Framework Mapping: Cisco Duo + CISA Zero Trust Maturity Model

Background

As U.S. Public Sector organizations transition toward a Zero Trust Architecture (ZTA), they align their strategies with the Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model (ZTMM) and National Institute of Standards and Technology (NIST) SP 800-207.

Cisco Duo is a premier solution for accelerating Zero Trust adoption, specifically designed to address the "Identity" and "Device" components of the framework. Duo provides a cloud-native approach to securing access to any application from any device. Duo acts as a critical **Policy Decision Point (PDP)**, ensuring that only trusted users and healthy devices can access protected resources.

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 (acts 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 Duo meets the CISA ZTMM standards.

[1] Visibility and Analytics enable organizations to monitor and analyze behavior and events across the five pillars. This foundation capability provides the data-driven insights necessary to identify anomalies, detect threats, and enforce Zero Trust polices.

[2] Automation and Orchestration ensure that Zero Trust principles are implemented consistently and efficiently across the five pillars. By automating security tasks and orchestrating responses, organizations can reduce human error and improve reaction times to potential threats.

[3] Governance ensures that security policies, processes, and compliance requirements are well-defined and constantly applied across all pillars. It provides the overarching framework for decision-making, accountability, and adherence to organizational goals and regulatory mandates.

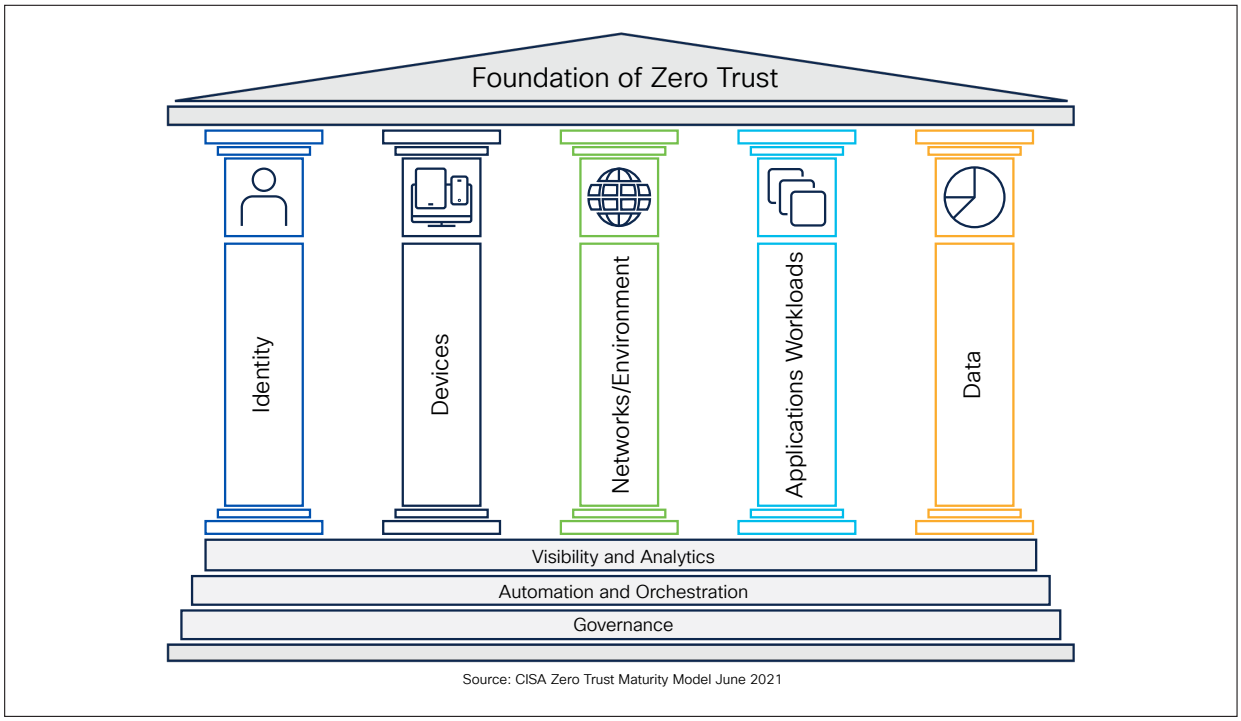

Figure 1. CISA Zero Trust Maturity Model

Duo's Role in the Five PIllars

Duo is a cornerstone of the Identity and Device pillars, with significant contributions to the Application Workload pillar.

- **Identity:** Duo provides industry-leading Multi-Factor Authentication (MFA), Single Sign-On (SSO), and risk-based authentication to ensure that identities are verified continuously.
- **Device:** Duo provides deep visibility into every device (managed or unmanaged) accessing applications, performing health checks and posture assessments before granting access.
- **Network / Environment:** Cisco Duo does not directly provide network-level segmentation or traffic control capabilities; it plays a critical role within Cisco's broader Zero Trust architecture.
- **Application Workload:** Duo protects individual applications—whether on-premises or in the cloud—by enforcing granular access policies at the application layer.
- **Data:** Duo protects data indirectly by ensuring that only authorized users on compliant devices can reach the applications where sensitive data resides.

Mapping to the CISA Zero Trust Five Pillars

Table 1. Mapping Cisco Duo Capabilities to the CISA Zero Trust Identity Pillar – Authentication and Identity Stores

CISA Zero Trust Pillars	CISA Functions	Cisco Duo Status	Cisco Duo Capabilities	Notes
Identity	Authentication	Optimal	Phishing-Resistant Multi-Factor Authentication (MFA)	Duo supports a variety of phishing-resistant methods including Proximity Verification via Bluetooth Low Energy (BLE), passwordless (including complete passwordless at user enrollment), and Fast IDentity Online 2 (FIDO2) security keys to provide strong MFA for all users attempting to access resources.
			Flexible Authenticator Support	Duo enables MFA with support for a wide range of authentication methods, including number-matching push verification, biometrics, security keys, phone call, and SMS. Users can authenticate using their PC or laptop, smartphone, tablet and select smartwatches.
			User Identity Verification	Duo provides multi-layered identity verification protecting self-service and help desk interactions. Help Desk Push enables IT staff to send verification requests to users' enrolled devices before privileged actions (password resets, device changes). Integration with Persona delivers government ID verification and biometric facial recognition for high-assurance help desk authentication.
			Adaptive and Conditional Access Policies	Duo enforces granular access policies based on user roles, device posture, geographic location, security agents, OS currency, IP-based targets, anonymous networks, and other contextual factors, simultaneously applying least-privilege principles to restrict access only to necessary resources.
			Device Trust Establishment	Duo continuously verifies device health and security policy compliance (e.g., OS version, screen lock, antivirus status) at every access attempt, ensuring that only trusted devices can access applications.
			Risk-Based Authentication	Duo's Risk-based Authentication analyzes user and device behavior patterns to detect anomalies and automatically prompt additional "step-up" authentication or block access in real time when unusual activity is detected.
			Broad MFA Coverage	Duo protects access to all applications, whether on-premises or in the cloud, including coverage for legacy authentication protocols – NT LAN Manager (NTLM) and Kerberos.
	Identity Stores	Advanced	Synchronized Integration with Identity Providers	Duo's Identity Routing Engine and System for Cross-domain Identity Management (SCIM) provisioning allow for just-in-time, seamless orchestration of identities across a global, multi-vendor ecosystem. Duo Directory synchronizes user and group data from external directories via the Duo Authentication Proxy (for on-premises like Active Directory and Lightweight Directory Access Protocol (LDAP) or direct cloud connections (Security Assertion Markup Language (SAML), for providers like Entra and Okta). Syncs run automatically—with high-frequency sync options.
			Hosted Identity Store	Duo Directory supports multiple deployment options-flexibly meeting customers where they are or need. Organizations can host users directly in Duo without requiring an external identity store. Duo can also run as a sidecar directory, ideal for third-party (contractor/partner/vendor) management and scenarios requiring data sovereignty. Duo can run as a secure identity broker layer in front of multiple Identity Providers (IdPs), (ex: larger organizations, mergers & acquisitions, etc.) - where Duo provides a consistent and secure policy across the hybrid organization (ex: passwordless).

Table 2. Mapping Cisco Duo Capabilities to the CISA Zero Trust Device Identity Pillar – Risk Assessments, Access Management, and Visibility and Analytics

CISA Zero Trust Pillars	CISA Functions	Cisco Duo Status	Cisco Duo Capabilities	Notes
Identity	Risk Assessments	Optimal	Continuous Monitoring and Risk Assessments	Cisco Duo enables evaluation of user posture and risk at continuous intervals to ensure access remains compliant with Zero Trust policies. This includes dynamic risk-based access decisions that adapt based on real-time user and device context.
			Cross-Platform Risk Assessment	Duo Identity and Access Management (IAM) uses Identity Intelligence to deliver end-to-end visibility into access entitlements, enabling least privilege and reducing identity sprawl across hybrid environments. It aggregates identity data from core sources (e.g., Duo, Entra ID, Okta), business apps (GitHub, Salesforce, Google Workspace), and Human Resource Information Systems (HRIS) like Workday, then intelligently merges accounts into a unified source of truth. Identity Intelligence reduces certification fatigue with filtering and context. Shows complete group membership chains with attribution, change logs, and app-access mappings. Admins can identify over-privileged users, export entitlements, and use HRIS correlation to surface orphaned accounts from terminated employees who still have access.
			User Trust Level	Identity Intelligence synthesizes four risk dimensions—inherent (role-based targeting), posture (authentication hygiene), behavioral (baseline deviations), and action (per-event context)—into a unified Untrusted-to-Trusted scale. This User Trust Level can be used to inform access decisions across Cisco Secure Access, Firewall policies, and XDR investigations.
			Threat Research	In addition to an in-house threat research team, Duo integrates with Cisco Talos to get updated threat intelligence.
	Access Management	Initial	Just-In-Time Access	Duo can implement practical Just-in-Time (JIT) access patterns by issuing user-scoped, admin-generated secret that lets an approved user complete authn to a resource for a bounded window.
			Dynamic Policy Enforcement	Duo enforces conditional access policies that grant or restrict access based on user roles, device posture, and contextual factors, supporting privileged access management. Duo transitions “Access Management” from a static gatekeeper to a dynamic orchestrator that responds to changes in risk on a per-application basis.
			Least Privilege Access Policies	Through Cisco policy enforcement, Duo applies least-privilege principles by restricting access to only the resources required for a user’s role and/or device posture.
			Device Trust	Duo provides device visibility and health checks for all integrated, integrating device posture into access decisions to ensure secure access.
			Adaptive Access Policies	Duo supports adaptive access policies that dynamically adjust access permissions based on real-time risk assessments and contextual information.
	Visibility and Analytics Capability	Optimal	Threat Intelligence Analytics	Cisco Identity Intelligence (CII) provides comprehensive analytics spanning all connected identity providers. The platform analyzes all ingested data through both dedicated check logic and advanced AI and ML techniques. Intelligence establishes behavioral baselines to detect account compromise, insider threats, and automated attacks. Cisco Identity Intelligence integrates with Talos®, Cisco XDR, and Security Information and Event Management (SIEM) tools like Splunk. It participates in a data sharing ecosystem with partners and security vendors to enhance security effectiveness.

Table 3. Mapping Cisco Duo Capabilities to the CISA Zero Trust Identity Pillar – Automation and Orchestration and Governance

CISA Zero Trust Pillars	CISA Functions	Cisco Duo Status	Cisco Duo Capabilities	Notes
Identity	Automation and Orchestration Capability	Advanced	Policy-Based Enforcement Point	Cisco SaaS-based policy and access control dynamically enforce access policies based on user identity, device posture, and contextual factors. This enforcement applies to both remote and on-premises users.
			Identity Management	Duo Directory serves as a flexible, secure source of truth for primary authentication and can operate standalone or integrate with existing IAM systems. The platform supports integrations with major identity data sources through event streaming, directory synchronization, and inbound SCIM provisioning.
			Automated Provisioning	Use Duo to automatically provision, maintain, and deprovision users and groups into supported downstream SAML and OpenID Connect (OIDC) single sign-on (SSO) service provider applications. SCIM 2.0 support allows real-time provisioning changes from source systems.
			Multiple-IdP Routing Rules	Duo SSO adds support for simultaneously authenticating users to multiple SAML identity providers and multiple AD sources. Routing Rules also improves the well-adopted support for multiple AD sources by allowing for more targeted requests to the proper AD environment.
	Governance Capability	Advanced	Role-Based Access Policy Syncs	Duo syncs user roles from primary identity stores and applies least privileged access policies through administrative units, administrative roles, and user group-based policy for segmented permissions.
			Access Review Support	Identity Intelligence reduces certification fatigue with filtering and context. Shows complete group membership chains with attribution, change logs, and app-access mappings. Admins can identify over-privileged users, export entitlements, and use HRIS correlation to surface orphaned accounts from terminated employees who still have access.
			AI-Driven Policy Optimization	Cisco AI Assistant for Identity helps optimize policy updates by analyzing auth logs, detecting access anomalies, and providing intelligent troubleshooting recommendations. Risk-Based Authentication employs machine learning to establish behavioral baselines and automatically step-up authentication requirements.
			Posture Enforcement	Duo enables continuous monitoring of user and device posture, helping organizations enforce hygiene through access policies. Cisco Identity Intelligence supports ongoing risk assessments and compliance monitoring with automated checks for identity posture.
			Dynamic Policy Enforcement	Dynamic policy enforcement grants privileged access based on user roles, device posture, and contextual factors. Demonstrates consistent policy application, least-privilege enforcement, and auditable controls for federal requirements.
			Detailed Reporting and Audit Capabilities	Offers detailed compliance reports and audit logs for regulatory and governance needs, including system-wide reporting and user device posture reports.
			Continuous Monitoring and Risk Assessments	Evaluates both user and device posture continuously to ensure access remains compliant with Zero Trust policies.

CISA Zero Trust Network/Environment Pillar – Cisco Duo doesn't handle network segmentation, but it strengthens Cisco's Zero Trust strategy by enforcing adaptive user and device authentication before access. Combined with Cisco's broader Zero Trust stack (SD-WAN, identity-based segmentation, and Security Service Edge), Duo helps deliver an identity-driven approach that reduces implicit trust and improves network security.

Table 4. Mapping Cisco Duo Capabilities to the CISA Zero Trust Device Pillar

CISA Zero Trust Pillars	CISA Functions	Cisco Duo Status	Cisco Duo Capabilities	Notes
Device	Policy Enforcement & Compliance Monitoring	Initial	Device Visibility & Inventory	Duo captures details on every device (OS, browser, plugins) that touches the environment, including Bring Your Own Device (BYOD).
			Device Health Checks	Duo blocks access if a device is out of date, lacks encryption, or has security features (like screen lock) disabled. Users are providing step-by-step instructions to bring the device back into compliance without needing to create a Help Desk ticket.
			Trusted Endpoints	Duo uses certificates and device identifiers to distinguish between registered and unregistered devices, whether corporate-managed or unmanaged to establish trust.
	Asset & Supply Chain Risk Management	Traditional	Device Visibility	Duo adds visibility into accessing devices including third-party supply chain devices. Duo integrates with Cisco Identity Services Engine (ISE) for more granular asset control.
	Resource Access (formerly Data Access)	Advanced	Adaptive Policies	Duo's adaptive policies enforce least-privilege access by restricting resource access based on user roles, device posture, and contextual factors, enabling secure, VPN-less access to corporate applications and data. This continuous verification approach prevents unauthorized lateral movement and protects against compromised credentials and risky devices, aligning with zero trust principles for resource access.
			Desktop Health Check	Duo Desktop provides device insights at each authentication to provide up-to-date device health. In addition, it provides Trusted Endpoint capabilities to restrict access to known, trusted devices.
			Device Visibility	Duo collects and verifies device attributes (e.g., OS/patch level, certificate validation, jailbreak/root status, endpoint security signals via integrations) during authentication.
			Trusted Endpoints	Duo lets you define and manage trusted endpoints and grant secure access to your organization's applications with policies that verify systems using Duo application verification or management status.
	Device Threat Protection	Initial	Multi-Factor Authentication (MFA)	Verifies user identity at every access attempt to ensure only authorized users gain access.
			Device Health Checks	Duo Desktop provides device insights at each authentication to provide up to date device health. In addition, it provides Trusted Endpoint capabilities to restrict access to known, trusted devices.
			Adaptive Access Policies	Enforce least-privilege access by restricting resource access based on user roles, device posture, and contextual factors.
	Visibility and Analytics Capability	Advanced (supports)	Device Inventory & Health	Duo collects device insights on user authenticating devices including desktops and laptops, mobile phones, tablets, and their virtual devices. Duo offers visibility into device health status through comprehensive logging and reporting, dashboard, and anomaly risk signals.
			Non-Human Identity Visibility	Identity Intelligence offers a variety of continuous checks for non-human identity credential use, expiration, and management - ensuring timely resets and proper use. Duo IAM leverages a machine identity discovery engine to identify AI agent accounts through behavioral signatures and user type classification across integrated platforms. The platform distinguishes AI agents from traditional service accounts by analyzing authentication patterns, Application Programming Interface (API) call frequencies, resource access scope, and inter-system communication behaviors.

Table 5. Mapping Cisco Duo Capabilities to the CISA Zero Trust Application Workload Pillar

CISA Zero Trust Pillars	CISA Functions	Cisco Duo Status	Cisco Duo Capabilities	Notes
Application Workload	Application Access (formerly Access Authorization)	Advanced	Application Access Admin Panel	Duo provides a dashboard of all integrated cloud and on-premises applications being accessed by the enterprise.
			Risk-Based Authentication	Duo provides the option to set per-application access policies informed by user attributes, device compliance, geolocation, and other contextual analytics for real-time risk-based authentication.
			Duo Passport	Share remembered device sessions between your applications when accessed from a browser or from a desktop client with Duo Passport, Duo Desktop, and a remembered devices policy applied to applications. When you use Duo Passport with Duo Authentication for Windows Logon and Duo SSO, users can sign in to Windows with Duo and then seamlessly access browser and desktop applications without needing to re-enter their service credentials or repeat Duo two-factor authentication (2FA).
			Identity Intelligence	Identity Intelligence analyzes application access across all identity stores and reduces certification fatigue with filtering and context. Shows complete group membership chains with attribution, change logs, and app-access mappings. Admins can identify over-privileged users, export entitlements, and use HRIS correlation to surface orphaned accounts from terminated employees who still have access.
			Application Entitlement Hygiene	The Applications tab in CII highlights unused application assignments, identifying over-provisioned access and licenses. Admins can compare median apps per user against department/org benchmarks to spot entitlement anomalies.
	Application threat Protections (formerly Threat Protections)	Initial	User Identity Verification and MFA	Cisco Duo provides strong user identity verification and multi-factor authentication to in front of application access attempts, protecting against known and novel identity-based threats on a per-application basis.
			Identity Intelligence	Identity Intelligence detects anomalies in application access based on known and novel threat detections. Continual checks provide posture recommendations to protect against identity-based attacks. Identity Posture Score weights entitlement risk by severity and population impact, prioritizing remediation of privilege sprawl.
	Access Applications (formerly Accessibility)	Initial	Duo Network Gateway	Duo provides users with secure remote access to your on-premises private applications and internal servers without having to worry about managing VPN credentials.
			Policy Settings	Duo can limit authentications to requests coming from specified networks, as part of granular policy setting.

Table 6. Mapping Cisco Duo Capabilities to the CISA Zero Trust Data Pillar

CISA Zero Trust Pillars	CISA Functions	Cisco Duo Status	Cisco Duo Capabilities	Notes
Data	Data Access	Initial	User and Device Trust	Duo controls access to applications and data. Duo provides continuous verification of user identity through MFA and device health checks, ensuring that only authorized users and compliant devices can access applications which house sensitive data.
			Role-Based Access Controls	Duo Administrative roles and granular policy engine allows per-user group role-based access controls to applications which house sensitive data.
	Visibility and Analytics Capability	Traditional	Logging	Duo provides visibility into user location, device health, and authentication outcome, at point of authentication.

Key observations

- **Identity and Device Leader:** Duo is purpose-built for the first two pillars of the CISA model. It excels at verifying "Who" is connecting and "What" they are connecting with.
- **Ease of Deployment:** Unlike network-heavy Zero Trust implementations, Duo can be deployed rapidly to protect SaaS and on-premises applications, providing an immediate jump in Zero Trust maturity.
- **Complementary to ISE:** While ISE manages the Network (Pillar 3), Duo manages the Application Access (Pillar 4). Together, they provide a full-stack Zero Trust solution.
- **Visibility:** Duo provides unique visibility into the "Shadow IT" and BYOD landscape, which is a core requirement for the CISA "Device" pillar.

Summary

Cisco Duo is an essential component of a CISA-aligned Zero Trust roadmap. It provides the necessary controls to move from "Traditional" to "Advanced" or "Optimal" maturity levels in the Identity and Device pillars by implementing phishing-resistant MFA, continuous risk assessment, and deep identity intelligence with device health visibility.

Resources

For more information, please refer to the following:

Getting Started with Duo

Security First IAM