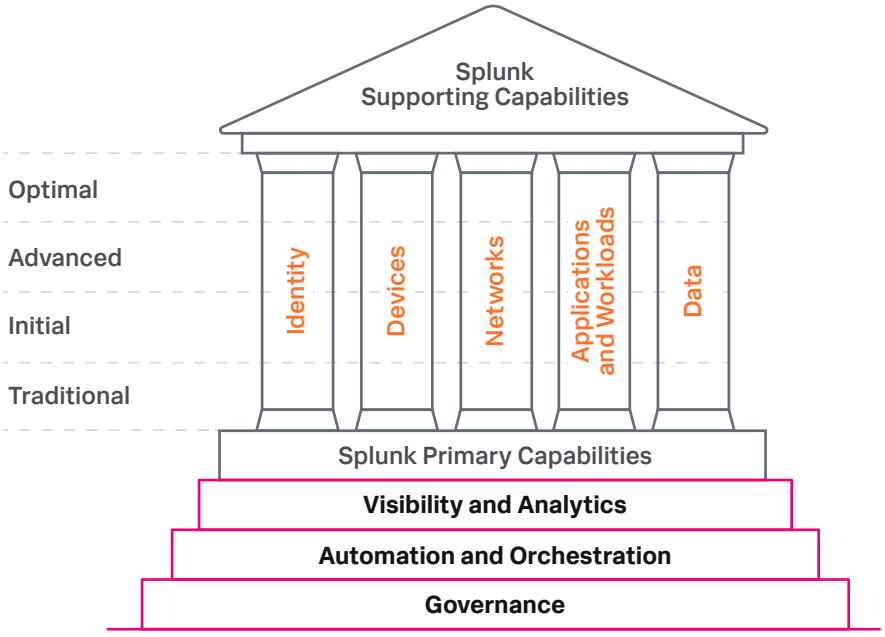
How Splunk Supports CISA's Zero Trust Strategy

Splunk aims to create a digital world that is safer and more resilient. Splunk can assist agencies in their Zero Trust (ZT) initiative, as stated in CISA's Zero Trust Maturity Model. 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 create a comprehensive view of the environment, allowing that data to be actioned on.

Creating a more resilient agency with Splunk means incorporating data sets that are traditionally thought of as only being security- or IT operations-focused and looking at them in one holistic view. A resilient agency is one that marries security information with ITOps information, which leads to quick and comprehensive decision making for any sort of incident.

Splunk supports any environment and has existing integrations with hundreds of other technologies to support existing architectures and seamless additions afterward. We support multicloud monitoring, and our Splunk Cloud SaaS offering supports sensitive information up to FedRAMP high and IL5. We can also deploy on-premises for air-gapped or highly classified areas, meeting civilian agencies where they are and where they want to go.



Pillar Capabilities

The CISA Zero Trust Maturity Model 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. While Splunk may not play a direct role in each individual pillar, Splunk plays a foundational role in each cross-cutting capability, affording agencies a unified place for Visibility and Analytics and Automation and Orchestration across each individual pillar.

Visibility and Analytics

Splunk Enterprise is a software product that lets you search, analyze and visualize data gathered from the components of your IT infrastructure or business. Splunk Enterprise takes data from websites, applications, servers, sensors, devices, etc. After you define the data source, Splunk Enterprise indexes the data stream and parses it into a series of individual events that you can view and search.

5.1 Identity

The Splunk Platform, incorporating the use of Splunk's market-leading SIEM application, Enterprise Security, can provide a deep understanding of users and their identities throughout an agency. Frameworks such as the asset and identity system and risk-based alerting (RBA) ensure the correct analytics are surfaced appropriately. RBA, a core functionality within Enterprise Security, allows an agency to understand how risky an individual is by using all of the data collected within the environment to build risk profiles.

Building on Splunk Enterprise Security, Splunk User Behavior Analytics introduces advanced machine learning to detect anomalous behavior that users may be carrying out in an environment. By pulling from data sources across an environment, Splunk can capture a comprehensive picture of identity, making it actionable through dashboards and automation.

5.2 Devices

Splunk Enterprise, Splunk Enterprise Security, and Splunk IT Service Intelligence (ITSI) all provide capabilities around monitoring devices such as: laptops, switches, servers, printers and other network endpoints. Together, Splunk Enterprise and ITSI provide a complete view of an enterprise's device performance and the services they comprise, while Splunk Enterprise Security can unlock additional visibility into the posture of all endpoints that exist on the network as well as form risk profiles through risk-based alerting. Splunk User Behavior Analytics introduces the ability to generate alerts based on anomalous device behaviors while working in conjunction with Splunk Enterprise Security to build out comprehensive dashboards. Whether through Splunk's correlation engine or machine learning, high-fidelity alerts can be generated to track device behavior and identify when it strays.

5.3 Networks

Splunk Enterprise has long been used for monitoring network traffic flows and the infrastructure supporting traffic flow across the network. Splunk can ingest Simple Network Management Protocol (SNMP) traps from network devices, as well as logs and metrics, and can even ingest Netflow data that provides a comprehensive view of the makeup of the traffic flowing across devices. Splunk Stream can be used to monitor and then create visualizations and allow for ad hoc searches of network traffic data, including the direction of traffic, the volume of traffic, and much more.

Not only can Splunk Enterprise automate the collection of network telemetry regardless of source, but it can also generate high-fidelity alerts through Splunk Enterprise Security by using 700+ out-of-the-box detections that are aligned to industry frameworks such as MITRE ATT&CK, NIST, CIS 20, and Kill Chain for misconfigurations as well as anomalous behaviors carried out by users and devices.

5.4 Applications and Workloads

Splunk Enterprise will passively discover applications and services in use across the enterprise as part of the regular consumption of system logs, just as it will passively discover user and device data. Splunk can also be used to help diagnose debug logs and test logs. Splunk's Observability suite can be used to combine traces with logs and metrics for a fuller understanding of what is happening during the software development and testing. Supply chain attacks can also be detected using Splunk. Lastly, Splunk provides capabilities, along with complementary partner solutions, to help customers maintain an understanding of their continuous monitoring and authorization status.

5.5 Data

Splunk Enterprise can both aggregate data and make it searchable across the data lifecycle, such as from databases, Data Loss Prevention (DLP) tools and endpoints. Splunk Dashboards help agencies have quick and deep understanding of their data posture, while Splunk Enterprise Security can quickly alert when potential violations are outside of tolerance levels. The Splunk Machine Learning Toolkit can operationalize machine learning models directly within Splunk to gain even more intelligence for more advanced trends and decision making.

Automation and Orchestration

Splunk has been a leader in integrating Automation and Orchestration with advanced Threat Detection where the marriage of Splunk SOAR and Splunk Enterprise Security has unlocked countless use cases for civilian agencies across the pillars of Zero Trust. Splunk SOAR can take any action in any Zero Trust environment through playbooks that automatically communicate with 3rd-party tools and workbooks that streamline actions performed by analysts. 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.

5.1 Identity

Splunk SOAR can help agencies streamline the management of all identities across an environment by acting as a single point to implement standard operating procedures. Whether onboarding new users, sunsetting stale accounts or responding to an alert raised by Splunk Enterprise Security for risky behavior, Splunk SOAR uses playbooks to immediately carry out any required action, directly interfacing with popular identity tools such as Active Directory, Okta and many more with a simple click of a button or fully automatically with no analyst interaction at all.

5.2 Devices

Splunk SOAR has over 60 pre-defined playbooks, helping civilian agencies achieve rapid operational capability with existing security technologies to orchestrate and automate policies and rulesets. With Splunk Enterprise Security's deep understanding of a device's posture, Splunk SOAR can fully automate any isolation and remediation and any external ticketing requirements for cross-functional notification. Deep integrations between Enterprise Security and SOAR ensure that any potential attack vectors are quickly limited and mitigated without the need for human interaction.

5.3 Networks

Splunk SOAR can directly interface with popular microsegmentation tools such as Zscaler to bring the full breadth of an agency's data closer to being operationalized. As an identity or device's risk profile changes in Splunk Enterprise Security, Splunk SOAR can request Zscaler take additional action for that particular asset. Splunk SOAR can incorporate data sets that are traditionally not visible to microsegmentation tools such as device performance or comprehensive risk profiles and use that to influence decisions being made on the network. Splunk SOAR can also integrate with popular Network Access Control surfaces to introduce holistic Comply-to-Remain strategies that take advantage of the rich and diverse information being stored in Splunk as well as Splunk SOAR's ability to scale across an enterprise.

5.4 Applications and Workloads

Splunk IT Service Intelligence and Splunk SOAR come together to form a cohesive solution to identify and resolve poorly optimized applications or poorly performing assets. Splunk SOAR can respond to alerts generated by Splunk ITSI for service outages as well as downward trends in performance to immediately notify required teams and also begin to enrich and ticket the event, reducing triage time.

5.5 Data

Splunk Enterprise and Splunk Enterprise Security can identify instances of the established data lifecycle of an agency being potentially violated, either due to a threat actor, an insider threat or a benign low-risk employee. Working with Splunk SOAR, playbooks can immediately be triggered to begin to isolate any offenders, ticket the event, notify required teams and restore any potentially modified policies — all before any data is potentially lost.

Learn more

24-512150-Splunk-How Splunk Supports CISAs Zero Trust Strategy-SG-106