DoD Zero Trust capability mapping

Cisco + Splunk

A Zero Trust model of security prompts organizations to assess trust at every access attempt.

Our view is that a Zero Trust approach should:

- **Establish trust for users**, devices and applications trying to access an environment
- **Enforce trust-based access** based on the principle of least privilege, only granting access to applications and data that users/devices explicitly need
- **Continuously verify trust** to detect any change in risk even after initial access is granted
- **Respond to change in trust** by investigating and orchestrating response to potential incidents

With this approach, agencies gain better visibility across users, devices, networks, containers, and applications, because they can verify temporal security state and apply risk-based policy with every access attempt. Organizations can also reduce their attack surface by segmenting resources and granting the absolute minimum access needed per request. Applying this Zero Trust model helps entities comply with DoD Comply-to-Connect (C2C), Executive Order 14028, NSM-8, and OMB mandates. End users ultimately get a more consistent and productive security experience - regardless of their location, which endpoints are used, or where their applications live in today's hybrid cloud environments.

Establish Trust

- User / Device / Service Identity
- Posture + context
- Risk-based authentication

Enforce Trust Based Access

- Micro-segmentation
- Unified access control
- Least privilege + explicit trust

Continuously Verify Trust

- Re-assessment of trust
- Indicators of compromise
- Shared signals
- Behavior monitoring - threat and non-threat activity
- Vulnerability management

Respond to Change in Trust

- Prioritize incident response
- Orchestrated remediation
- Integrated + open workflows

Better together

Cisco and Splunk help create a digital world that is safer and more resilient. Our technologies can assist the DoD in their Zero Trust (ZT) initiative, as stated in the DoD Zero Trust Capability Execution Roadmap and the DoD Zero Trust Strategy. Cisco and Splunk enable "Cross-Pillar Capabilities" with data and network telemetry this provides profound Visibility and Analytics and empowering Automation and Orchestration.

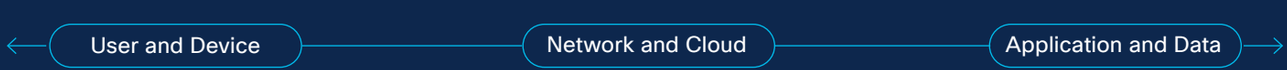
Cisco's Security portfolio offers extensive threat intelligence and advanced analytics which enhances visibility and control across users, devices, networks and applications. Splunk is a data-driven, open, integrated networking and security platform with hundreds of integrations to other technologies supporting existing environments. Splunk also supports multicloud monitoring and Splunk Cloud SaaS offering is authorized and accredited to FedRAMP Moderate, High, and IL5 standards. Additionally, Splunk has numerous existing deployments in on-premises and highly-classified environments throughout the DoD and Federal Government. Our architects are available to help find the best solution for any situation.

The DoD Zero Trust Strategy outlines a seven pillar zero trust model and associated capabilities, to standardize the way missions and programs implement and adopt zero trust principles. The comprehensive portfolio that Cisco and Splunk brings to the DoD can help integrate data, networking, and security solutions to bring together zero trust outcomes more efficiently with improved user and operator experience.

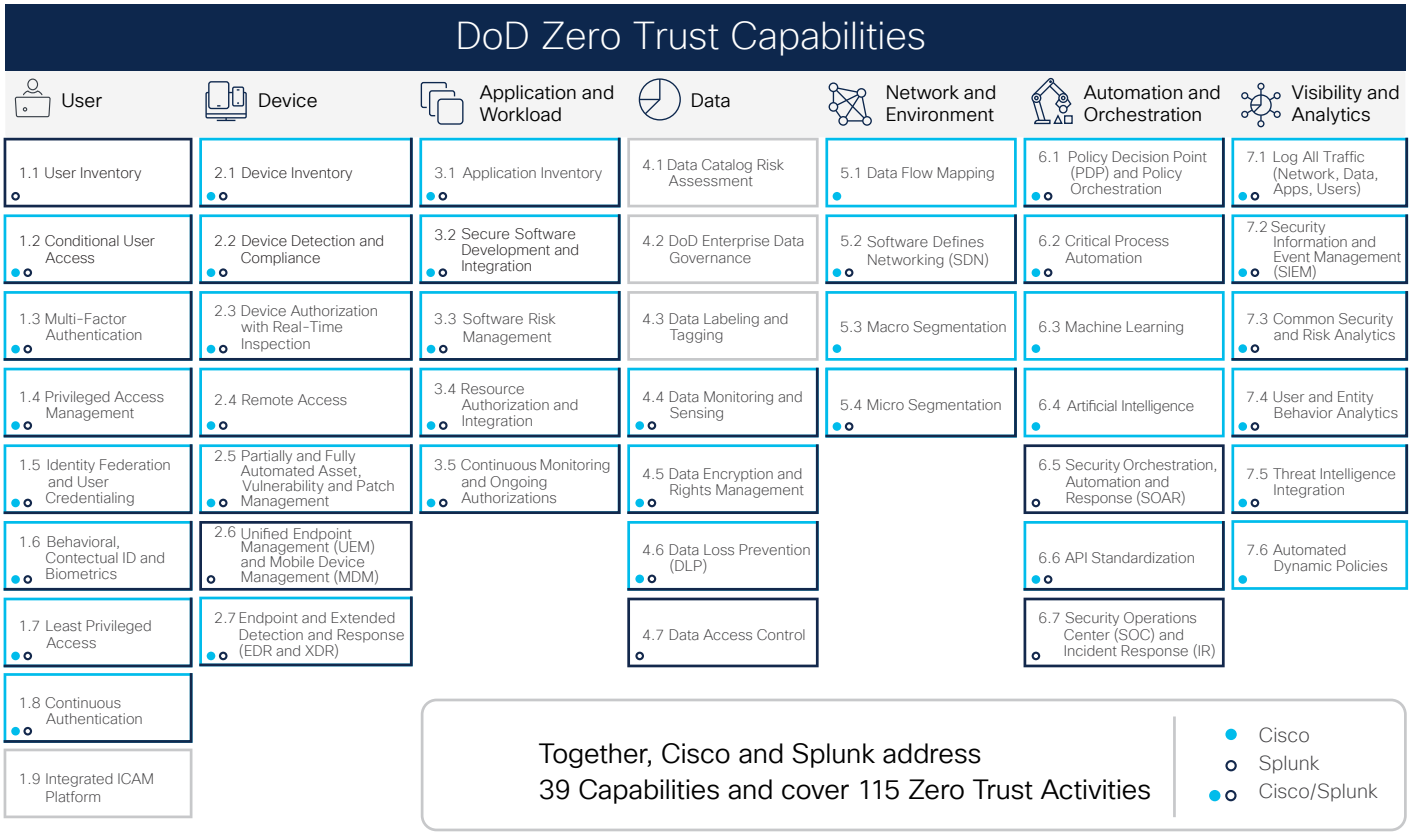
Identity
Continually verify trust at every access decision

Access
Provide least privilege access for users, devices, apps: across networks and clouds

Response
Detect and stop threats faster powered by AI/ML



DoD Zero Trust Capabilities



Cisco Solution	Zero Trust Capability
Cisco Identity Services Engine	1.2, 1.4, 1.7, 1.8, 2.1–2.4, 5.2–5.4, 6.1
Cisco Secure Network Analytics	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
Panoptica	3.2–3.4, 6.6
Kenna Security	3.3, 7.3, 7.5
Cisco Umbrella SIG/Investigate	4.4, 4.6, 7.5
Cisco Secure Endpoint	2.7
Cisco Email	4.6
Cisco Secure Analytics and Logging	7.1

Cisco Enterprise Networking	Facilitates ZT Capabilities
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
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
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 Capabilities
Splunk Enterprise	1.1–1.3,1.7, 2.3, 2.6, 4.4, 7.1
Splunk Enterprise Security	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, 2.2–2.7, 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 ITSI	2.1, 2.3–2.6, 3.1–3.4, 6.5, 7.1–7.4
Splunk UBA	1.3–1.6, 1.8, 2.3, 4.4, 7.2–7.4

1476243197 10/24