Zero Trust Frameworks

Architecture Guide

May, 2023

Contents

Introduction

This document provides guidance on the various Zero Trust Frameworks and their relationship to the Cisco Zero Trust Framework. For each of the Zero Trust Frameworks a mapping to Cisco product is provided.

Cisco Zero Trust Framework

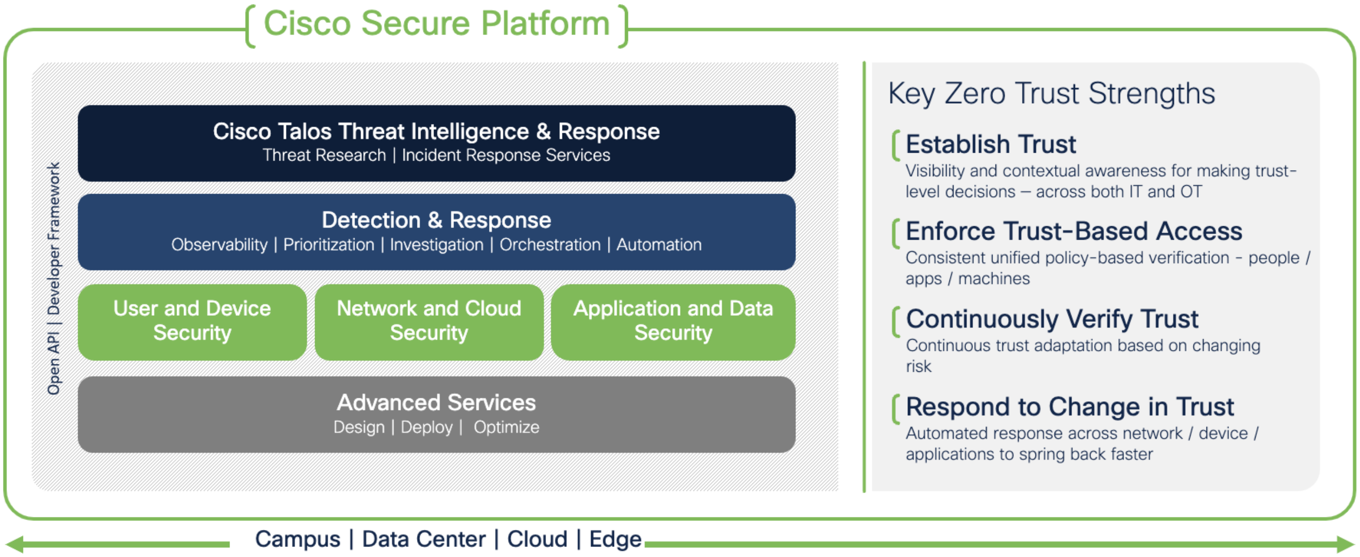
Cisco Secure Platform
Open API | Developer Framework
Cisco Talos Threat Intelligence & Response
Threat Research | Incident Response Services
Detection & Response
Observability | Prioritization | Investigation | Orchestration | Automation
User and Device Security
Network and Cloud Security
Application and Data Security
Advanced Services
Design | Deploy | Optimize
Key Zero Trust Strengths
Establish Trust
Visibility and contextual awareness for making trust-level decisions – across both IT and OT
Enforce Trust-Based Access
Consistent unified policy-based verification - people / apps / machines
Continuously Verify Trust
Continuous trust adaptation based on changing risk
Respond to Change in Trust
Automated response across network / device / applications to spring back faster
Campus | Data Center | Cloud | Edge

Figure 1. Cisco Zero Trust Framework

Security is not a one-size-fits-all and Zero Trust is more than network segmentation. To help understand the architecture, Cisco has broken it down into three pillars:

- **User and Device Security:** ensure users and devices can be trusted as they access systems, regardless of location
- **Network and Cloud Security:** protect all network resources on-prem and in the cloud, and ensure secure access for all connecting users
- **Application and Data Security:** prevent unauthorized access within application environments irrespective of where they are hosted

Zero Trust cannot be solved by a single product. Zero Trust can only be realized by proper integration of security tools to provide an adaptive, scalable and integrated security solution that applies all of the Zero Trust principles. In general, excessive use of the “best” point products does not create the cohesive security strategy that Zero Trust can.

Zero Trust Security Frameworks

The following table shows how Zero Trust Frameworks map to the Cisco Zero Trust Framework.

Cisco	NIST 800-207 Zero Trust Architecture	CISA Zero Trust Maturity Model	DISA Zero Trust Framework	Common
User and Device Security	Users and/or Devices	Identity	Users	Visibility & Analytics Automation & Orchestration Governancec
		Devices	Devices	
Network and Cloud Security	Policy Decision and Enforcement Points	Networks	Network/Environment	
Application and Data Security	Enterprise Resources	Applications and Workloads	Workloads	
		Data	Data	

Table 1. Zero Trust Frameworks Mapping

NIST Special Publication 800-207 – Zero Trust Architecture

The National Institute of Standards and Technology (NIST) develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies and the broader public.

NIST defines both Zero Trust and a Zero Trust Architecture as: "Zero trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. Zero Trust Architecture (ZTA) is an enterprise's cybersecurity plan that uses zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a ZTA plan." (NIST 800-207 - 2.0 - Zero Trust Basics)

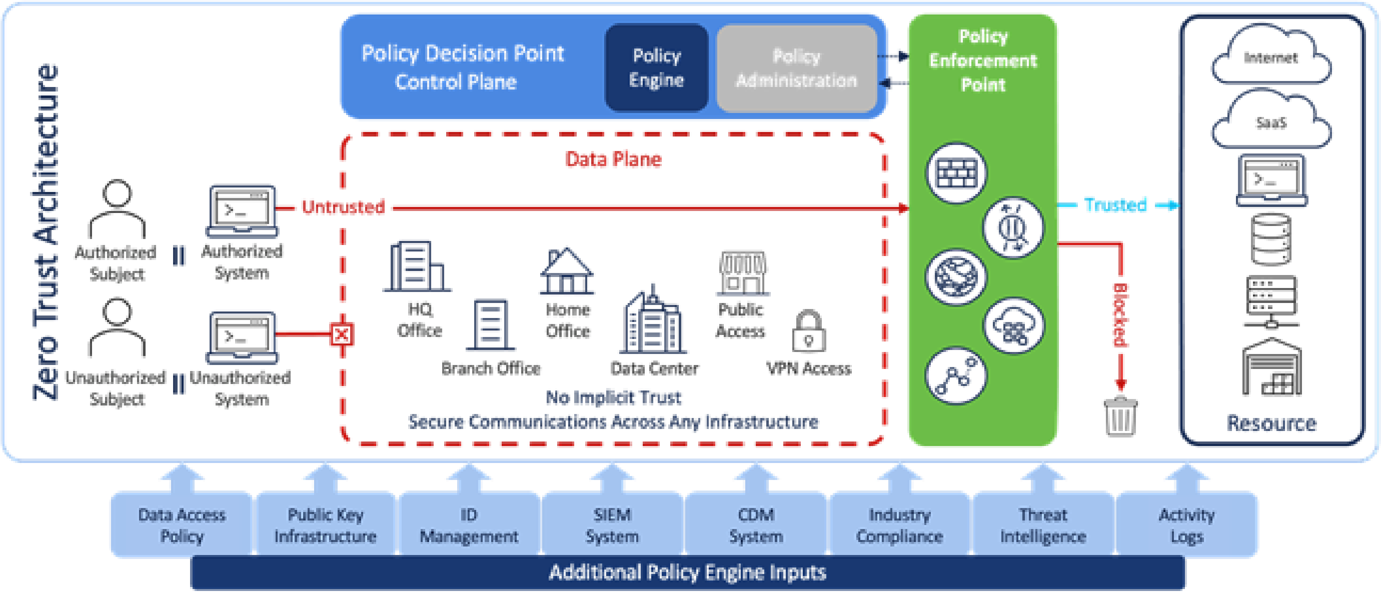

Figure 2. **NIST Zero Trust Architecture**

The following table is the mapping of NIST Special Publication 800-207 – Zero Trust Architecture to Cisco Products.

NIST 800-207 Logical Component	Cisco Product
Policy Engine (PE)	Cisco Secure Access by Duo Cisco Umbrella Cisco Identity Services Engine
Policy Administrator (PA)	Cisco Secure Access by Duo Cisco Umbrella Cisco Identity Services Engine Cisco Defense Orchestrator Cisco Secure Firewall Management Center Cisco Secure Workload
Data Access Policies	Cisco Secure Access by Duo Cisco Umbrella Cisco Identity Services Engine Cisco Defense Orchestrator Cisco Secure Firewall Management Center Cisco Secure Workload Cisco Secure Network Analytics Cisco Network Devices Cisco Wireless Devices
Continuous Diagnostics and Mitigation System	Cisco Secure Access by Duo Cisco Identity Services Engine Cisco Defense Orchestrator Cisco Secure Firewall Management Center Cisco Secure Workload Cisco Secure Network Analytics Cisco Secure Application Cisco Secure Application Cloud Native Cisco Network Devices Cisco Wireless Devices
Industry Compliance System	Cisco Secure Access by Duo Cisco Identity Services Engine Cisco Secure Network Analytics
Public Key Infrastructure	
Policy Enforcement Point	Cisco Secure Access by Duo Cisco Umbrella Cisco Identity Services Engine Cisco Secure Firewall Cisco Secure Workload Cisco Cyber Vision Cisco Network Devices Cisco Wireless Devices
Threat Intelligence Feed(s)	Cisco Secure Firewall Cisco Identity Services Engine Cisco Secure XDR Cisco Talos Cisco Secure Insights Cisco Network Devices Cisco Wireless Devices Cisco Security Analytics and Logging (SAL) Kenna Security
Network and System Activity Logs	Cisco Secure Access by Duo Cisco Secure Application Cisco Secure Application Cloud Native Cisco Network Devices Cisco Wireless Devices
ID Management System	

NIST 800-207 Logical Component	Cisco Product
Security Information and Event Management (SIEM)	Cisco Secure XDR

Table 2. NIST SP800-207 – Zero Trust Architecture mapping to Cisco Product

CISA Zero Trust Maturity Model V2.0

The Cybersecurity and Infrastructure Security Agency (CISA) leads the Unites States' national effort to understand, manage, and reduce risk to our cyber and physical infrastructure. Their mission expands across three primary areas: cybersecurity, infrastructure security, and emergency communications.

CISA Zero Trust Maturity Model v2.0 is one of many roadmaps that agencies can reference as they transition towards a zero trust architecture. The maturity model aims to assist agencies in the development of zero trust strategies and implementation plans and to present ways in which various CISA services can support zero trust solutions across agencies.

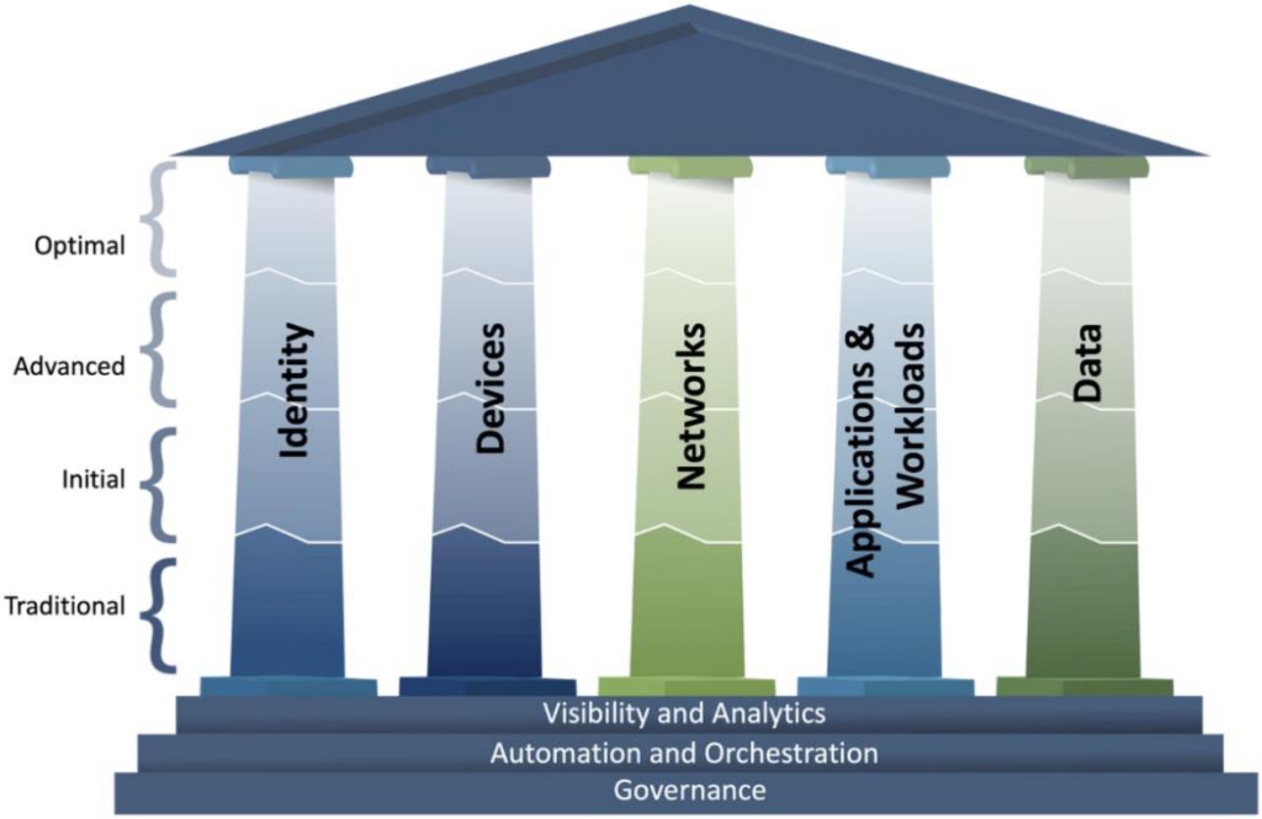

Figure 3. **CISA Zero Trust Maturity Evoluton**

Source: CISA Zero Trust Maturity Model V2.0

Agencies should use the following guiding criteria of each stage to identify maturity for each zero trust technology pillar and provide consistency across the maturity model:

- **Traditional**–manually configured lifecycles (i.e., from establishment to decommissioning) and assignments of attributes (security and logging); static security policies and solutions that address one pillar at a time with discrete dependencies on external systems; least privilege established only at provisioning; siloed pillars of policy enforcement; manual response and mitigation deployment; and limited correlation of dependencies, logs, and telemetry
- **Initial**–starting automation of attribute assignment and configuration of lifecycles, policy decisions and enforcement, and initial cross-pillar solutions with integration of external systems; some responsive changes to least privilege after provisioning; and aggregated visibility for internal systems
- **Advanced**–wherever applicable, automated controls for lifecycle and assignment of configurations and policies with cross-pillar coordination; centralized visibility and identity control; policy enforcement integrated across pillars; response to pre-defined mitigations; changes to least privilege based on risk and posture assessments; and building toward enterprise-wide awareness (including externally hosted resources)
- **Optimal**–fully automated, just-in-time lifecycles and assignments of attributes to assets and resources that self-report with dynamic policies based on automated/observed triggers; dynamic least privilege access (just-enough and within thresholds) for assets and their respective dependencies enterprise-wide; cross-pillar interoperability with continuous monitoring; and centralized visibility with comprehensive situational awareness

The following table is the CISA Zero Trust Maturity Model with the mapping to Cisco Products.

CISA Zero Trust Pillar	Function	Traditional	Initial	Advanced	Optimal	Cisco Product
Identity	Authentication	Agency authenticates identity using either passwords or multi-factor authentication (MFA) with static access for entity identity.	Agency authenticates identity using MFA, which may include passwords as one factor and requires validation of multiple entity attributes (e.g., locale or activity).	Agency begins to authenticate all identity using phishing-resistant MFA and attributes, including initial implementation of password- less MFA via FIDO2 or PIV.	Agency continuously validates identity with phishing-resistant MFA, not just when access is initially granted.	Cisco Secure Access by Duo
	Identity Stores	Agency only uses self-managed, on-premises (i.e., planned, deployed, and maintained by agency) identity stores.	Agency has a combination of self-managed identity stores and hosted identity store(s) (e.g., cloud or other agency) with minimal integration between the store(s) (e.g., Single Sign-on.).	Agency begins to securely consolidate and integrate some self-managed and hosted identity stores.	Agency securely integrates their identity stores across all partners and environments as appropriate.	Cisco Secure Access by Duo
	Risk Assessment	Agency makes limited determinations for identity risk (i.e., likelihood that an identity is compromised).	Agency determines identity risk using manual methods and static rules to support visibility.	Agency determines identity risk with some automated analysis and dynamic rules to inform access decisions and response activities.	Agency determines identity risk in real time based on continuous analysis and dynamic rules to deliver ongoing protection.	Cisco XDR with Secure Cloud Insights Kenna Security
	Access Management	Agency authorizes permanent access with periodic review for both privileged and unprivileged accounts	Agency authorizes access, including for privileged access requests, that expires with automated review.	Agency authorizes need-based and session-based access, including for privileged access request, that is tailored to actions and resources.	Agency uses automation to authorize just-in-time and just-enough access tailored to individual actions and individual resource needs.	Cisco Secure Access by Duo Cisco Identity Services Engine

CISA Zero Trust Pillar	Function	Traditional	Initial	Advanced	Optimal	Cisco Product
	Visibility and Analytics Capability	Agency collects user and entity activity logs, especially for privileged credentials, and performs some routine manual analysis.	Agency collects user and entity activity logs and performs routine manual analysis and some automated analysis, with limited correlation between log types.	Agency performs automated analysis across some user and entity activity log types and augments collection to address gaps in visibility.	Agency maintains comprehensive visibility and situational awareness across enterprise by performing automated analysis over user activity log types, including behavior-based analytics.	Cisco Secure XDR Cisco Secure Firewall Cisoc Secure Network Analytics Cisco Telemetry Broker
	Automation and Orchestration Capability	Agency manually orchestrates (onboards, offboards, and disables) self-managed identities (users and entities), with little integration, and performs regular review.	Agency manually orchestrates privileged and external identities and automates orchestration of non-privileged users and of self-managed entities.	Agency manually orchestrates privileged user identities and automates orchestration of all identities with integration across all environments.	Agency automates orchestration of all identities with full integration across all environments based on behaviors, enrollments, and deployment needs.	Cisco Secure XDR
	Governance Capability	Agency implements identity policies (authentication, credentials, access, lifecycle, etc.) with enforcement via static technical mechanisms and manual review.	Agency defines and begins implementing identity policies for enterprise-wide enforcement with minimal automation and manual updates.	Agency implements identity policies for enterprise-wide enforcement with automation and updates policies periodically.	Agency implements and fully automates enterprise-wide identity policies for all users and entities across all systems with continuous enforcement and dynamic updates.	Cisco Secure XDR

CISA Zero Trust Pillar	Function	Traditional	Initial	Advanced	Optimal	Cisco Product
Devices	Policy Enforcement & Compliance Monitoring	Agency has limited, if any, visibility (i.e., ability to inspect device behavior) into device compliance with few methods of enforcing policies or managing software, configurations, or vulnerabilities.	Agency receives self-reported device characteristics (e.g., keys, tokens, users, etc., on the device) but has limited enforcement mechanisms. Agency has a preliminary, basic process in place to approve software use and push updates and configuration changes to devices.	Agency has verified insights (i.e., an administrator can inspect and verify the data on device) on initial access to device and enforces compliance for most devices and virtual assets. Agency uses automated methods to manage devices and virtual assets, approve software, and identify vulnerabilities and install patches.	Agency continuously verifies insights and enforces compliance throughout the lifetime of devices and virtual assets. Agency integrates device, software, configuration, and vulnerability management across all agency environments, including for virtual assets.	Cisco XDR with Secure Device Insights Cisco Secure Access by Duo Cisco Secure Firewall Cisco Secure Workload Cisco Identity Services Engine Cisco Umbrella Cisco Cyber Vision Cisco Network Devices Cisco Wireless Devices
	Asset & Supply Chain Risk Management	Agency does not track physical or virtual assets in an enterprise-wide or crossvendor manner and manages its own supply chain acquisition of devices and services in ad hoc fashion with a limited view of enterprise risks.	Agency tracks all physical and some virtual assets and manages supply chain risks by establishing policies and control baselines according to federal recommendations using a robust framework, (e.g., NIST SCRM.)	Agency begins to develop a comprehensive enterprise view of physical and virtual assets via automated processes that can function across multiple vendors to verify acquisitions, track development cycles, and provide third-party assessments.	Agency has a comprehensive, at- or nearreal-time view of all assets across vendors and service providers, automates its supply chain risk management as applicable, builds operations that tolerate supply chain failures, and incorporates best practices.	Cisco XDR with Secure Device Insights

CISA Zero Trust Pillar	Function	Traditional	Initial	Advanced	Optimal	Cisco Product
	Resource Access	Agency does not require visibility into devices or virtual assets used to access resources.	Agency requires some devices or virtual assets to report characteristics then use this information to approve resource access.	Agency's initial resource access considers verified device or virtual asset insights.	Agency's resource access considers real-time risk analytics within device and virtual assets.	Cisco Secure XDR with Secure Device Insights
	Device Threat Protection	Agency manually deploys threat protection capabilities to some devices.	Agency has some automated processes for deploying and updating threat protection capabilities to devices and to virtual assets with limited policy enforcement and compliance monitoring integration.	Agency begins to consolidate threat protection capabilities to centralized solutions for devices and virtual assets and integrates most of these capabilities with policy enforcement and compliance monitoring.	Agency has a centralized threat protection security solution(s) deployed with advanced capabilities for all devices and virtual assets and a unified approach for device threat protection, policy enforcement, and compliance monitoring.	Cisco Secure Endpoint
	Visibility and Analytics Capability	Agency uses a physically labeled inventory and limited software monitoring to review devices on a regular basis with some manual analysis.	Agency uses digital identifiers (e.g., interface addresses, digital tags) alongside a manual inventory and endpoint monitoring of devices when available. Some agency devices and virtual assets are under automated analysis (e.g., software-based scanning) for anomaly detection based on risk.	Agency automates both inventory collection (including endpoint monitoring on all standard user devices, e.g., desktops and laptops, mobile phones, tablets, and their virtual assets) and anomaly detection to detect unauthorized devices.	Agency automates status collection of all networkconnected devices and virtual assets while correlating with identities, conducting endpoint monitoring, and performing anomaly detection to inform resource access. Agency tracks patterns of provisioning and/or deprovisioning of virtual assets for anomalies.	Cisco XDR with Secure Device Insights Cisco Secure Client

CISA Zero Trust Pillar	Function	Traditional	Initial	Advanced	Optimal	Cisco Product
	Automation and Orchestration Capability	Agency manually provisions, configures, and/or registers devices within the enterprise.	Agency begins to use tools and scripts to automate the process of provisioning, configuration, registration, and/or deprovisioning for devices and virtual assets.	Agency has implemented monitoring and enforcement mechanisms to identify and manually disconnect or isolate non-compliant (vulnerable, unverified certificate; unregistered mac address) devices and virtual assets.	Agency has fully automated processes for provisioning, registering, monitoring, isolating, remediating, and deprovisioning devices and virtual assets.	Cisco XDR Cisco Meraki Mobile Device Managem ent
	Governance Capability	Agency sets some policies for the lifecycle of their traditional and peripheral computing devices and relies on manual processes to maintain (e.g., update, patch, sanitize) these devices.	Agency sets and enforces policies for the procurement of new devices, the lifecycle of non-traditional computing devices and virtual assets, and for regularly conducting monitoring and scanning of devices.	Agency sets enterprise-wide policies for the lifecycle of devices and virtual assets, including their enumeration and accountability, with some automated enforcement mechanisms.	Agency automates policies for the lifecycle of all network-connected devices and virtual assets across the enterprise.	Cisco XDR with Secure Device Insights
Networks	Network Segmentation	Agency defines their network architecture using large perimeter/macrosegmentation with minimal restrictions on reachability within network segments. Agency may also rely on multi-service interconnections (e.g., bulk traffic VPN tunnels).	Agency begins to deploy network architecture with the isolation of critical workloads, constraining connectivity to least function principles, and a transition toward service-specific interconnections.	Agency expands deployment of endpoint and application profile isolation mechanisms to more of their network architecture with ingress/egress microperimeters and servicespecific interconnections.	Agency network architecture consists of fully distributed ingress/egress microperimeters and extensive micro-segmentation based around application profiles with dynamic just-in-time and just-enough connectivity for service-specific interconnections.	Cisco Secure Firewall Cisco Identity Services Engine Cisco SD-WAN with Meraki Cisco SD-WAN with Viptela Cisco Secure Workload Cisco Cyber Vision Cisco Network Devices

CISA Zero Trust Pillar	Function	Traditional	Initial	Advanced	Optimal	Cisco Product
						Cisco Wireless Devices
	Network Traffic Management	Agency manually implements static network rules and configurations to manage traffic at service provisioning, with limited monitoring capabilities (e.g., application performance monitoring or anomaly detection) and manual audits and reviews of profile changes for mission critical applications.	Agency establishes application profiles with distinct traffic management features and begins to map all applications to these profiles. Agency expands application of static rules to all applications and performs periodic manual audits of application profile assessments.	Agency implements dynamic network rules and configurations for resource optimization that are periodically adapted based upon automated risk-aware and risk-responsive application profile assessments and monitoring.	Agency implements dynamic network rules and configurations that continuously evolve to meet application profile needs and reprioritize applications based on mission criticality, risk, etc.	Cisco Network Devices Cisco Wireless Devices Cisco Secure Firewall Cisco Cyber Vision Cisco Secure XDR
	Traffic Encryption	Agency encrypts minimal traffic and relies on manual or ad hoc processes to manage and secure encryption keys.	Agency begins to encrypt all traffic to internal applications, to prefer encryption for traffic to external applications, to formalize key management policies, and to secure server/service encryption keys.	Agency ensures encryption for all applicable internal and external traffic protocols, manages issuance and rotation of keys and certificates, and begins to incorporate best practices for cryptographic agility.	Agency continues to encrypt traffic as appropriate, enforces least privilege principles for secure key management enterprisewide, and incorporates best practices for cryptographic agility as widely as possible.	Cisco Secure Client Cisco Secure Firewall Cisco SD-WAN with Meraki Cisco SD-WAN with Viptela

CISA Zero Trust Pillar	Function	Traditional	Initial	Advanced	Optimal	Cisco Product
	Network Resilience	Agency configures network capabilities on a case-by-case basis to only match individual application availability demands with limited resilience mechanisms for workloads not deemed mission critical.	Agency begins to configure network capabilities to manage availability demands for additional applications and expand resilience mechanisms for workloads not deemed mission critical.	Agency has configured network capabilities to dynamically manage the availability demands and resilience mechanisms for the majority of their applications.	Agency integrates holistic delivery and awareness in adapting to changes in availability demands for all workloads and provides proportionate resilience.	
	Visibility and Analytics Capability	Agency incorporates limited boundary-focused network monitoring capabilities with minimal analysis to start developing centralized situational awareness.	Agency employs network monitoring capabilities based on known indicators of compromise (including network enumeration) to develop situational awareness in each environment and begins to correlate telemetry across traffic types and environments for analysis and threat hunting activities.	Agency deploys anomalybased network detection capabilities to develop situational awareness across all environments, begins to correlate telemetry from multiple sources for analysis, and incorporates automated processes for robust threat hunting activities.	Agency maintains visibility into communication across all agency networks and environments while enabling enterprise-wide situational awareness and advanced monitoring capabilities that automate telemetry correlation across all detection sources.	Cisco Secure XDR Cisco Secure Network Analytics Cisco Secure Client
	Automation and Orchestration Capability	Agency uses manual processes to manage the configuration and resource lifecycle for agency networks and environments with periodic integration of policy requirements and situational awareness.	Agency begins using automated methods to manage the configuration and resource lifecycle for some agency networks or environments and ensures that all resources have a defined lifetime based on policies and telemetry.	Agency uses automated change management methods (e.g., CI/CD) to manage the configuration and resource lifecycle for all agency networks and environments, responding to and enforcing policies and protections against perceived risks.	Agency networks and environments are defined using infrastructure-as-code managed by automated change management methods, including automated initiation and expiration to align with changing needs.	Cisco Secure XDR Cisco Defense Orchestrator Cisco Meraki Systems Manager

CISA Zero Trust Pillar	Function	Traditional	Initial	Advanced	Optimal	Cisco Product
	Governance Capability	Agency implements static network policies (access, protocols, segmentation, alerts, and remediation) with an approach focused on perimeter protections.	Agency defines and begins to implement policies tailored to individual network segments and resources while also inheriting corporate-wide rules as appropriate.	Agency incorporates automation in implementing tailored policies and facilitates the transition from perimeter-focused protections.	Agency implements enterprise-wide network policies that enable tailored, local controls; dynamic updates; and secure external connections based on application and user workflows.	Cisco Secure XDR Cisco Identity Services Engine
Applications and Workloads	Application Access	Agency authorizes access to applications primarily based on local authorization and static attributes.	Agency begins to implement authorizing access capabilities to applications that incorporate contextual information (e.g., identity, device compliance, and/or other attributes) per request with expiration.	Agency automates application access decisions with expanded contextual information and enforced expiration conditions that adhere to least privilege principles.	Agency continuously authorizes application access, incorporating realtime risk analytics and factors such as behavior or usage patterns.	Cisco Secure Workload Cisco Secure XDR with Secure Cloud Insights Cisco Secure Access by Duo
	Application Threat Protection	Agency threat protections have minimal integration with application workflows, applying general purpose protections for known threats. protections for known threats.	Agency integrates threat protections into mission critical application workflows, applying protections against known threats and some application specific threats.	Agency integrates threat protections into all application workflows, protecting against some application-specific and targeted threats.	Agency integrates advanced threat protections into all application workflows, offering real-time visibility and content-aware protections against sophisticated attacks tailored to applications.	Cisco Secure Workload
	Accessible Application	Agency makes some mission critical applications available only over private networks and protected public network connections (e.g., VPN) with monitoring.	Agency makes some of their applicable mission critical applications available over open public networks to authorized users with need via brokered connections.	Agency makes most of their applicable mission critical applications available over open public network connections to authorized users as needed.	Agency makes all applicable applications available over open public networks to authorized users and devices, where appropriate, as needed.	Cisco Umbrella Cisco Secure Firewall Cisco Secure Access by Duo (Duo Network Gateway (DNG))

CISA Zero Trust Pillar	Function	Traditional	Initial	Advanced	Optimal	Cisco Product
	Secure Application Development and Deployment Workflow	Agency has ad hoc development, testing, and production environments with non-robust code deployment mechanisms.	Agency provides infrastructure for development, testing, and production environments (including automation) with formal code deployment mechanisms through CI/CD pipelines and requisite access controls in support of least privilege principles	Agency uses distinct and coordinated teams for development, security, and operations while removing developer access to production environment for code deployment.	Agency leverages immutable workloads where feasible, only allowing changes to take effect through redeployment, and removes administrator access to deployment environments in favor of automated processes for code deployment.	Cisco AppDynamics Cisco Secure Application Cisco Secure Application Cloud Native
	Application Security Testing	Agency performs application security testing prior to deployment, primarily via manual testing methods.	Agency begins to use static and dynamic (i.e., application is executing) testing methods to perform security testing, including manual expert analysis, prior to application deployment.	Agency integrates application security testing into the application development and deployment process, including the use of periodic dynamic testing methods.	Agency integrates application security testing throughout the software development lifecycle across the enterprise with routine automated testing of deployed applications.	Cisco Secure Application
	Visibility and Analytics Capability	Agency performs some performance and security monitoring of mission critical applications with limited aggregation and analytics.	Agency begins to automate application profile (e.g., state, health, and performance) and security monitoring for improved log collection, aggregation, and analytics.	Agency automates profile and security monitoring for most applications with heuristics to identify application-specific and enterprise-wide trends and refines processes over time to address gaps in visibility.	Agency performs continuous and dynamic monitoring across all applications to maintain enterprise-wide comprehensive visibility	Cisco Secure Workload Cisco Secure XDR with Secure Cloud Insights
	Automation and Orchestration Capability	Agency manually establishes static application hosting location and access at provisioning with limited maintenance and review.	Agency periodically modifies application configurations (including location and access) to meet relevant security and performance goals.	Agency automates application configurations to respond to operational and environmental changes.	Agency automates application configurations to continuously optimize for security and performance.	Cisco Secure Workload Cisco Secure XDR with Secure Cloud Insights

CISA Zero Trust Pillar	Function	Traditional	Initial	Advanced	Optimal	Cisco Product
	Governance Capability	Agency relies primarily on manual enforcement policies for application access, development, deployment, software asset management, security testing and evaluation (ST&E) at technology insertion, patching, and tracking software dependencies.	Agency begins to automate policy enforcement for application development (including access to development infrastructure), deployment, software asset management, ST&E at technology insertion, patching, and tracking software dependencies based upon mission needs (for example, with Software Bill of Materials).	Agency implements tiered, tailored policies enterprisewide for applications and all aspects of the application development and deployment lifecycles and leverages automation, where possible, to support enforcement.	Agency fully automates policies governing applications development and deployment, including incorporating dynamic updates for applications through the CI/CD pipeline.	Cisco Secure Workload
Data	Data Inventory Management	Agency manually identifies and inventories some agency data (e.g., mission critical data)	Agency begins to automate data inventory processes for both on-premises and in cloud environments, covering most agency data, and begins to incorporate protections against data loss.	Agency automates data inventory and tracking enterprise-wide, covering all applicable agency data, with data loss prevention strategies based upon static attributes and/or labels.	Agency continuously inventories all applicable agency data and employs robust data loss prevention strategies that dynamically block suspected data exfiltration.	
	Data Categorization	Agency employs limited and ad hoc data categorization capabilities.	Agency begins to implement a data categorization strategy with defined labels and manual enforcement mechanisms.	Agency automates some data categorization and labeling processes in a consistent, tiered, targeted manner with simple, structured formats and regular review.	Agency automates data categorization and labeling enterprise-wide with robust techniques; granular, structured formats; and mechanisms to address all data types.	

CISA Zero Trust Pillar	Function	Traditional	Initial	Advanced	Optimal	Cisco Product
	Data Availability	Agency primarily makes data available from on-premises data stores with some off-site backups.	Agency makes some data available from redundant, highly available data stores (e.g., cloud) and maintains off-site backups for onpremises data.	Agency primarily makes data available from redundant, highly available data stores and ensures access to historical data.	Agency uses dynamic methods to optimize data availability, including historical data, according to user and entity need.	
	Data Access	Agency governs user and entity access (e.g., permissions to read, write, copy, grant others access, etc.) to data through static access controls.	Agency begins to deploy automated data access controls that incorporate elements of least privilege across the enterprise.	Agency automates data access controls that consider various attributes such as identity, device risk, application, data category, etc., and are time limited where applicable.	Agency automates dynamic just-in-time and just-enough data access controls enterprise-wide with continuous review of permissions.	Cisco Umbrella Cisco Cloudlock
	Data Encryption	Agency encrypts minimal agency data at rest and in transit and relies on manual or ad hoc processes to manage and secure encryption keys.	Agency encrypts all data in transit and, where feasible, data at rest (e.g., mission critical data and data stored in external environments) and begins to formalize key management policies and secure encryption keys.	Agency encrypts all data at rest and in transit across the enterprise to the maximum extent possible, begins to incorporate cryptographic agility, and protects encryption keys (i.e., secrets are not hard coded and are rotated on a regular basis).	Agency encrypts data in use where appropriate, enforces least privilege principles for secure key management enterprise-wide, and applies encryption using up-to-date standards and cryptographic agility to the extent possible.	

CISA Zero Trust Pillar	Function	Traditional	Initial	Advanced	Optimal	Cisco Product
	Visibility and Analytics Capability	Agency has limited visibility into data including location, access, and usage, with analysis consisting primarily of manual processes.	Agency obtains visibility based on data inventory management, categorization, encryption, and access attempts, with some automated analysis and correlation.	Agency maintains data visibility in a more comprehensive, enterprisewide manner with automated analysis and correlation and begins to employ predictive analytics.	Agency has visibility across the full data lifecycle with robust analytics, including predictive analytics, that support comprehensive views of agency data and continuous security posture assessment.	Cisco Cloudlock Cisco Umbrella
	Automation and Orchestration Capability	Agency implements data lifecycle and security policies (e.g., access, usage, storage, encryption, configurations, protections, backups, categorization, sanitization) through manual, and potentially ad hoc, processes.	Agency uses some automated processes to implement data lifecycle and security policies.	Agency implements data lifecycle and security policies primarily through automated methods for most agency data in a consistent, tiered, targeted manner across the enterprise.	Agency automates, to the maximum extent possible, data lifecycles and security policies for all agency data across the enterprise.	
	Governance Capability	Agency relies on ad hoc data governance policies (e.g., for protection, categorization, access, inventorying, storage, recovery, removal, etc.) with manual implementation.	Agency defines high-level data governance policies and relies primarily on manual, segmented implementation.	Agency begins integration of data lifecycle policy enforcement across the enterprise, enabling more unified definitions for data governance policies.	Agency data lifecycle policies are unified to the maximum extent possible and dynamically enforced across the enterprise.	

CISA Zero Trust Pillar	Function	Traditional	Initial	Advanced	Optimal	Cisco Product
Cross-Cutting Capabilities	Visibility and Analytics	Agency manually collects limited logs across their enterprise with low fidelity and minimal analysis.	Agency begins to automate the collection and analysis of logs and events for mission critical functions and regularly assesses processes for gaps in visibility.	Agency expands the automated collection of logs and events enterprise-wide (including virtual environments) for centralized analysis that correlates across multiple sources.	Agency maintains comprehensive visibility enterprise-wide via centralized dynamic monitoring and advanced analysis of logs and events.	Cisco Secure XDR Cisco Secure Firewall Cisoc Secure Network Analytics Cisco Secure Client (NVM) Cisco Telemetry Broker
	Automation and Orchestration	Agency relies on static and manual processes to orchestrate operations and response activities with limited automation.	Agency begins automating orchestration and response activities in support of critical mission functions.	Agency automates orchestration and response activities enterprise-wide, leveraging contextual information from multiple sources to inform decisions.	Agency orchestration and response activities dynamically respond to enterprise-wide changing requirements and environmental changes.	Cisco Secure XDR
	Governance	Agency implements policies in an ad hoc manner across the enterprise, with policies enforced via manual processes or static technical mechanisms.	Agency defines and begins implementing policies for enterprise-wide enforcement with minimal automation and manual updates.	Agency implements tiered, tailored policies enterprisewide and leverages automation where possible to support enforcement. Access policy decisions incorporate.	Agency implements and fully automates enterprise-wide policies that enable tailored local controls with continuous enforcement and dynamic updates.	Cisco Secure Access by Duo Cisco Umbrella Cisco Identity Services Engine Cisco Secure Firewall Cisco Secure Workload Cisco Cyber Vision Cisco Network Devices

CISA Zero Trust Pillar	Function	Traditional	Initial	Advanced	Optimal	Cisco Product
						Cisco Wireless Devices

Table 3. CISA Zero Trust Maturity Model mapping to Cisco Product

DISA Zero Trust Framework

The DISA Zero Trust Framework is a set of security principles and best practices developed by the U.S. Defense Information Systems Agency (DISA) to enhance cybersecurity in government agencies and other organizations. The framework is designed to minimize the risk of cyberattacks and data breaches by assuming that no user, device, or network is inherently trusted, and instead verifying each request before granting access to sensitive resources.

Zero Trust Pillars are identified and are in alignment with the common industry identification of Zero Trust Pillars. A Pillar is a key focus area for implementation of Zero Trust controls. Zero Trust is depicted as interlocking puzzle pieces below that symbolize a data Pillar surrounded by Pillars of protection. All protection Pillars work together to effectively secure the Data Pillar.

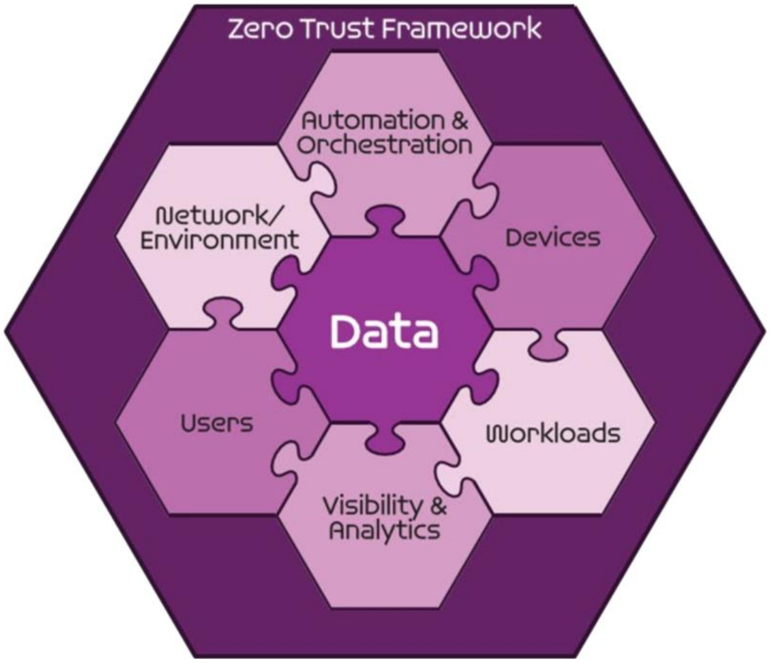

Figure 4. **DISA Zero Trust Pillars**

To implement the DISA Zero Trust Framework, organizations typically adopt a multi-layered approach that includes technologies such as network segmentation, identity and access management (IAM), privileged access management (PAM), and continuous monitoring and threat detection tools. This approach helps organizations to maintain a high level of security and reduce the risk of data breaches and cyberattacks.

Appendix

Appendix A – References

- Cisco Zero Trust Security
- Zero Trust: Going Beyond the Perimeter
- Cisco Secure Workload
- Cisco Software-Defined Access
- Cisco SAFE
- Cisco Zero Trust Architecture Guide
- Cisco Zero Trust: User and Device Design Guide (CVD)
- Cisco Zero Trust: Network and Cloud Security Design Guide (CVD)
- CISA Zero Trust Maturity Model V2.0
- NIST Special Publication 800-207 – Zero Trust Architecture
- DISA Zero Trust Framework

Appendix B – Feedback

If you have feedback on this document, please send an email to ask-security-cvd@cisco.com.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.