MeriTalk
Improving the Outcomes of Government IT

splunk>
turn data into doing™

Accelerating Zero Trust in Government

Rethinking cybersecurity

Organizations used to approach cybersecurity by building a hardened perimeter – one that would keep the enemy from infiltrating from the outside. This concept, called defense-in-depth, layered security tools like moats and walls around a castle. But this proliferated into a heterogeneous landfill of dozens of security tools – where organizations lacked visibility and were blind to a holistic security posture.

Defense-in-depth makes sense when cyber threats only come from the outside and our assets live on-premises. But this is no longer the case. Today, our world is changing at rapid pace – with use of remote work, mobile devices, and hybrid and multi-cloud environments rising. These new technologies open up the attack surface, "de-perimeterizing" organizations by letting data and workloads live, operate and be accessed outside traditional walls.

That's the new landscape we must address today. The cloud, mobile devices and "anywhere, anytime" access do not conform to traditional security principles. Defense-in-depth and our old ways of securing assets are becoming less effective and provide malicious actors with more opportunities to take advantage. It's even more important for Federal agencies to gain visibility, control and security of their data. The rapid shift to remote work and user access has only increased the urgency – and opportunity to rethink security as the U.S. government accelerates modernization.

Agencies need resiliency

Agencies must adapt to de-perimeterization but face a dual challenge: to protect government data amid budget constraints and serve their mission with greater velocity. To make the most of their resources, organizations should focus on being resilient – how they can manage risk and go forward knowing that risks will exist. Resiliency depends on securing an agency's data and resources, rather than its network.

Mission enablement requires that IT provides decision-makers with trusted access to data quickly, so they can make confident decisions and take action at mission speeds. Instead of checking users' compliance to allow them to connect to the network, users should be compliant in order to connect – or remain connected – to a resource. With the speed at which organizations and malicious actors work today, government does not have time to manually validate that information is safe and accurate. If there is an issue, mission demands could dictate that they are fixed immediately or in near real-time.

Simply moving assets to the cloud or modernizing systems will not yield effective results if they are not secure. Organizational resiliency is essential for agencies to meet mission goals, given their critical nature, while protecting our national assets and allowing the government to realize the benefits promised by modern technology.

The Zero Trust (ZT) Foundation:

- ZT provides a consistent security strategy of users accessing data that resides anywhere, from anywhere in any way;
- ZT assumes a "'never trust and always verify" stance when accessing services and/or data;
- ZT requires continuous validation and authorization based on agency criteria; and
- ZT increases visibility and trust in decisions.

Zero Trust Assertions:

- The network is always assumed to be hostile;
- External and internal threats exist on the network at all times;
- Network locality is not sufficient for deciding trust in a network;
- Every device, user and network flow is authenticated and authorized; and
- Policies must be dynamic and calculated from as many sources of data as possible.

Source: ACT-IAC

Enter Zero Trust

To address the new environment and our need for resiliency, we need to evolve from defense-in-depth to new approaches. Zero Trust (ZT) is a security concept anchored on the principle that organizations need to proactively secure all access to data and resources to reduce security risks to acceptable levels. Its goal is to ensure the trustworthiness of the user, device or service requesting access to an agency resource at any time. The ZT infrastructure should also allow for continuous assessment and authorization based on various conditions – such as location, device or time of day and any others – while monitoring threats, vulnerabilities, risk, behavior and other relevant information. If changes in circumstance or environment are detected, earlier permissions may be restricted or revoked.

Clearly, this type of dynamic assessment is possible only with data as the foundation and collected from all relevant sources. Using data as the fundamental currency, ZT helps gain real-time visibility across all the relevant entities – users, workloads, networks and devices – and use analytics to continuously assess organizations' security standing and determine their worthiness to connect – and remain connected – to a given enterprise resource.

Organizations embracing ZT need the ability to continually monitor the ecosystem and adherence to established policies, and pinpoint issues for quick resolution. Monitoring helps ensure the performance and availability of resources to support the agency mission at the speed that its workloads

demand. Orchestration capabilities connect and manage across disparate security tools, and automation helps automate repetitive tasks and workflows with the goal of reducing response times and overall costs.

Data is not only our new digital currency but is also essential for empowering agencies to accelerate to a ZT model. Simply put, ZT is about identifying who needs access and to which enterprise resources, as well as the conditions they have to meet to gain the trust to connect and remain connected. The decision-making depends on continuous validation of the connecting entity; a data aggregation and analytics platform is critical to this.

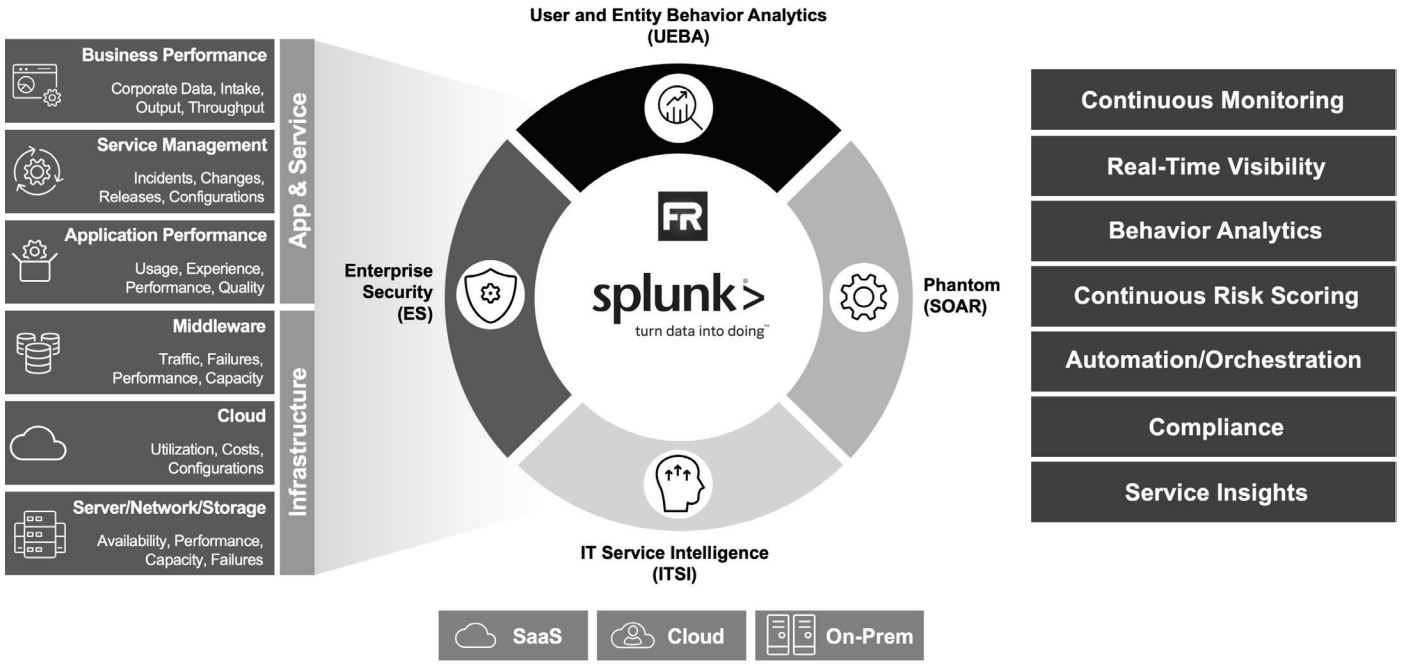
Splunk unlocks the value of data for Zero Trust

Splunk increases confidence and trust in access decisions to enterprise resources. It provides granular visibility to help assess a connecting entity's current profile, and continuously monitor events and metrics across the organization for fast and informed decision-making to manage risk effectively. It delivers rich, contextual details on any user, asset or service requesting enterprise resource access as needed, and provides the analytics necessary for fast insights into the entity's posture. Splunk utilizes artificial intelligence and machine learning to sift through volumes of data and bring out the relevant aspects across hybrid infrastructures into a single integrated view. By combining a sophisticated yet integrated set of capabilities like security information and event management, advanced security analytics, and behavior analytics augmented with machine learning, Splunk helps determine the risk scores of entities in real-time.

Splunk helps optimize and increase the effectiveness of the ZT ecosystem by delivering continuous, full-stack visibility into service health, component relationships and infrastructure, ensuring performance and availability – and predicts issues before they happen.

Splunk reduces manual effort, analyst fatigue and costs through automation. It assists in monitoring and managing disparate security systems through a single interface and orchestrates any remediations of configuration drifts or risky behavior. Agencies can save time and money through a reusable template/ playbook approach for automating highly repetitive and routine tasks.

Supporting many of the core ZT logical components as established by NIST – continuous diagnostics and mitigation, industry compliance, threat intelligence, activity logs and SIEM – Splunk's platform helps ensure visibility and analytics and continuous validation, and automates and orchestrates workflows to create more secure institutions.



Zero Trust Use Cases

1. A user is connected to a classified database while working from home on a government-issued device. The user performs many different activities that elevate their risk score over time. Splunk can deliver information in real-time to take action and potentially deny access if the risk score goes beyond a pre-determined threshold.
2. A user tries to connect with a particular device after, say, 30 days. Splunk can automate the checks to make sure there isn't any adverse malware, anomalies or other issues associated with the device. If an issue is detected, Splunk can orchestrate a workflow with automated tasks to scrub the device to ensure it is brought back to compliance.
3. A government analyst identifies a threat that could exploit a vulnerability. An automated task runs through Splunk to see which assets are patched against the vulnerability and which are not. Assets lacking the patch are blocked from access until they are patched – another process available for automation.

Splunk's suite of software solutions helps organizations across all three branches of the U.S. government, all cabinet-level agencies, and all four branches of the U.S. military protect their assets and critical infrastructures. It has been deployed pervasively to meet cybersecurity objectives across many state, city and county government agencies. Splunk offers a flexible deployment strategy to meet the unique needs of our diverse customer base. Agencies may elect to deploy on-premises, within their own private cloud, or leverage Splunk Cloud as a service, which is the first data analytics and security analytics service to be FedRAMP-authorized.

To learn more about enabling ZT through our analytics, automation and orchestration capabilities, visit **www.splunk.com/publicsector or www.splunk.com/asksales**