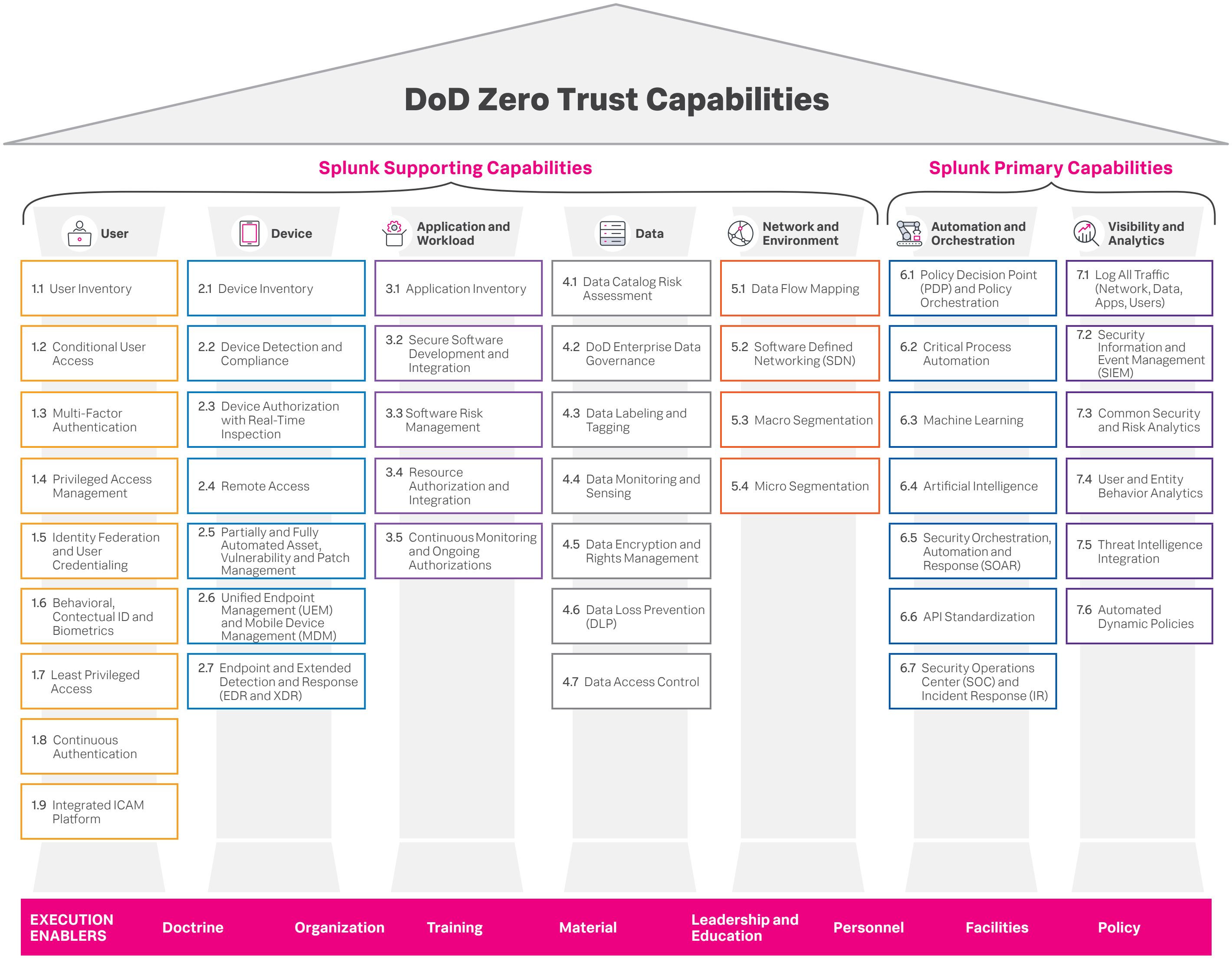
splunk>

SOLUTION GUIDE

How Splunk Supports the DoD's Zero Trust Strategy

Splunk aims to create a digital world that is safer and more resilient. Splunk 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. Specifically, Splunk technology supports the "Cross-Cutting Capabilities" identified in CISA's Zero Trust Maturity Model, such as Visibility and Analytics, Automation and Orchestration, and Governance. Splunk also aligns with the additional pillars by integrating with those technologies to have a holistic view into the environment.

Splunk supports any environment and has existing integrations with hundreds of other technologies to support existing architectures and seamless additions afterward. Splunk supports multicloud monitoring and Splunk's Cloud SaaS offering can handle sensitive information up to FedRAMP high and IL5. Additionally, Splunk can be deployed on-premises for air-gapped or highly classified areas. Splunk's architects are available to help find the best solution for any situation.



DoD Zero Trust Capabilities

Splunk Supporting Capabilities (User, Device, Application and Workload, Data, Network and Environment)

Splunk Primary Capabilities (Automation and Orchestration, Visibility and Analytics)

User	Device	Application and Workload	Data	Network and Environment	Automation and Orchestration	Visibility and Analytics
1.1 User Inventory	2.1 Device Inventory	3.1 Application Inventory	4.1 Data Catalog Risk Assessment	5.1 Data Flow Mapping	6.1 Policy Decision Point (PDP) and Policy Orchestration	7.1 Log All Traffic (Network, Data, Apps, Users)
1.2 Conditional User Access	2.2 Device Detection and Compliance	3.2 Secure Software Development and Integration	4.2 DoD Enterprise Data Governance	5.2 Software Defined Networking (SDN)	6.2 Critical Process Automation	7.2 Security Information and Event Management (SIEM)
1.3 Multi-Factor Authentication	2.3 Device Authorization with Real-Time Inspection	3.3 Software Risk Management	4.3 Data Labeling and Tagging	5.3 Macro Segmentation	6.3 Machine Learning	7.3 Common Security and Risk Analytics
1.4 Privileged Access Management	2.4 Remote Access	3.4 Resource Authorization and Integration	4.4 Data Monitoring and Sensing	5.4 Micro Segmentation	6.4 Artificial Intelligence	7.4 User and Entity Behavior Analytics
1.5 Identity Federation and User Credentialing	2.5 Partially and Fully Automated Asset, Vulnerability and Patch Management	3.5 Continuous Monitoring and Ongoing Authorizations	4.5 Data Encryption and Rights Management		6.5 Security Orchestration, Automation and Response (SOAR)	7.5 Threat Intelligence Integration
1.6 Behavioral, Contectual ID and Biometrics	2.6 Unified Endpoint Management (UEM) and Mobile Device Management (MDM)		4.6 Data Loss Prevention (DLP)		6.6 API Standardization	7.6 Automated Dynamic Policies
1.7 Least Privileged Access	2.7 Endpoint and Extended Detection and Response (EDR and XDR)		4.7 Data Access Control		6.7 Security Operations Center (SOC) and Incident Response (IR)	
1.8 Continuous Authentication						
1.9 Integrated ICAM Platform						

EXECUTION ENABLERS	Doctrine	Organization	Training	Material	Leadership and Education	Personnel	Facilities	Policy

Figure 1: Splunk abilities across the Zero Trust pillars

Pillar capabilities

The DoD Zero Trust Capability Execution Roadmap defines each pillar by a list of capabilities. This is how Splunk maps to our primary capabilities in the Visibility and Analytics and the Automation and Orchestration pillars. The numbering below matches Figure 1 above and the Execution Roadmap for easy cross-referencing.

Pillar 6: Automation and orchestration

6.1 Policy decision point (PDP) and policy orchestration

After an agency documents their rule-based policies to orchestrate across the security stack, the policy rules are replicated in Splunk. Splunk monitors data from across the organization which allows it to detect cross-pillar activity and make resourcing decisions. Splunk's vast network of integrations enables orchestration based on these predefined policy violations.

6.2 Critical process automation

Splunk's Security Orchestration, Automation, and Response (SOAR) solution addresses repeatable, repetitive tasks such as data enrichment, security controls and incident response workflows. Splunk SOAR has over 60 existing playbooks with more added regularly.

6.3 Machine learning

Splunk has multiple machine learning capabilities. Our User Behavior Analytics (UBA) solution uses machine learning to baseline behavior and detect anomalies, especially in insider threats. Our Machine Learning Toolkit (MLTK) allows for rapidly developing machine learning techniques using common algorithms for tagging and faster incident identification and response. The Splunk App for Data Science and Deep Learning supports advanced, custom algorithms and workflows using Jupyter Labs Notebooks.

6.4 Artificial intelligence

Splunk IT Service Intelligence (ITSI) leverages artificial intelligence for IT operations (AIOps). It provides visibility into the health of critical IT and business services and their infrastructure. This allows ITSI to organize and correlate events cross-functionally and understand their service context for quicker investigations, root cause analysis and reduced time to incident resolution.

Our Risk-based alerting capabilities provide for cumulative risk scoring. It enriches events with additional context from industry-standard cybersecurity mappings, such as the MITRE ATT&CK Framework. The risk score is assigned to assets and identities based on this context and other contributing information such as critical system tagging.

6.5 Security Orchestration, Automation and Response (SOAR)

Splunk SOAR has over 60 pre-defined playbooks helping DoD agencies achieve rapid operational capability with existing security technologies to orchestrate and automate policies and rulesets. These policies and rulesets improve security operations, threat and vulnerability management, and security incident response by ingesting alert data and triggering playbooks for automated response and remediation.

6.6 API standardization

Splunk follows the REpresentational State Transfer (REST) API standard. We have existing integrations with hundreds of the most common security tool providers. These are easily found on our application database, Splunkbase. Documentation of our API calls can be found on our REST API Reference Manual.

6.7 Security operations center (SOC) and incident response (IR)

Splunk Enterprise Security (Splunk ES) currently has over 1,400 detection analytics and over 180 analytic stories for threat identification. This works directly with Splunk SOAR, which has over 60 playbooks available. As the SIEM industry recognized leader by three independent market analyst reports, our platform already has integrations with the most common cybersecurity technologies. Splunk provides the overall enterprise security view for security operations centers (SOCs) including both upward and downward visibility. This results in standardized, coordinated and accelerated incident response and investigative efforts.

Pillar 7: Visibility and analytics

Splunk products are actively used in DOD customer security operations center (SOC) and Cyber Security Service Provider (CSSP) environments and encapsulated in various weapons systems. Splunk provides for log collection, parsing and analysis. Splunk ES is the SIEM industry leader. Gartner's SIEM Magic Quadrant has recognized Splunk ES as a leader for 9 years straight. Splunk ES provides for common and advanced security and risk analytics. Splunk UBA is our user and entity behavior analytics platform. Threat intelligence solutions include Splunk Threat Intelligence Management (TIM) a feature of Splunk ES and integrations with other leading threat intelligence providers. Splunk continues to expand capabilities through our free Splunk content updates based on Splunk security research.

7.1 Log all traffic (network, data, apps and users)

Splunk has hundreds of existing Integrations with all major security and IT solutions to collect and process all logs including network, data, application, device and user logs. These logs are stored in a standardized format and the raw event data is preserved. Splunk analytics and detections are ever-growing with over 1,400 existing correlation searches. These logs are readily available to SOCs and Cyber Security Service Providers (CSSPs) through our web search interface allowing for automated ad-hoc searches, dashboards, and alerts for rapid visibility.

7.2 Security information and event management (SIEM)

Splunk is the SIEM industry leader as supported by third party reviewers. Our industry accolades include being named a leader in Gartner's SIEM Magic Quadrant (9 years straight), International Data Corporation Marketscape, and Forrester Wave. Splunk is the only SIEM to be named a leader by all three reports over the past year.

Splunk ES provides free content updates with over 1,400 analytics to date. This project gives you access to our repository of analytic stories which are security guides that provide background on tactics, techniques and procedures (TTPs), mapped to the MITRE ATT&CK framework, the Lockheed Martin Kill Chain, and CIS controls. They include Splunk searches, machine-learning algorithms and Splunk SOAR playbooks (where available) — all designed to work together to detect, investigate and respond to threats.

7.3 Common security and risk analytics

Splunk provides for unifying data collection from across the enterprise and the ability to examine events, activities, and behavior. Splunk ES provides common and advanced security and risk analytics through our Machine Learning Toolkit (MLTK) and our integration with common analytics platforms such as Jupyter Notebook allowing for behavior baselining and anomaly detection.

7.4 User and entity behavior analytics

Splunk UBA, MLTK and integration with Jupyter Notebooks employ advanced analytics to baseline and correlate user and entity behavior and detect anomalies across the security stack. Splunk research is constantly adding to these capabilities.

7.5 Threat intelligence integration

As a feature of both Splunk Enterprise Security (ES) and Splunk Mission Control, Splunk Threat Intelligence Management enables analysts to fully investigate security events or suspicious activity by enriching events with information and streams about identities, motivations, characteristics, and TTPs with data collected in the SIEM. This enhances monitoring efforts and incident response.

7.6 Automated dynamic policies

Splunk's solutions can dynamically and automatically update security profiles and device configuration through continuous security posture monitoring and risk and confidence scoring. Splunk risk-based alerting incorporates threat intelligence with critical entity information and the MITRE ATT&CK Framework to dynamically and automatically adjust risk and confidence scoring. Although Splunk isn't a patch management tool, it can still work with them by alerting the relevant team.

If you would like to learn more about Splunk, get in touch.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com