Zero Trust Frameworks

Architecture Guide

June, 2022

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

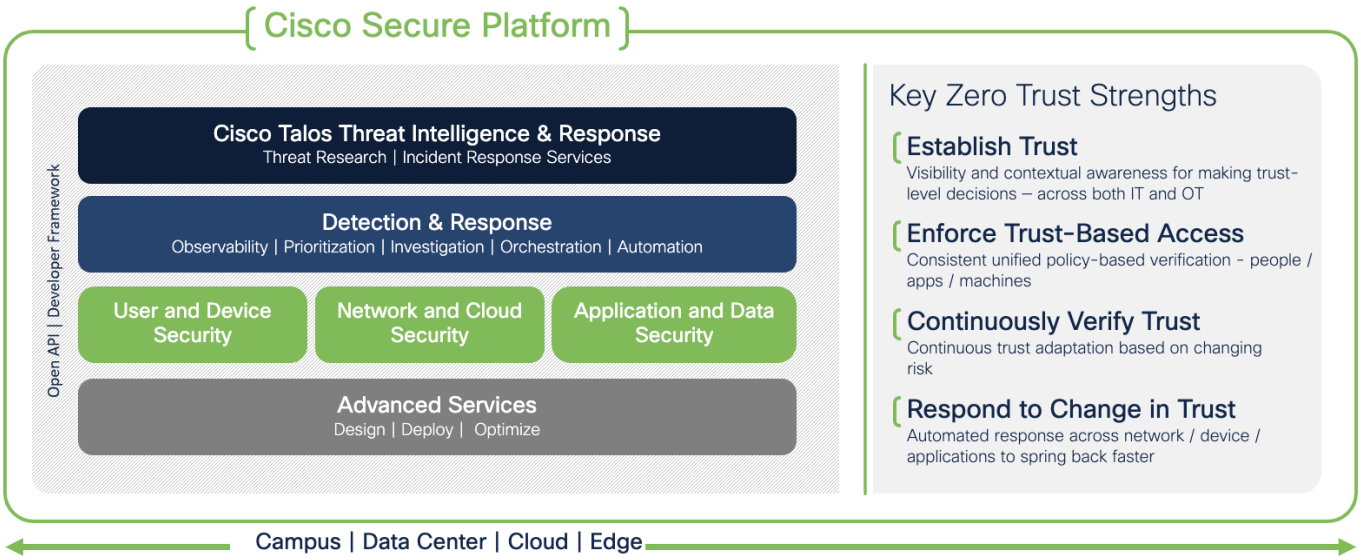

Figure 1. Cisco Zero Trust Framework

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**: making sure 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**: preventing unauthorized access within application environments irrespective of where they are hosted

Zero Trust Security Frameworks

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

Cisco	NIST Cyber Security Framework	CISA	Common
User and Device Security	Users	Identity	Visibility & Analytics Automation & Orchestration Governance
	Devices	Device	
Network and Cloud Security	Networks/Hybrid Multi-Cloud	Network/ Environment	
Application and Data Security	Applications	Application Workload	

Cisco	NIST Cyber Security Framework	CISA	Common
	Data	Data	

National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (NIST) defines Zero Trust as: " Zero trust 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. ZTA (Zero Trust Architecture) 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."

Cybersecurity & Infrastructure Security Agency (CISA)

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.

NIST Special Publication 800-207 – Zero Trust Architecture

NIST Special Publication 800-207 – Zero Trust Architecture

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

	Logical Component	Cisco Product
Policy Decision Point (PDP)	Policy Engine (PE)	Cisco Secure Access by Duo Cisco Umbrella Cisco Identity Services Engine Cisco Secure Firewall Cisco Secure Workload
	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
Control Plane	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
	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
	Industry Compliance System	Cisco Secure Access by Duo Cisco Identity Services Engine Cisco Secure Network Analytics

	Logical Component	Cisco Product
	Public Key Infrastructure	Cisco Secure Access by Duo Cisco Umbrella Cisco Identity Services Engine Cisco Network Devices
Data Plane	Policy Enforcement Point	Cisco Secure Access by Duo Cisco Umbrella Cisco Identity Services Engine Cisco Secure Firewall Cisco Secure Workload Cisco Network Devices
	Threat Intelligence Feed(s)	Cisco Secure Firewall Cisco Identity Services Engine Cisco SecureX Cisco Talos Cisco Secure Insights Cisco Network Devices
	Network and System Activity Logs	Cisco Secure Access by Duo Cisco Secure Application Cisco Secure Application Cloud Native Cisco Network Devices
	ID Management System	Cisco Secure Access by Duo Cisco Identity Services Engine Cisco Network Devices
	Security Information and Event Management (SIEM)	

NIST Cybersecurity Framework

The NIST Cybersecurity Framework is a set of guidelines and best practices to help organizations build and improve their cybersecurity posture. The framework puts forth a set of recommendations and standards that enable organizations to be better prepared in identifying and detecting cyber-attacks, and provides guidelines on how to respond, prevent, and recover from cyber incidents.

The following table shows how Cisco Security products map to the NIST Cybersecurity Framework.

Asset	Identify	Protect	Detect	Respond	Recover
Users	Cisco Secure Access by Duo	Cisco Secure Access by Duo	Cisco Secure Access by Duo	Cisco Secure Access by Duo	Cisco Professional Services
Data	Cisco SecureX		Cisco SecureX	Cisco SecureX	Cisco Professional Services
Applications	Cisco Secure Workload Cisco Secure Application Cisco Secure Application Cloud Native Cisco SecureX	Cisco Secure Workload Cisco Secure Application Cisco Secure Application Cloud Native	Cisco Secure Workload Cisco SecureX	Cisco SecureX	Cisco Professional Services
Devices	Kenna Security Cisco SecureX	Cisco Secure Endpoint Cisco Secure Malware Analytics Kenna Security	Cisco Secure Endpoint Cisco Secure Malware Analytics Cisco Secure Connector Cisco SecureX	Cisco SecureX	Cisco Professional Services
Networks/Hybrid Multi-Cloud	Cisco Secure Email Cisco Identity Services Engine Cisco Secure Analytics Cisco AnyConnect Cisco Secure	Cisco Secure Email Cisco Identity Services Engine Cisco Secure Analytics Cisco AnyConnect Cisco Secure	Cisco Secure Email Cisco Identity Services Engine Cisco Umbrella Cisco SD-WAN Cisco Secure Firewall	Cisco Secure Email Cisco Identity Services Engine Cisco Umbrella Cisco Secure Firewall Cisco SecureX	Cisco Professional Services

Asset	Identify	Protect	Detect	Respond	Recover
	Firewall Cisco Secure Web Appliance Cisco SecureX	Firewall Cisco Secure Web Appliance Cisco SD-WAN Cisco Umbrella Cisco Secure Cloud Analytics	Cisco Secure Web Appliance Cisco Secure Cloud Analytics Cisco SecureX		

CISA Zero Trust Maturity Model

CISA Zero Trust Maturity Model

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

Pillar	Function	Traditional	Advanced	Optimal	Cisco Product
Identity	Authentication	Agency authenticates identity using either passwords or multi-factor authentication (MFA).	Agency authenticates identity using MFA.	Agency continuously validates identity, not just when access is initially granted.	Cisco Secure Access by Duo
	Identity Stores	Agency only uses on-premises identity providers.	Agency federates some identity with cloud and on-premises systems.	Agency has global identity awareness across cloud and on-premises environments.	Cisco Secure Access by Duo
	Risk Assessment	Agency makes limited determinations for identity risk.	Agency determines identity risk based on simple analytics and static rules.	Agency analyzes user behavior in real time with machine learning algorithms to determine risk and deliver ongoing protection.	Cisco SecureX with Secure Cloud Insights with JupiterOne
	Visibility and Analytics Capability	Agency segments user activity visibility with basic and static attributes.	Agency aggregates user activity visibility with basic attributes and then analyzes and reports for manual refinement.	Agency fully orchestrates the identity lifecycle Dynamic user profiling, dynamic identity and group membership, just-in-time and just-enough access controls are implemented.	Cisco SecureX with Cisco Secure Access by Duo
	Automation and Orchestration Capability	Agency manually administers and orchestrates (replicates) identity and credentials.	Agency uses basic automated orchestration to federate identity and permit administration across identity stores.	Agency fully automates technical enforcement of policies. Agency updates policies to reflect new orchestration options.	Cisco SecureX with Cisco Secure Access by Duo
	Governance Capability	Agency manually audits identities and permissions after initial provisioning using static technical enforcement of credential policies (e.g., complexity, reuse, length, clipping, MFA, etc.).	Agency uses policy-based automated access revocation. There are no shared accounts.		Cisco SecureX with Cisco Secure Access by Duo

Pillar	Function	Traditional	Advanced	Optimal	Cisco Product
Device	Compliance Monitoring	Agency has limited visibility into device compliance.	Agency employs compliance enforcement mechanisms for most devices.	Agency constantly monitors and validates device security posture.	Cisco Secure Access by Duo Cisco Identity Services Engine
	Data Access	Agency's access to data does not depend on visibility into the device that is being used to access the data.	Agency's access to data considers device posture on first-access.	Agency's access to data considers real-time risk analytics about devices.	Cisco Secure Endpoint
	Asset Management	Agency has a simplified and manually-tracked device inventory.	Agency uses automated methods to manage assets, identify vulnerabilities, and patch assets.	Agency integrates asset and vulnerability management across all agency environments, including cloud and remote.	Cisco SecureX with Device Insights and Meraki Mobile Device Management
	Visibility and Analytics Capability	Agency's device management relies upon manual inspections of labels and periodic network discovery and reporting.	Agency reconciles device inventories against sanctioned lists with isolation of non-compliant components.	Agency continuously runs device posture assessments (e.g., using endpoint detection and response (EDR) tools).	Cisco SecureX with Device Insights and Meraki Mobile Device Management
	Automation and Orchestration Capability	Agency manually provisions devices with static capacity allocations.	Agency provisions devices using automated, repeatable methods with policy-driven capacity allocations and reactive scaling.	Agency's device capacity and deployment uses continuous integration and continuous deployment (CI/CD) principles with dynamic scaling.	Cisco SecureX with Device Insights and Meraki Mobile Device Management
	Governance Capability	Agency manually defines and enforces device acquisition channels and establishes and implements inventory frequency policy. Device retirement requires extensive sanitation to remove residual access and data.	Agency devices natively support modern security functions in hardware. Agency minimizes the quantity of legacy equipment that is unable to perform desired security functions.	Agency devices permit data access and use without resident plain-text copies, reducing asset supply chain risks.	Cisco SecureX with Device Insights and Meraki Mobile Device Management
Network/ Environment	Network Segmentation	Agency defines their network architecture using large perimeter/ macro-segmentation.	Agency defines more of their network architecture by ingress/egress micro- perimeters with some internal micro- segmentation.	Agency network architecture consists of fully distributed ingress/egress micro- perimeters and deeper internal microsegmentation based around application workflows.	Cisco Secure Firewall Cisco Identity Services Engine Cisco SD-WAN with Meraki Cisco SD-WAN with Viptela Cisco Secure Workload
	Threat Protection	Agency bases threat protections primarily on known threats and static traffic filtering.	Agency includes basic analytics to proactively discover threats.	Agency integrates machine learning-based threat protection and filtering with context-based signals.	Cisco Talos Cisco Secure Firewall Cisco SecureX

Pillar	Function	Traditional	Advanced	Optimal	Cisco Product
	Encryption	Agency explicitly encrypts minimal internal or external traffic.	Agency encrypts all traffic to internal applications, as well as some external traffic.	Agency encrypts all traffic to internal and external locations, where possible.	Cisco Secure Firewall Cisco SD-WAN with Meraki Cisco SD-WAN with Viptela
	Visibility and Analytics Capability	Agency provides visibility at perimeter with centralized aggregation and analysis.	Agency integrates analysis across multiple sensor types and positions with manual policy-driven alerts and triggers.	Agency integrates analysis across multiple sensor types and positions with automated alerts and triggers.	Cisco SecureX Cisco Secure Network Analytics
	Automation and Orchestration Capability	Agency manually initiates and executes network and environment changes following change management workflows.	Agency uses automated workflows to manually initiate network and environment changes.	Agency network and environment configurations use infrastructure-as-code, with pervasive automation, following (CI/CD) deployment models.	Cisco SecureX Cisco Defense Orchestrator Cisco Meraki Systems Manager
	Governance Capability	Agency uses manual policies to identify sanctioned networks, devices, and services, with manual discovery and remediation of unauthorized entities.	Agency uses manual policies to identify sanctioned networks, devices, and services, with alerts and triggers and manual remediation for unauthorized entities.	Agency uses automated discovery of networks, devices, and services, with manual or dynamic authorization and automated remediation of unauthorized entities.	Cisco SecureX Cisco Identity Services Engine
Application Workload	Access Authorization	Agency's access to applications is primarily based on local authorization and static attributes.	Agency's access to applications relies on centralized authentication, authorization, monitoring, and attributes.	Agency continuously authorizes access to applications, considering real-time risk analytics.	Cisco Secure Workload Cisco SecureX with Secure Cloud Insights with JupiterOne
	Threat Protection	Agency threat protections have minimal integration with application workflows, applying general purpose protections for known threats.	Agency has basic integration of threat protections into application workflows, primarily applying protections for known threats with some application-specific protections.	Agency strongly integrates threat protections into application workflows, with analytics to provide protections that understand and account for application behavior.	Cisco Talos Cisco Secure Workload
	Accessibility	Some critical cloud applications are directly accessible to users over the internet, with all others available through a virtual private network (VPN).	All cloud applications and some on-premises applications are directly accessible to users over the internet, with all others available through a VPN.	All applications are directly accessible to users over the internet.	Cisco Umbrella Cisco Secure Firewall Cisco Secure Access by Duo (Duo Network Gateway (DNG))
	Application Security	Agency performs application security testing prior to deployment, primarily through static and manual testing methods.	Agency integrates application security testing into the application development and deployment process, including the use of dynamic testing	Agency integrates application security testing throughout the development and deployment process, with regular automated testing of deployed	Cisco Secure Application Cisco Secure Application Cloud Native

Pillar	Function	Traditional	Advanced	Optimal	Cisco Product
			methods.	applications.	
	Visibility and Analytics Capability	Agency performs application health and security monitoring in isolation of external sensors and systems.	Agency performs application health and security monitoring in context with some external sensors and systems.	Agency performs continuous and dynamic application health and security monitoring with external sensors and systems.	Cisco Secure Workload Cisco SecureX with Secure Cloud Insights with JupiterOne
	Automation and Orchestration Capability	Agency establishes application hosting location and access at provisioning.	Applications can inform device and network components of changing state.	Applications adapt to ongoing environmental changes for security and performance optimization.	Cisco Secure Workload Cisco SecureX with Secure Cloud Insights with JupiterOne
	Governance Capability	Agency has legacy policies and conducts manual enforcement for software development, software asset management, security tests and evaluations (ST&E) at technology insertion, and tracking software dependencies.	Agency has updated policies and centralized enforcement.	Agency has updated policies and dynamic enforcement.	Cisco Secure Workload
Data	Inventory Management	Agency manually categorizes data and has poor data inventorying, leading to inconsistent categorization.	Agency primarily inventories data manually with some automated tracking. Agency performs data categorization using a combination of manual and static analysis methods.	Agency continuously inventories data with robust tagging and tracking. Agency augments categorization with machine learning models.	Cisco Umbrella Cisco Cloudlock
	Access Determination	Agency governs access to data by using static access controls.	Agency governs access to data using least privilege controls that consider identity, device risk, and other attributes.	Agency's access to data is dynamic, supporting just- in-time and just-enough principles, and continual risk-based determinations.	Cisco Umbrella Cisco Cloudlock Cisco Secure Access by Duo
	Encryption	Agency primarily stores data in on-premises data stores and where they are unencrypted at rest.	Agency stores data in cloud or remote environments where they are encrypted at rest.	Agency encrypts all data at rest.	
	Visibility and Analytics Capability	Agency has limited data inventories that prevent useful visibility and analytics except possibly in specific circumstances.	Most of the agency's data are inventoried and can be accounted for since the last inventory update. Analytics are limited to plaintext data.	Agency's data are inventoried and can always be accounted for. Agency logs and analyzes all access events for suspicious behaviors. Agencies perform analytics on encrypted data.	
	Automation and Orchestration Capability	Agency lacks consistent categorization and labeling, which prevents automation	Agency runs scheduled audits that locate high- value data and analyze access controls.	Agency automatically enforces strict access controls for high-value data. All	

Pillar	Function	Traditional	Advanced	Optimal	Cisco Product
		and orchestration. Some data management tasks run automatically.	There is limited automatic orchestration to apply controls and ensure backups are in place.	high-value data is backed up regardless of its storage location. Data inventories are automatically updated.	
	Governance Capability	Agency largely enforces data protection and handling policies through administrative controls. Data categorization and data access authorizations are largely defined by distributed decision making.	Agency enforces data protections through mostly technical and some administrative controls. Data categorization and data access authorizations are defined with a method that better integrates diverse data sources.	Agency automatically always enforces data protections required by policy. Data categorization and data access authorizations are defined using a fully unified approach that integrates data, independent of source.	

Appendix

Appendix A - References

- Cisco Zero Trust Security
- Zero Trust: Going Beyond the Perimeter
- Cisco Secure Workload
- Software-Defined Access
- Cisco SAFE

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**.