Framework Mapping: Cisco Secure Access for Government + 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.

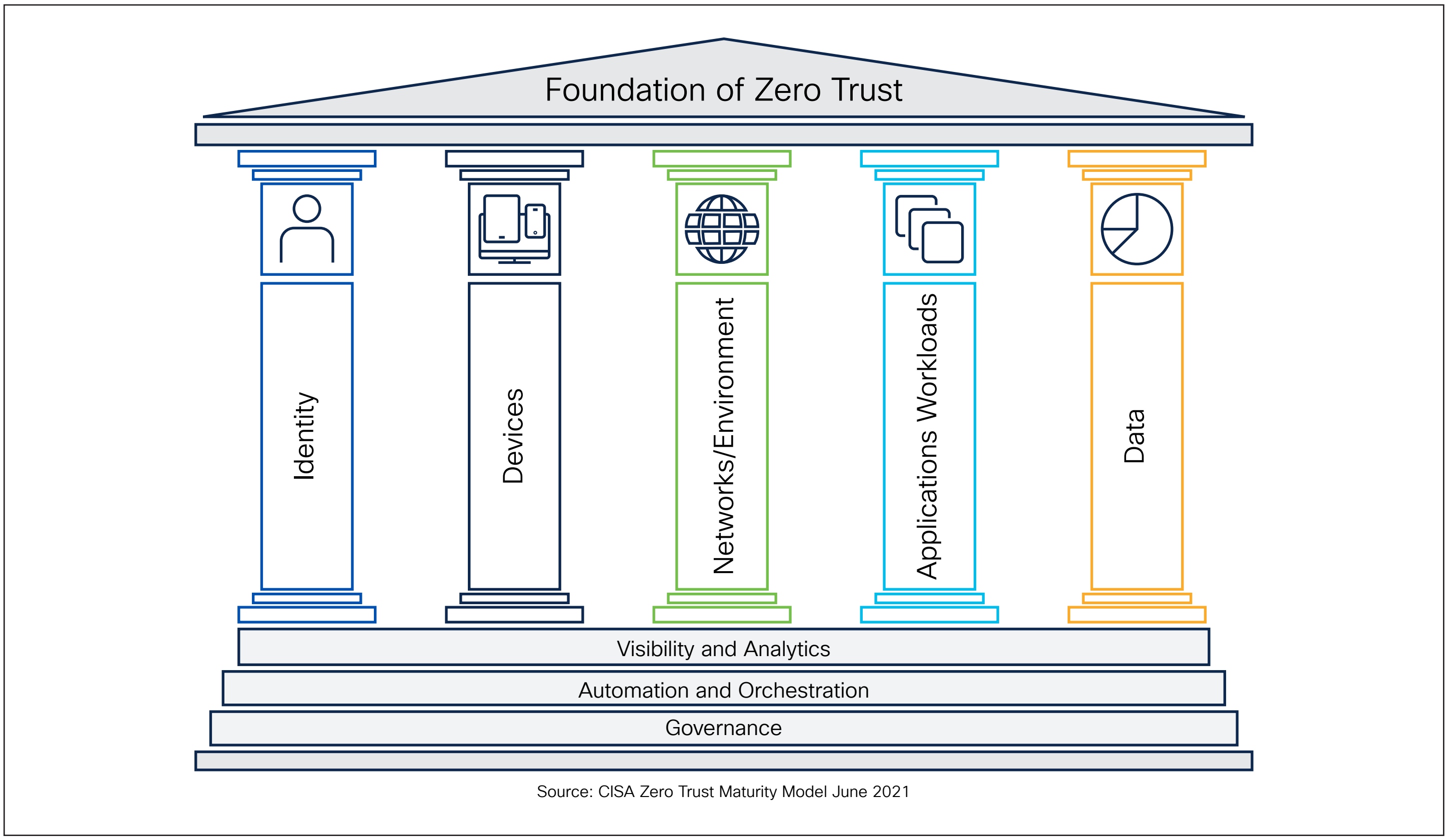
The CISA Zero Trust Model also builds on the foundational capabilities of the cross-cutting pillars with **Visibility and Analytics**,[1] **Automation and Orchestration**,[2] and **Governance**,[3] which support (act as the Pillar Base) and enhance the maturity of each core pillar.

Cisco® provides proven solutions for accelerating Zero Trust adoption. In this document we discuss how Cisco Secure Access for Government meets the requirements of 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.



Source: CISA Zero Trust Maturity Model June 2021

Figure 1. CISA Zero Trust Maturity Model

Cisco Secure Access for Government enables the CISA ZTMM by excelling in the **Identity**, **Device**, and **Network** 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 for Government 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 for Government 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 for Government provides comprehensive visibility and enforcement across the network, ensuring that security policies are consistently applied. As a cornerstone of the U.S. Public Sector CISA ZTMM roadmap, Cisco Secure Access for Government 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 for Government 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 Cisco Secure Access for Government features and the foundational components of a Zero Trust architecture, illustrating how its capabilities support each pillar and enhance overall security. By breaking down each pillar, function, and capability, the table offers valuable context for understanding how Cisco Secure Access for Government enables government organizations to advance their Zero Trust maturity.

Table 1. Mapping Cisco Secure Access for Government 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	Ensures robust identity verification through integration with Cisco Duo and other identity providers.
	Multi-Factor Authentication	Multi-Factor Authentication (MFA)	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 Multi-Factor Authentication (MFA) for all users attempting to access resources.
	Privileged Access Management	Conditional Access Policies	Enforces policies that grant privileged access based on user roles and device posture.
	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 for Government Capabilities to the CISA Zero Trust Device Pillar

CISA Zero Trust Pillars	CISA Functions	Cisco Capabilities	Notes
Device	Device Inventory	Device Visibility and Metrics	Provides visibility into registered devices accessing the network, including device type and posture.
	Device Security Posture	Posture Assessment	Ensures connecting devices meet security requirements (e.g., OS version, disk encryption, and host firewall state, etc.) before granting access to private applications.
	Device Trust	Device Trust Verification	Verifies device trust based on device certificate and compliance before authorizing access.
	Secure Remote Access	Secure Remote Access	Provides secure, VPN-less (Zero Trust) and VPNaaS, and browser-based access to corporate applications and data, particularly in hybrid or remote work environments.

Table 3. Mapping Cisco Secure Access for Government 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	Cloud-based enforcement of 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	Enables secure encrypted communication with these protocols: IKEv2 IPSEC, UDP/443 (DTLS), TCP/443 (TLS)

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

CISA Zero Trust Pillars	CISA Functions	Cisco Capabilities	Notes
Application Workload	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/ 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 for Government 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 built-in global classifications for Personally Identifiable Information (PII), spanning countries as well, for compliance with Personal Health Information (PHI), General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI), and more.
	Data Discovery	SaaS Data Loss Prevention	Scans data storage platforms using their native APIs to discover DLP violations based on policy.
	Encrypt Data at Rest and in Transit	Supports Data Encryption	Data is stored within the Amazon Web Services (AWS) Gov Cloud boundary with Federal Risk and Authorization Management Program (FedRAMP) compliant encryption. When data is in transit, Cisco Secure Access utilizes the following encryption standards: IKEv2 IPSEC, UDP/443 (DTLS), TCP/443 (TLS).
	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 for Government 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	Provides real-time activity monitoring	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® 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. 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	Provides a single unified activity log	Logs and uses activity data allow for centralized visibility and reporting.

Mapping Cisco Secure Access for Government Capabilities to the CISA Zero Trust Automation and Orchestration Supporting Pillar

The initial FedRAMP release of Cisco Secure Access for Government does not support the Automation and Orchestration pillar, as its current feature set does not include APIs.

Table 7. Mapping Cisco Secure Access for Government 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 reports and audit logs for regulatory and governance needs. Secure Access for Government provides customizable reporting.
	Continuous Monitoring and Risk Assessments	Posture Checks at continuous intervals and Risk-Based Access	Provides evaluation of both user and device posture to ensure access remains compliant with Zero Trust policies. Cisco Secure Access for Government complies with FedRAMP requirements.
	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. Custom and prebuilt reports are also available through the Admin Dashboard.

Key observations

1. Core Strengths in Identity and Device Security

- Cisco Secure Access for Government 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 for Government 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 for Government 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 for Government provides 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 for Government enhances visibility through **analytics**, **centralized logging**, and integration with Cisco's broader security ecosystem.
- Its ability to track user and device activity in real time ensures proactive threat detection and supports compliance initiatives.

6. Governance

- Cisco Secure Access for Government supports governance with **detailed reporting**, **audit capabilities**, and **policy management tools** that ensure Zero Trust policies are consistently applied.
- Continuous risk assessments and posture checks strengthen compliance efforts, ensuring secure access to resources while aligning with regulatory requirements.

Summary

Cisco Secure Access for Government 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 for Government 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 for Government delivers robust protection for critical resources.

Resources

Cisco Secure Access for Government

Cisco Secure Access for Government At-a-Glance