Framework Mapping: Cisco and Splunk + DoD Zero Trust

As the Department of Defense advances its Zero Trust Architecture (ZTA) journey, agencies must align with the DoD Zero Trust Strategy and Zero Trust Capability Execution Roadmap, informed by NIST SP 800-207.

The DoD Zero Trust model defines seven interconnected pillars that enable consistent implementation, continuous verification, least-privilege access, and rapid response across DoD environments.

Zero Trust within the DoD is not a single product or control—it is a continuous verification model that assumes breach, minimizes implicit trust, and dynamically enforces least-privilege access across users, devices, networks, applications, and data.

Applying this Zero Trust approach also helps DoD organizations support compliance with key mandates and initiatives, including Comply-to-Connect (C2C) and evolving DoD CIO and OMB cybersecurity requirements. These mandates emphasize continuous monitoring, validated device and user trust, improved visibility, and rapid response to cyber threats.

DoD Zero Trust at a Glance

Establish Trust
- Verify user and service identity
- Assess device health and posture
- Apply risk-based authentication

Enforce Least-Privilege Access
- Explicit, policy-based access
- Identity-driven microsegmentation
- Minimum access per request

Continuously Verify Trust
- Ongoing trust reassessment
- Behavioral and risk analytics
- Shared security signals

Respond to Changes in Trust
- Rapid threat investigation
- Automated response workflows
- Coordinated remediation actions

DoD Zero Trust Pillars

The DoD Zero Trust model organizes required capabilities across seven pillars:

User
Verifies user and non-person entity identities at every access request using strong authentication, behavior, and contextual risk rather than static credentials.

Device
Ensures devices accessing DoD resources are identified, monitored, and assessed for security posture, with trust decisions based on device health and compliance.

Application & Workload
Protects applications and services by controlling access and continuously validating interactions and runtime behavior across on-premises and cloud environments.

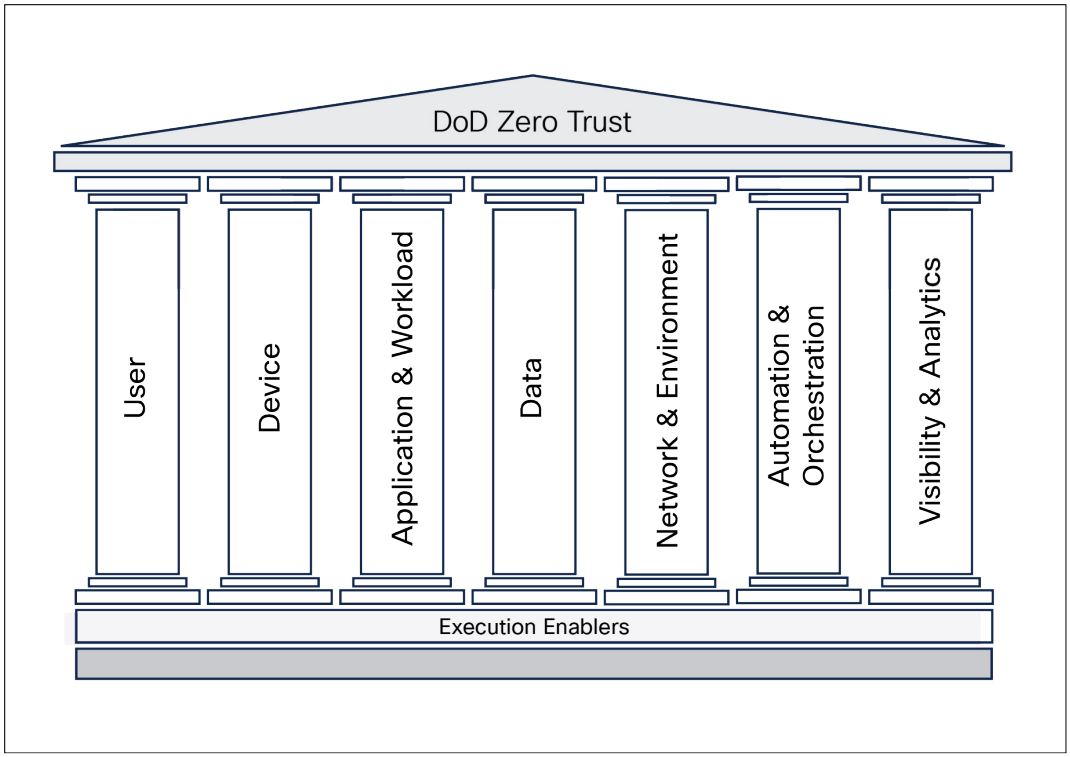
Data
Safeguards data through classification, access controls, encryption, and monitoring, enforcing access dynamically based on identity, device, and mission context.

Network & Environment
Secures connectivity using identity-based controls, segmentation, and encryption to reduce attack surface and limit lateral movement.

Automation & Orchestration
Applies Zero Trust policies at scale through automation, enabling rapid response, coordinated remediation, and consistent enforcement.

Visibility & Analytics
Provides foundational insight by collecting and correlating telemetry across all pillars to enable continuous trust assessment and threat detection.

These pillars function as an integrated system– maturity gains in on pillar amplify effectiveness across the others.



Cisco + Splunk: Unified Zero Trust Platform

Cisco + Splunk's unified Zero Trust Platform integrates security, networking, and analytics to help DoD organizations implement Zero Trust consistently across all pillars of the DoD Zero Trust model. Rather than addressing Zero Trust as a collection of point solutions, Cisco + Splunk delivers a coordinated, platform-based approach that aligns policy, enforcement, and intelligence across the entire environment.

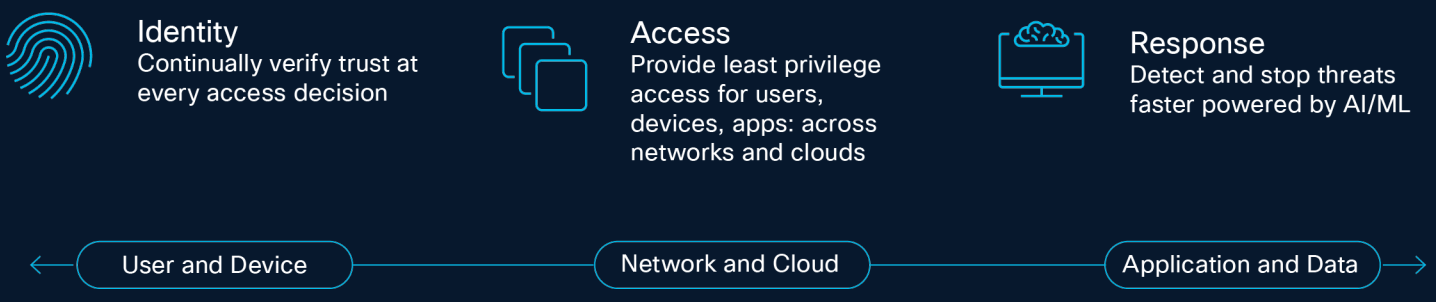
Cisco Security provides the enforcement foundation across the User, Device, Network & Environment, Application & Workload, and Data pillars. Cisco security capabilities enable continuous verification of users and devices, identity-driven access to applications and data, segmented and protected networks, and secure workloads across on-premises, cloud, tactical, and classified environments. By embedding security controls directly into access and connectivity layers, Cisco Security enables least-privilege access decisions to be enforced dynamically and as close to the point of access as possible.

Splunk, as a core component of the platform, underpins the Visibility & Analytics pillar by aggregating and correlating telemetry across users, devices, networks, applications, and security controls. This unified visibility provides the shared signals required to continuously assess trust, identify anomalous behavior, and inform policy enforcement across all Zero Trust pillars.

Together, Cisco Security and Splunk enable:

- Unified visibility across all Zero Trust pillars
- Policy-driven enforcement based on identity, device posture, and behavior
- Accelerated threat detection and response through integrated analytics
- Automated orchestration of security and IT workflows

This platform approach is critical for DoD organizations, where Zero Trust must function across hybrid, multicloud, disconnected, classified, and mission-critical environments. Cisco One with Splunk allows DoD organizations to advance Zero Trust maturity while leveraging existing investments and supporting mission continuity.



Role of Cisco and Splunk Across the Zero Trust Pillars

Cisco Security and Splunk work together to enable Zero Trust outcomes across all DoD Zero Trust pillars by combining policy-based enforcement, secure connectivity, and advanced analytics. Cisco provides the controls that establish and enforce trust at access points across users, devices, networks, applications, and data, while Splunk delivers the shared visibility, analytics, and operational intelligence required to continuously assess and respond to risk.

User & Device Pillars

Trust begins with strong identity and device verification. Cisco Duo, Identity Services Engine (ISE), and Secure Client support phishing-resistant authentication, identity federation, device posture assessment, and conditional access. Device and endpoint security is further strengthened through Cisco Secure Endpoint and CyberVision, providing visibility into managed, unmanaged, and operational technology (OT) assets. These capabilities ensure that access decisions account for identity, device health, and contextual risk at every request.

Network & Environment

Cisco enables identity-based networking and secure connectivity through Cisco SD-Access, Catalyst SD-WAN, Secure Firewall, and Catalyst Center. These solutions enforce segmentation, encrypted communications, and least-privilege access across enterprise, hybrid cloud, and tactical environments. Isovalent Enterprise extends Zero Trust principles into cloud-native and containerized networking environments.

Application & Workload

Applications and workloads are protected through controlled access, segmentation, and continuous monitoring. Secure Workload enforces workload visibility and segmentation, while Hybrid Cloud (DC-Cloud) capabilities support consistent Zero Trust controls across on-premises and cloud environments. Secure Access further enables policy-driven access to applications regardless of location.

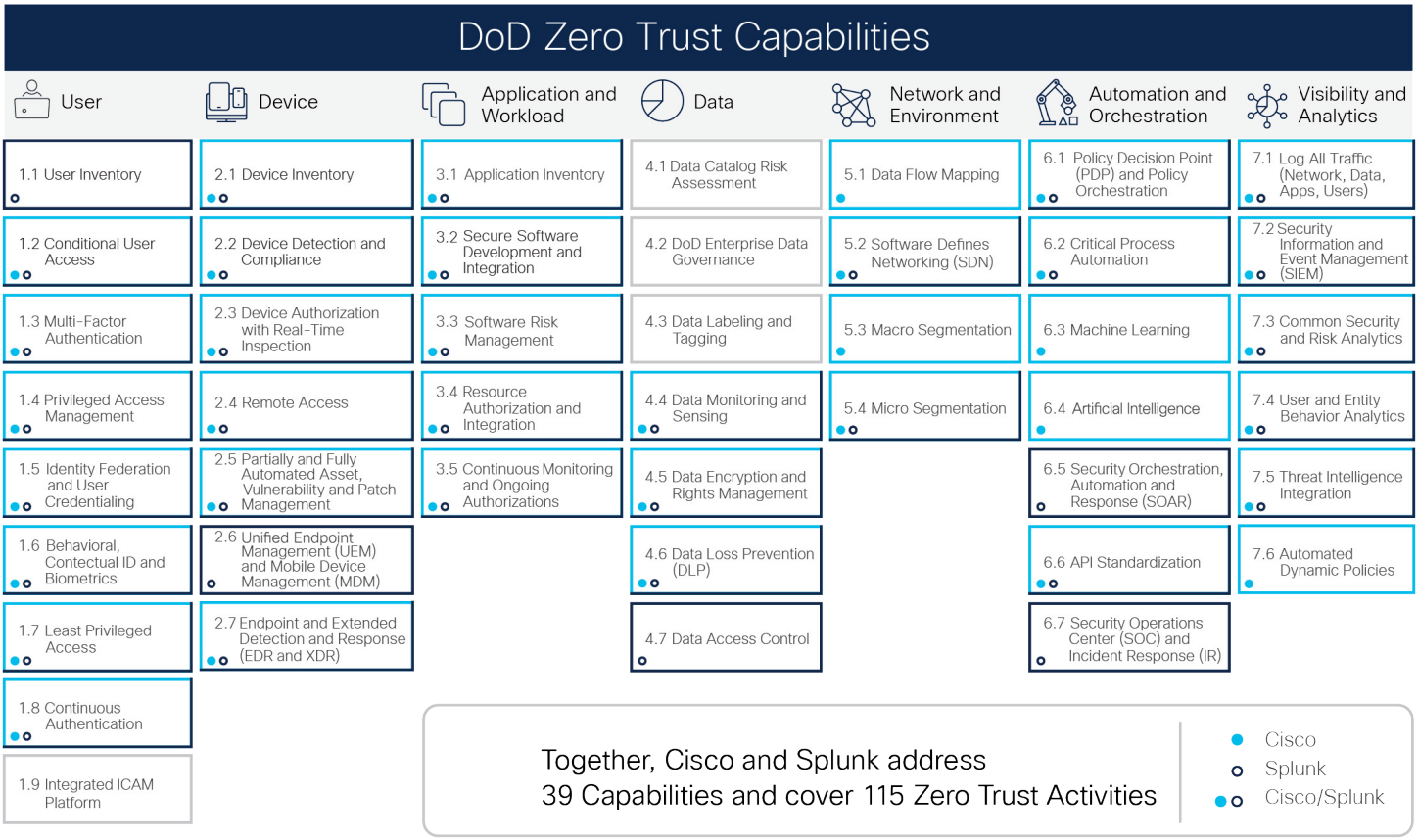
Data

Cisco security technologies help protect data through access controls, monitoring, and threat prevention. Secure Email, Secure Firewall, and Security Cloud Control reduce the risk of data loss, exfiltration, and policy violations by enforcing protections at key access and inspection points.

Visibility, Analytics, and Operations

Splunk Enterprise, Splunk Enterprise Security (SIEM), Splunk User Behavior Analytics (UBA), and Splunk IT Service Intelligence (ITSI) underpin the Visibility & Analytics pillar by aggregating and correlating telemetry from Cisco security, networking, endpoints, applications, and third-party systems. Splunk SOAR enables the Automation & Orchestration pillar by supporting investigation, coordinated response, and automated remediation across the Zero Trust architecture. Cisco Secure Analytics and Logging strengthens telemetry integration and operational insight.

These capabilities help DoD organizations respond to changes in trust in near real time, reducing dwell time and operational risk.



Cisco Solution	Zero Trust Capability
Cisco Identity Services Engine (ISE)	1.2, 1.4, 1.7, 1.8, 2.1–2.4, 5.2–5.4, 6.1
Cisco Secure Network Analytics (SNA)	1.6, 3.5, 4.5, 5.1, 7.1–7.4
Cisco Catalyst Center	1.6, 5.1–5.3, 6.4, 7.3, 7.4, 7.6
Cisco Secure Client	2.2–2.4, 4.5, 5.1, 5.4, 7.1, 7.4
Cisco Secure Firewall	2.2, 2.4, 4.5, 5.3, 5.4, 6.1, 6.3
Cisco Secure Workload	3.1, 3.3, 5.1, 5.4, 6.1, 7.3
Cisco Duo	1.2, 1.3, 1.5, 1.6, 7.2
Cisco CyberVision	2.2, 5.1, 7.1, 7.4
Isovalent Enterprise	3.2–3.4, 6.6
Cisco Secure Access	1.2, 2.2, 2.4, 4.4, 4.6, 7.5
Cisco Secure Endpoint	2.7
Cisco Secure Web Appliance	4.4, 4.6
Cisco Secure Email	4.6
Cisco Secure Analytics & Logging	7.1
Cisco Security Cloud Control	6.1

Cisco Enterprise Networking	Facilitates Zero Trust Capability
Cisco SD-Access	1.2–1.4, 1.6–1.8, 2.1–2.4, 3.3, 3.5, 4.5, 5.1, 5.2, 5.4, 6.1–6.3, 7.3, 7.4
Cisco Catalyst SD-WAN	1.2–1.4, 1.6–1.8, 2.1–2.4, 3.3, 3.5, 4.4–4.6, 5.1, 5.2, 5.4, 6.1–6.3, 7.3
Cisco Hybrid Cloud (DC-Cloud)	1.2–1.4, 1.6–1.8, 2.1–2.4, 3.3, 3.5, 4.5, 5.1–5.4, 6.1–6.3

Splunk Solution	Zero Trust Capability
Splunk Enterprise	1.1–1.3, 1.7, 2.3, 2.6, 4.4, 7.1
Splunk Enterprise Security (ES)	1.3–1.5, 1.8, 2.1–2.7, 3.2–3.5, 4.4, 4.6–4.7, 5.2, 5.4, 6.1, 6.5, 6.7, 7.1–7.5
Splunk SOAR	1.3, 1.5, 1.6, 1.8, 2.1–2.7, 3.3–3.5, 4.4, 4.6, 4.7, 5.2, 5.4, 6.1, 6.2, 6.5–6.7, 7.2, 7.5
Splunk IT Service Intelligence (ITSI)	2.1, 2.3–2.6, 3.1–3.4, 6.5, 7.1–7.4
Splunk User Behavior Analytics (UBA)	1.3–1.6, 1.8, 2.3, 4.4, 7.2–7.4