Framework Foundations: Zero Trust Models – CISA, DoD, and NIST

Introduction to the Zero Trust Models

The Zero Trust Model is a cybersecurity framework built on the principle of “never trust, always verify.” It assumes that threats can originate from both inside and outside the network perimeter, and therefore requires continuous validation of every user, device, and application attempting to access resources.

Three major frameworks guide Zero Trust implementation across federal and defense environments:

- **CISA’s Zero Trust Maturity Model 2.0** (2023) offers a flexible, agency-driven roadmap structured around five pillars – Identity, Devices, Networks, Applications & Workloads, and Data – plus three cross-cutting capabilities: Visibility & Analytics, Automation & Orchestration, and Governance.
- **DoD’s Zero Trust Strategy** (2022) provides a more prescriptive, mission-aligned approach with seven pillars and 45 mapped capabilities, targeting full adoption across all DoD components by FY 2027.
- **NIST SP 800-207 Zero Trust Architecture** (2020) defines the foundational principles of Zero Trust for federal agencies. It emphasizes continuous verification, strict access control, and dynamic policy enforcement across users, devices, and workloads.

Objectives

- Eliminate implicit trust by continuously validating access based on identity, context, and risk.
- Minimize attack surface, prevent lateral movement, and enhance real-time threat detection and response.
- Align cybersecurity with mission resilience to ensure secure operations across all environments.
- Enable dynamic policy enforcement and continuous monitoring across all enterprise assets, as emphasized by NIST SP 800-207.

Key Requirements

Despite structural differences, the CISA, DoD, and NIST Zero Trust frameworks share the foundational goal of eliminating implicit trust and enforcing continuous, risk-based access control. All three emphasize identity-centric security, dynamic policy enforcement, continuous monitoring, and automated response as core elements of Zero Trust. While implementation approaches vary–CISA offers a flexible maturity model, DoD provides a prescriptive strategy, and NIST defines the architectural principles–they align on key requirements such as:

CISA Zero Trust Maturity Model

- 5 Pillars: Identity, Devices, Networks, Applications and Workloads, Data
- 3 Cross-Cutting Capabilities: Visibility and Analytics, Automation and Orchestration, Governance
- 4 Maturity Levels: Traditional → Initial → Advanced → Optimal
- Flexible Implementation: Agencies tailor adoption based on mission needs and existing infrastructure
- Alignment with OMB M-22-09: Federal mandate for Zero Trust adoption

DoD Zero Trust Strategy

- 7 Pillars: User, Device, Network/ Environment, Application and Workload, Data, Visibility and Analytics, Automation and Orchestration
- 45 Capabilities: Mapped to each pillar for comprehensive coverage
- Prescriptive Execution: Mission-driven implementation across DoD components
- Target Timeline: Full Zero Trust adoption by FY 2027

NIST SP 800-207 Zero Trust Architecture

- 3 Core Components: Policy Engine, Policy Administrator, Policy Enforcement Point
- 5 Key Tenets: Secure all communications, dynamic access, continuous verification, least privilege, resource-based access
- Architecture Focus: Defines principles and logical components for Zero Trust implementation
- Vendor-Neutral Guidance: Adaptable to hybrid environments and existing infrastructure

How Cisco + Splunk Support Compliance

Cisco offers a comprehensive portfolio of security solutions that can help organizations meet the requirements of Zero Trust.

Zero Trust Requirement	How Cisco + Splunk Supports Compliance	Relevant Products
Identity Verification (CISA, DoD, NIST)	Centralized identity management, multi-factor authentication, and identity-based access control.	Cisco Duo, Cisco Identity Services Engine (ISE), Cisco Secure Access, Splunk Enterprise Security (ES), Splunk SOAR
Device Security (CISA, DoD, NIST)	Endpoint protection, device compliance enforcement, and visibility into device posture.	Cisco Secure Endpoint, Cisco Secure Access, Meraki Systems Manager, Splunk Enterprise, Splunk User Behavior Analytics (UBA)
Network Segmentation (CISA, DoD, NIST)	Role-based access control, DNS-layer security, and network segmentation.	Cisco Secure Firewall, Cisco Umbrella, Cisco Secure Access, Splunk ES, Splunk IT Service Intelligence (ITSI)
Application Security (CISA, DoD, NIST)	Threat detection, application visibility, and workload protection.	Cisco XDR, Talos Threat Intelligence, Splunk ES, Splunk SOAR
Data Protection (CISA, DoD, NIST)	Data encryption, secure communications, and malware protection.	Cisco Umbrella, Cisco Secure Access, Cisco Secure Email, Splunk ES, Splunk Enterprise
Visibility and Analytics (CISA, DoD, NIST)	Centralized logging, behavioral analytics, and threat correlation.	Cisco Secure Network Analytics (SNA), Cisco XDR, Splunk Enterprise, Splunk ES
Automation and Orchestration (CISA, DoD, NIST)	Automated security workflows, response actions, and cloud-native orchestration.	Cisco XDR, Splunk SOAR, Splunk ITSI
Governance (CISA)	Policy enforcement, compliance monitoring, and configuration management.	Cisco XDR, Cisco Splunk ES, Splunk Enterprise
User Security (DoD)	User authentication, access control, and identity enforcement.	Cisco Duo, Cisco ISE, Cisco Secure Access, Splunk ES
Environment Security (DoD)	Encrypted traffic inspection, secure web gateway, and infrastructure protection.	Cisco Secure Firewall, Cisco Umbrella, Cisco Secure Access, Splunk ES, Splunk Enterprise

Zero Trust Requirement	How Cisco + Splunk Supports Compliance	Relevant Products
Policy Decision Framework (NIST)	Centralized policy engine and enforcement points for dynamic access control.	Cisco Secure Access, Cisco ISE, Splunk SOAR, Splunk ES
Session-Based Access Control (NIST)	Per-session authorization and continuous validation of user/resource interactions.	Cisco Duo, Cisco Secure Access, Splunk ES
Resource-Based Access (NIST)	Treats all data and services as resources; accses is granted based on identity and context.	Cisco Umbrella, Cisco Secure Access, Cisco Secure Firewall, Splunk ES

Zero Trust Compliance with Cisco Security + Splunk

As federal agencies and defense organizations accelerate their transition to Zero Trust, the need for integrated, scalable, and mission-aligned security solutions has never been greater. Whether following CISA's flexible maturity model, DoD's prescriptive strategy, or NIST's architectural blueprint, the core principle remains the same: trust is never assumed—access must be continuously verified.

Cisco and Splunk together provide a strong foundation for Zero Trust implementation across all three frameworks. Cisco delivers identity verification, device compliance, network segmentation, and dynamic policy enforcement. Splunk adds centralized visibility, behavioral analytics, and automation for adaptive access decisions and rapid incident response.

Our integrated solutions align with CISA, DoD, and NIST SP 800-207, supporting automated enforcement, session-based access control, and scalable deployment. By adopting Cisco and Splunk, organizations can strengthen resilience, reduce risk, and ensure secure, mission-ready operations across hybrid environments.

Resources

For more information and guidance on Zero Trust compliance, please refer to the following resources:

- Cisco: What is Zero Trust?
- Cisco Zero Trust Security
- How Splunk Supports the DoD's Zero Trust Strategy
- Splunk: The Essential Guide to Zero Trust