White paper Cisco public

Framework Mapping: Cisco Secure Workload + CISA Zero Trust Model

© 2025 Cisco and/or its affiliates. All rights reserved.

Background

U.S. Public Sector organizations are embarking on a Zero Trust roadmap—a structured and phased approach to transition their cybersecurity frameworks 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.

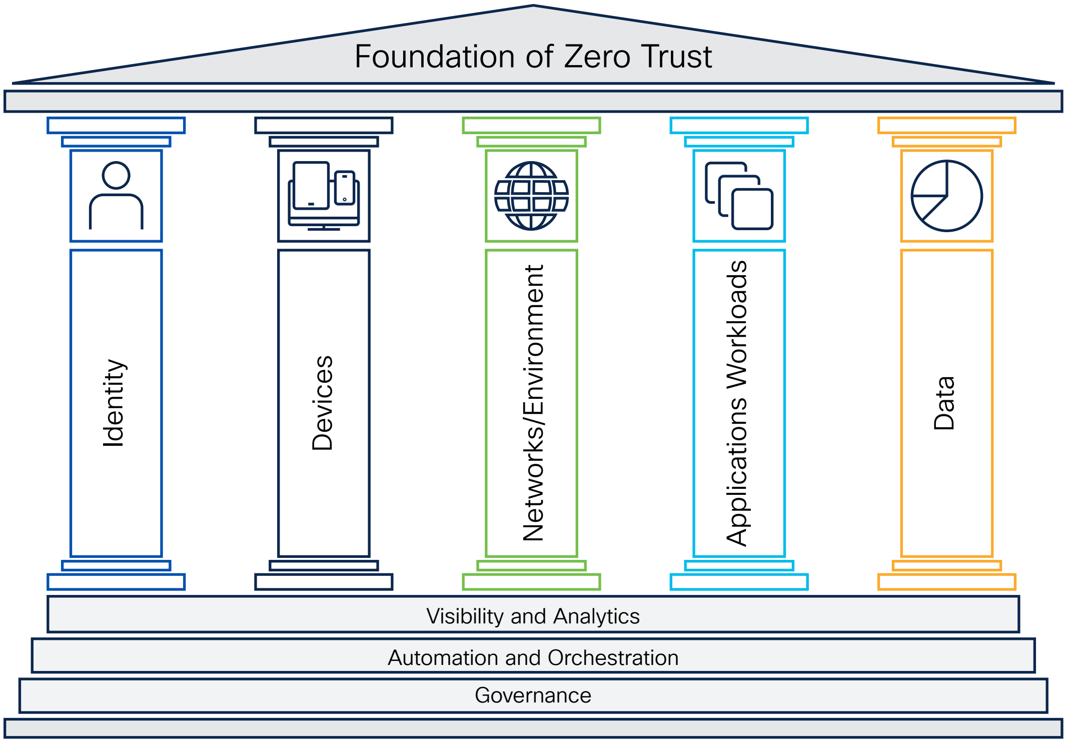
Cisco® provides proven solutions for accelerating Zero Trust adoption. In this document we discuss how Cisco Secure Workload meets the CISA ZTMM.

[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.

© 2025 Cisco and/or its affiliates. All rights reserved.



Source: CISA Zero Trust Maturity Model June 2021

Figure 1. CISA Zero Trust Maturity Model

Cisco Secure Workload plays a vital role in supporting Zero Trust strategies by excelling in the **Application Workload, Network,** and **Visibility and Analytics** pillars. Secure Workload provides robust capabilities for **workload inventory, risk management, micro-segmentation,** and **security analytics**, ensuring that applications and workloads are secured against internal and external threats. By dynamically monitoring workloads and applying granular segmentation, Secure Workload reduces the attack surface and prevents unauthorized lateral movement within the network. Its analytics capabilities further enable an organization to identify vulnerabilities, track workload behavior, and enforce Zero Trust policies with precision.

In addition to its primary strengths, Cisco Secure Workload indirectly supports the **Data** pillar by enabling **data flow mapping** and **segmentation**, which help protect sensitive information as it moves across workloads. While its role in the **Identity** and **Device** pillars is more limited, Secure Workload complements other Cisco solutions by providing critical insights and enforcing workload-level security controls. As a core component of an organization's Zero Trust roadmap, Cisco Secure Workload integrates seamlessly with the broader Zero Trust architecture, empowering the organization to enhance workload security, mitigate risks, and achieve alignment with national cybersecurity standards and best practices.

© 2025 Cisco and/or its affiliates. All rights reserved.

Mapping to the CISA Zero Trust 5 Pillars

Below is a detailed mapping of Cisco Secure Workload capabilities to the CISA Zero Trust 5 Pillars and their corresponding functions. This table provides a clear alignment between Secure Workload's 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 Secure Workload enables government organizations, like Health and Human Services (HHS), to advance their Zero Trust maturity.

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

CISA Zero Trust Pillars	CISA Functions	Cisco Capabilities	Notes
Identity	Enterprise Identity and Access Management		Cisco Secure Workload does not directly manage user identities but complements identity-based controls by enforcing workload policies. Cisco Secure Workload complements Access Management by leveraging a policy model where Role-Based Access Control (RBAC) can be assigned to different personas, effectively delegating policy controls to multiple users (e.g., application owners, network security teams, InfoSec teams). Cisco Secure Workload can also fetch user identity information and attributes (e.g., user, user groups) from Identity Stores (e.g., Microsoft AD, Microsoft Entra ID, Lightweight Directory Access Protocol [LDAP]) or directly via integration with Cisco Secure Client and Cisco Identity Services Engine (ISE) for user identity control.
	Multi-Factor Authentication		MFA is not a direct capability but can be integrated with other tools to enhance identity-based secure workload access.
	Privileged Access Management		Indirectly supports privileged access management by enforcing security policies to restrict unauthorized access to workloads.
	Least Privilege Access		Supports least privilege by enforcing granular workload-level access and micro-segmentation policies.

© 2025 Cisco and/or its affiliates. All rights reserved.

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

CISA Zero Trust Pillars	CISA Functions	Cisco Capabilities	Notes
Device	Device Inventory		Cisco Secure Workload does not directly manage device inventories but supports workload visibility and segmentation. Cisco Secure Workload complements device inventory by integrating with Cisco Identity Services Engine (ISE), pulling inventory information from multiple endpoints and devices.
	Device Security Posture		While the Cisco Secure Workload solution focuses on workload security rather than individual device posture, it does have the capabilities to inform customers about their workload security posture (e.g., process information as well as the vulnerable packages on the workload). Secure Workload can also detect malicious processes running and gather a process tree with all actions executed by each process. Cisco Secure Workload can pull endpoint and device posture information by integrating with Cisco Identity Services Engine (ISE) and Cisco Secure Client, enabling access control based on security context and endpoint risk context. Cisco Secure Workload can integrate with Cisco ISE to check the security posture observing and detecting risky inventory.
	Device Trust		Indirectly supports device trust by ensuring that workloads and their associated devices communicate within defined policies and compliance. Cisco Secure Workload can pull endpoint and device trust assessment by integrating with Cisco Identity Services Engine, dynamically changing access control based to assets.

© 2025 Cisco and/or its affiliates. All rights reserved.

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

CISA Zero Trust Pillars	CISA Functions	Cisco Capabilities	Notes
Network/Environment	Segmentation of Network	Micro-Segmentation	Cisco Secure Workload enforces micro-segmentation to isolate workloads and restrict lateral movement.
	Secure Network Access	Data Flow Mapping	Provides visibility into data flows between workloads, enabling secure and optimized communication across the network. Cisco Secure Workload provides a network map to visualize and plot traffic flows between different workload access.
	Encrypted Network Traffic		While encryption itself is not a direct capability, Secure Workload ensures encrypted traffic adheres to defined policies. Cisco Secure Workload complements mandated encryption on traffic flows by providing flow observability of weak or obsolete Transport Layer Security (TLS) versions and ciphers, ensuring data-in-transit is protected using modern encryption protocols.

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

CISA Zero Trust Pillars	CISA Functions	Cisco Capabilities	Notes
Application Workload	Enterprise Application Inventory	Application Inventory	Cisco Secure Workload maintains an inventory of applications workloads and their communication patterns to enhance visibility and security.
	Secure Application Access	Software Risk Management	Analyzes software risks and vulnerabilities within workloads to ensure secure application and workload access.
		Policy Decision Point (PDP)	Enforces security policies for workloads dynamically, ensuring secure communication and application access.

© 2025 Cisco and/or its affiliates. All rights reserved.

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

CISA Zero Trust Pillars	CISA Functions	Cisco Capabilities	Notes
Data	Data Classification		Cisco Secure Workload does not classify data but provides insights into data flows between workloads. Cisco Secure Workload complements data classification by leveraging up to 32 labels, allowing contextual information to workload assets.
	Data Discovery		Data discovery is not a direct capability, but Secure Workload maps data flows to identify critical paths and potential risks.
	Encrypt Data at Rest and in Transit		While encryption is not managed directly, Cisco Secure Workload ensures that traffic adheres to security policies, reducing risks to encrypted data. Cisco Secure Workload complements mandated encryption on traffic flows by providing flow observability of weak or obsolete TLS versions and ciphers, ensuring data-in-transit is protected using modern encryption protocols.
	Prevent Data Exfiltration		Supports prevention of unauthorized data exfiltration by restricting and monitoring workload communication paths. Cisco Secure Workload provides monitoring capabilities to detect data leakage/data exfiltration from applications.

Table 6. Mapping Cisco Secure Workload 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 Monitoring and Visibility	Common Security and Risk Analysis	Provides advanced security analytics and risk assessments for workloads and applications.
			Enables visibility into workload behavior and communication to detect anomalies and risks.

© 2025 Cisco and/or its affiliates. All rights reserved.

Key observations

1. Core Strengths in Application Workload Security:

- Cisco Secure Workload strongly aligns with the **Application Workload** pillar by providing **application inventory** and **software risk management** capabilities, ensuring visibility into workloads and their risks.

2. Contributions to Network Security:

- Within the Network pillar, Cisco Secure Workload provides **micro-segmentation** and **data flow mapping** capabilities, ensuring secure communication between workloads and minimizing lateral movement of threats.

3. Support for Data Security:

- While Cisco Secure Workload does not directly classify or encrypt data, its focus on segmentation and data flow mapping contributes to **data protection** and helps prevent unauthorized exfiltration.

4. Visibility and Analytics Enhancements:

- Cisco Secure Workload supports the **Visibility and Analytics** pillar with **common security and risk analysis**, providing visibility into workload behavior and risks to improve threat detection.

5. Limited Role in Identity and Device Security:

- Cisco Secure Workload does not directly manage identities or devices but complements these areas by enforcing workload- and policy-level controls to ensure secure access and communication.

Summary

Cisco Secure Workload excels in the **Application Workload, Network,** and **Visibility and Analytics** pillars of the CISA Zero Trust model, offering robust capabilities for workload inventory, risk management, micro-segmentation, and security analytics. Its contributions to the **Data** pillar are indirect, focusing on data flow mapping and segmentation to protect sensitive information. While its role in the **Identity** and **Device** pillars is limited, it complements other tools in enforcing Zero Trust principles across workloads.

Resources

Cisco Secure Workload

Cisco Secure Workload At-a-Glance

Cisco Secure Workload Datasheet

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)