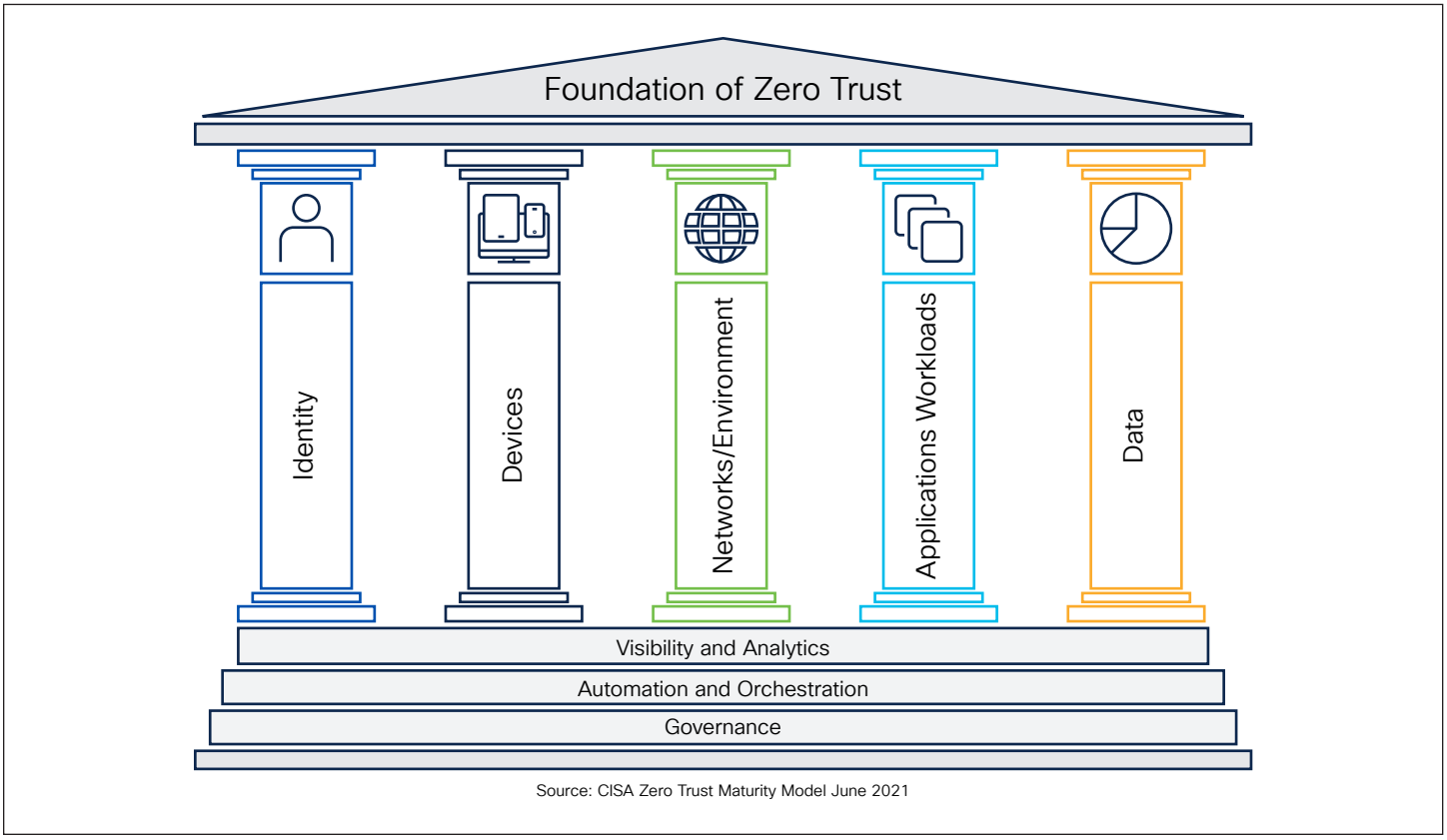


**Figure 1. CISA Zero Trust Maturity Model**

Cisco Secure Access enables the CISA ZTMM by excelling in the **Identity**, **Device**, and **Network/Environment** pillars of the CISA model. It ensures secure access to resources through **user identity verification**, **device compliance enforcement**, and **contextual access controls** that consider factors such as user activity monitoring, location, and device posture. Additionally, Cisco Secure Access supports **secure remote access** for hybrid work environments and enables **network segmentation** to prevent unauthorized lateral movement of threats. These capabilities are critical for safeguarding sensitive systems and ensuring that access policies are enforced dynamically across the organization.

While Cisco Secure Access contributions to the **Application Workload** and **Data** pillars are indirect, it complements other tools within the Zero Trust architecture by securing access to these resources through robust identity and device controls. By integrating seamlessly with other Cisco security solutions, Secure Access provides comprehensive visibility and enforcement across the network, ensuring that security policies are consistently applied. As a cornerstone the U.S. Public Sectors CISA ZTMM roadmap, Cisco Secure Access empowers the organization to build a scalable and secure architecture that aligns with national standards and best practices, helping it achieve its mission of delivering healthcare services with confidence and resilience.

# Mapping to the CISA Zero Trust Five Pillars

Below is a detailed mapping of **Cisco Secure Access** capabilities to the CISA Five Pillars of Zero Trust (Identity, Device, Network/Environment, Application Workload, and Data) and their corresponding functions. The mapping also consists of the three Base Pillars of the CISA Zero Trust Model (Visibility and Analytics, Automation and Orchestration, and Governance).

The following tables provide a clear alignment between Secure Access' features and the foundational components of a Zero Trust architecture, illustrating how the architecture's capabilities support each pillar and enhance overall security. By breaking down each pillar, function, and capability, the table offers valuable context for understanding how Secure Access enables organizations to advance their Zero Trust maturity.

**Table 1. Mapping Cisco Secure Access Capabilities to the CISA Zero Trust Identity Pillar**

| CISA Zero Trust Pillars | CISA Functions | Cisco Capabilities | Notes |
|---|---|---|---|
| **Identity** | Enterprise Identity and Access Management | User identity verification | Cisco Security Service Edge (SSE) ensures robust identity verification through integration with Cisco Duo and other identity providers. |
| | Multi-Factor Authentication | Multi-Factor Authentication (MFA) | Cisco SSE leverages an assortment of authentication methods (e.g., (Security Assertion Markup Language [SAML] or Remote Authentication Dial-In User Service [RADIUS], etc.) and thus can integrate MFAs for all users attempting to access resources. |
| | Privileged Access Management | Conditional Access Policies | Enforces policies that grant privileged access based on user roles, device posture, and contextual factors. |
| | Least Privilege Access | Cisco Policy Enforcement (e.g., Zero Trust) | Applies least-privilege principles by restricting access to only the resources required for a user's role and/or device posture. |

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

| CISA Zero Trust Pillars | CISA Functions | Cisco Capabilities | Notes |
|---|---|---|---|
| **Device** | Device Inventory | Device Visibility and Metrics | Cisco SSE provides visibility into devices accessing the network, including device type and posture. With ThousandEyes, Device Metrics are given (CPU, Memory, Network Interface and Metrics). |
| | Device Security Posture | Posture Assessment | Ensures connecting devices meet security requirements (e.g., updated OS, OS Version, Web Browser Version, Disk Encryption, Certificates, Process Checks, Registry Checks, Password Checks, Endpoint Detection and Response [EDR], et al.) before granting access. |
| | Device Trust | Device Trust Verification | Cisco SSE verifies device trust based on endpoint posture and compliance before authorizing access. |
| | Secure Remote Access | Secure Remote Access | Provides secure, VPN-less (Zero Trust) and VPN as a Service (VPNaaS) to corporate applications and data, particularly in hybrid or remote work environments. |

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

| CISA Zero Trust Pillars | CISA Functions | Cisco Capabilities | Notes |
|---|---|---|---|
| **Network/Environment** | Segmentation of Network | Policy-Based Access Control | Enforces network segmentation through access control policies that limit lateral movement and isolate unauthorized devices. |
| | Secure Network Access | VPNaaS and ZTNA | Enforces secure access to network resources, even for remote or cloud-based users. |
| | Encrypted Network Traffic | Encrypted Network Traffic | Cisco SSE enables secure encrypted communication with these protocols:<br><br>IKEv2 IPSEC, UDP/443 (DTLS), TCP/443 (TLS), and QUIC |

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

| CISA Zero Trust Pillars | CISA Functions | Cisco Capabilities | Notes |
|---|---|---|---|
| **Application Workload** | Enterprise Application Inventory | Private Resource Discovery | Monitors private network traffic, discovers usage patterns, and provides suggestions and a workflow for administrators to define Private Resources in SSE. |
| | Secure Application Access | Zero Trust Network Access (ZTNA) | Provides granular, app-specific secure access to private apps in on-premises data centers or in cloud/Infrastructure as a Service (IaaS) environments (based on User and Posture controls). |
| | | Unified Access Control | Offers unified intent-based policies for both cloud-based and on-premises applications, simplifying secure access management. |

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

| CISA Zero Trust Pillars | CISA Functions | Cisco Capabilities | Notes |
|---|---|---|---|
| **Data** | Data Classification | Multimode Data Loss Prevention (DLP) | DLP provides 1,200+ built-in global classifications for Personally Identifiable Information (PII), spanning 77 countries, for compliance with Personal Health Information (PHI), General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), PCI DSS (Payment Card Industry Data Security Standard), and more. |
| | Data Discovery | SaaS Data Loss Prevention (DLP) | Data discovery is not a primary function of Cisco Secure Access, but it can be integrated with other tools for comprehensive data security. |
| | Encrypt Data at Rest and in Transit | Supports Data Encryption | Cisco SSE does not store any customer data. Therefore, encryption for Data at Rest is supported and handled by data storage repositories. Secure Access does store its logfiles with approved encryption.<br><br>When Data is in transit Cisco Secure Access utilizes the following encryption standards: IKEv2 IPSEC, UDP/443 (DTLS), TCP/443 (TLS), and QUIC. |

| CISA Zero Trust Pillars | CISA Functions | Cisco Capabilities | Notes |
|---|---|---|---|
| **Data** | Prevent Data Exfiltration | Data Loss Prevention (DLP) | Multimode Data Loss Prevention (DLP) analyzes data in-line to provide visibility and control over sensitive data leaving your organization. API-based functionality for out-of-band analysis of data at rest in the cloud. Unified policies and reporting for more efficient administration and regulatory compliance. |

Table 6. Mapping Cisco Secure Access Capabilities to the CISA Zero Trust Visibility and Analytics Supporting Pillar

| CISA Zero Trust Pillar Base | CISA Functions | Cisco Capabilities | Notes |
|---|---|---|---|
| **Visibility and Analytics** | Security and Monitoring and Visibility | Cisco Secure Access provides real-time activity monitoring | Cisco SSE provides insights into user activity for monitoring and threat detection. Traffic is inspected as it enters and leaves the environment. |
| | Threat Intelligence Integration | Integration with Talos®, Cisco Extended Detection and Response (XDR), and Security Information and Event Management (SIEM tools like Splunk) | Cisco utilizes a data sharing ecosystem, both internally and with partners, to enhance security effectiveness.<br><br>Cisco actively partners with hundreds of security vendors through the Cisco Security Technical Alliance (CSTA) and is a member of the OpenID Foundation which contributes to a broader Shared Signals and Events ecosystem. |
| | Centralized Data Aggregation and Reporting | Cisco SSE has a single unified activity log | Consolidated access logs and use activity data allow for centralized visibility and reporting. |

Table 7. Mapping Cisco Secure Access Capabilities to the CISA Zero Trust Automation and Orchestration Supporting Pillar

| CISA Zero Trust Pillar Base | CISA Functions | Cisco Capabilities | Notes |
|---|---|---|---|
| **Automation and Orchestration** | Policy Decision and Enforcement | Policy-Based Access Control | Cisco SaaS-based Policy and Access Control dynamically enforces access policies based on user identity, device posture, and contextual factors.<br>This can be enforced for both remote and on-prem users. |
| | Workflow Integration and Process Automation | Cisco SSE has API Integration that provides monitoring and configuration capabilities | Using API capabilities customers can automate responses and workflows for environments ensuring seamless policy enforcement. |
| | Configuration Management | Centralized Policy Management | Enables administrators to define and centrally manage both access and internet polices that are consistently enforced. |
| | Automated Threat Detection and Response | Conditional Access Policies and Real-Time Enforcement | Cisco SSE supports automated threat detection and response. |

Table 8. Mapping Cisco Secure Access to the CISA Zero Trust Governance Supporting Pillar

| CISA Zero Trust Pillar Base | CISA Functions | Cisco Capabilities | Notes |
|---|---|---|---|
| **Governance** | Compliance Monitoring and Reporting | Detailed Reporting and Audit Capabilities | Provides detailed compliance reports and audit logs for regulatory and governance needs. SSE provides both systemwide reporting and user device posture reports. |
| | Continuous Monitoring and Risk Assessments | Posture Checks at continuous intervals and Risk-Based Access | Cisco SSE provides evaluation of both user and device posture to ensure access remains compliant with Zero Trust policies. |
| | Policy Definition and Management | Single management and reporting console | Unified security policy creation and management, using intent-based rules, across internet, public SaaS app, and private app access. |
| | Auditing and Reporting | Unified polices and reporting | Provides extensive logging and the ability to export logs to enterprise SOC. |

## Key observations

**1. Core Strengths in Identity and Device Security:**

- Cisco Secure Access excels in the Identity pillar, offering robust identity verification, MFA, and conditional access policies that align with Zero Trust principles.
- It also provides strong support for the Device pillar by verifying device posture, ensuring compliance, and securing remote access to resources.

**2. Contributions to Network Security:**

- Cisco Secure Access contributes to the Network pillar by enabling secure remote access and supporting network segmentation through policy-based access control.
- Its integration with Secure Access Service Edge (SASE) technologies further enhances secure connectivity for remote and distributed users.

**3. Limited Role in Application Workload and Data Pillars:**

- While Cisco Secure Access does not directly manage application workloads or classify data, it indirectly supports these pillars by securing access to applications and ensuring that only authorized users and devices can interact with sensitive information.

**4. Zero Trust Network Access (ZTNA):**

- Cisco Secure Access plays a key role in enabling Zero Trust Network Access, which aligns closely with the Application Workload pillar by ensuring secure and seamless access to applications, regardless of user location.

**5. Visibility and Analytics:**

- Cisco Secure Access enhances visibility through **analytics**, **centralized logging**, and integration with Cisco's broader security ecosystem (e.g., Talos, Duo, and XDR).
- Cisco Secure Access provides real-time tracking of user and device activity, enabling proactive threat detection and supporting compliance efforts.

**6. Automation and Orchestration:**

- Secure Access leverages **policy-based automation** to dynamically adjust access controls based on user context, device compliance, and real-time risk assessments.
- Its integration across hybrid environments automates workflows, ensuring seamless enforcement of security policies and reducing manual administrative overhead.

**7. Governance:**

- Cisco Secure Access supports governance with **detailed reporting**, **audit capabilities**, and **policy management tools** that ensure Zero Trust policies are consistently applied.
- Cisco Secure Access enhances compliance efforts through continuous risk assessments and posture checks, ensuring secure resource access while adhering to regulatory requirements.

## Summary

Cisco Secure Access plays a key role in advancing Zero Trust principles by aligning with the CISA Zero Trust model. It strengthens the **Network/Environment** pillar through capabilities such as macro-segmentation, data flow mapping, and user and entity behavior analytics to secure and monitor network environments effectively. In addition, it bolsters the **Identity** pillar with advanced behavioral and contextual analytics, enabling dynamic and risk-based access decisions. While its contributions to the **Device** and **Data** pillars are indirect, they enhance the overall Zero Trust architecture by ensuring device compliance and protecting sensitive data flows.

Through its holistic capabilities and seamless integration across multiple Zero Trust pillars, Cisco Secure Access empowers organizations to build a scalable, resilient, and secure Zero Trust environment that aligns with federal cybersecurity requirements. Its role in the **Application Workload** and **Data** pillars is more complementary, supporting other tools within a broader Zero Trust architecture. By verifying user identity, ensuring device compliance, and enabling secure remote access and network segmentation, Cisco Secure Access delivers robust protection for critical resources.

## Resources

Cisco Secure Access

Cisco Secure Access At-a-Glance

Cisco Secure Access Data Sheet

Cisco Secure Access – Modern Zero Trust Access



C11-5273399-00 07/25