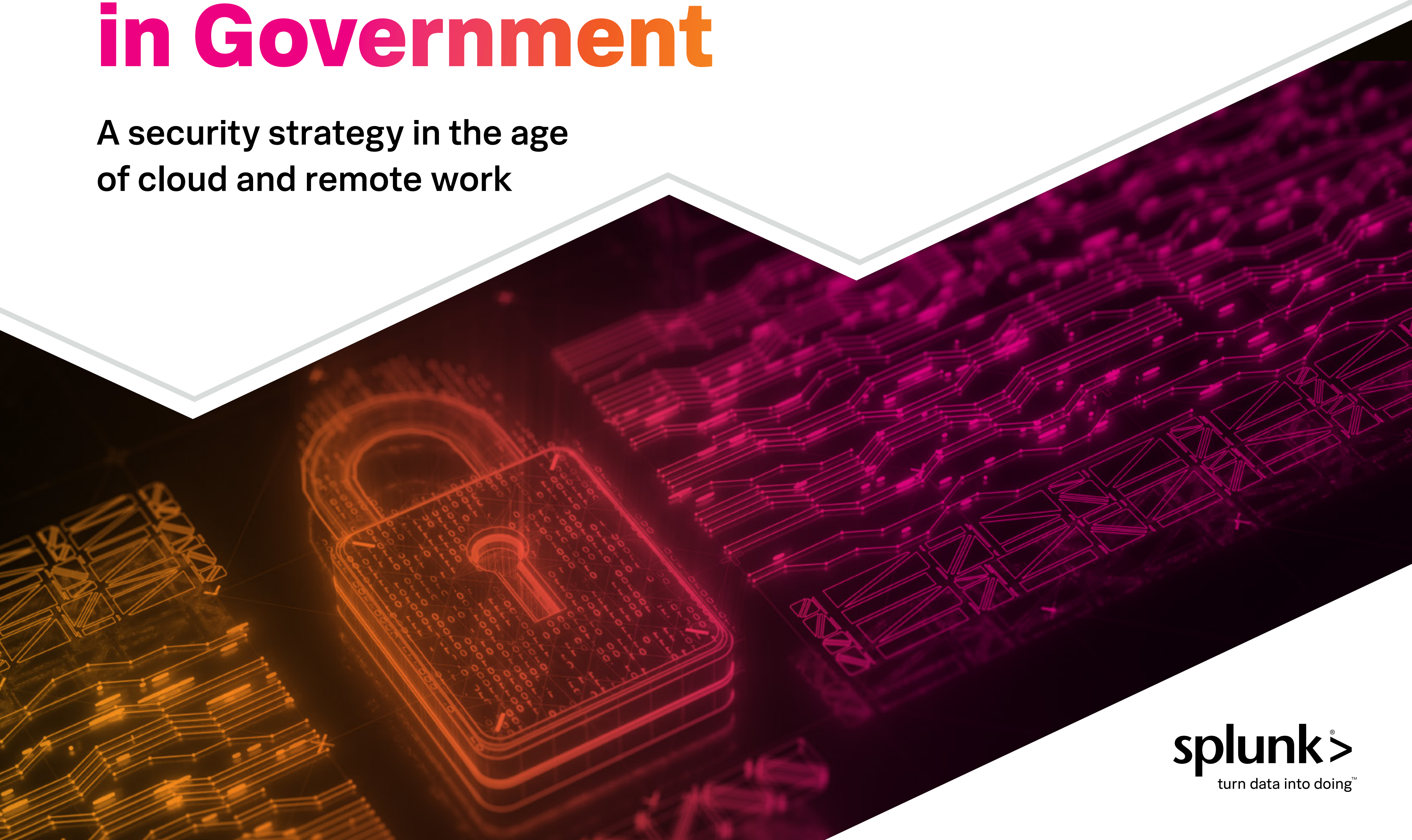
A Guide to Embracing a **Zero Trust Security Model in Government**

A security strategy in the age of cloud and remote work



splunk> turn data into doing™

Public sector agencies are in the middle of a massive digital transformation. Technology advances like cloud, mobile, microservices and more are transforming the public sector to help them:

- Deliver services as efficient as commercial businesses,
- Meet growing mission-critical demands, and
- Catch up with market expectations and be more efficient.

This allows public sector employees and constituents to work remotely and have access to their organization's applications and services — from anywhere at any time for both constituents and employees.

While digital transformation and cloud migration can help agencies reap many benefits such as efficiencies, agility and happy customers, it moves precious data out of the perceived safety of on-premises systems. This has subsequently led to the dissolution of the traditional enterprise perimeter.

This transformation also opens up new avenues for cyberthreats and expands the attack surface. Fears tied to these threats and the perceived challenges of moving to the cloud have slowed down the government's migration and the adoption of modern tools, and is one of the main reasons many legacy systems still dominate the halls of government.

In response to a proliferation of cyberattacks and this expanded attack surface, the Biden Administration has issued an executive order (EO) on improving the nation's cybersecurity through better cyber incident readiness and response.

This EO resulted in the OMB M-21-31 mandate which sets requirements for some high-level government work streams. It prescribes an enterprise logging maturity model with four levels and deadlines for achieving each. Each level becomes increasingly sophisticated by requiring more data sources, longer retention and eventually requiring business analytics and security orchestration and automation (SOAR) capabilities.

The bottom line? Despite the fears and challenges, the time has come for federal agencies to modernize their security operations, fortify networks and apply available expertise to become more informed and prepared for the next cyberattack.

COVID-19 forces government agencies to keep up with the times

The pandemic served as a wake-up call that forced many government agencies to accelerate their transformation. Overnight, government workers were forced to work remotely, which strained the public sector's existing capacity for IT and security.

Typically, government agencies rely on VPN solutions to manage access to the enterprise, while maintaining their security posture. But agencies found it difficult to scale since the solutions were not architected to handle a massive increase in its remote workload overnight.

This also exposed the public sector to new security threats. The legacy tools government organizations were using rely on an old school "defense-in-depth" approach to security, which needs a defined enterprise perimeter to secure an organization. But the rapid shift in work habits caused by the pandemic stretched the traditional approach to cybersecurity to its breaking point.

In a traditional approach to security, a threat could penetrate the network, and once the perimeter was breached, a hacker could exploit existing vulnerabilities to gain authorized access and move laterally across the network as well as any connected systems — compromising assets and causing irrevocable damage.

When organizations move to the cloud, user access moves outside their traditional perimeter, creating new challenges for visibility, control and the security of data.

Each device on the network — and the data it has access to — needs to be protected in its own right. Protection and authentication should be continually applied at both the device and user level, instead of the traditional reliance on the perimeter.

When coupled with the threat and adversary landscape, government agencies must assume they've already been compromised and take the necessary steps to protect themselves.

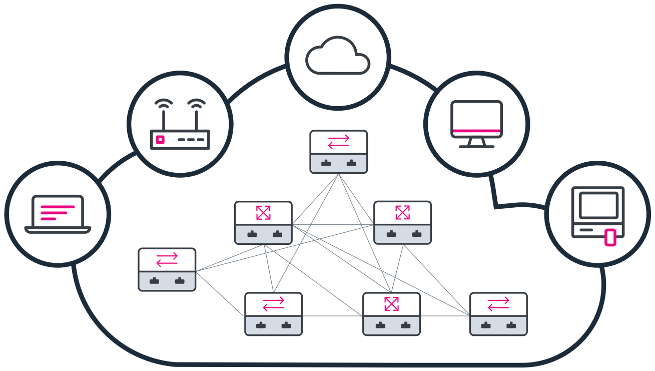
With this mindset, every user, device, service that is given access is considered hostile, even if it is a known and approved device or user.

And not all data is created equally. As security teams fight to protect the enterprise, one thing has become abundantly clear: not all assets can — or need to be — protected at the same level. It's essential to gauge the sensitivity and importance of data to help drive meaningful and effective security measures as the perimeter dissolves, and data moves outside enterprise walls.

Without addressing these issues, simply moving to the cloud or modernizing your infrastructure wouldn't yield effective results for both the capacity and security of public sector agencies. The government would be unable to properly protect assets and realize the potential benefits technology advances have to offer.

Government agencies need a modern approach that can look beyond perimeter-based security strategies to survive in the era of COVID-19 and beyond.

Traditional Network



A new approach to security: trust no one

One approach to security that has the potential to improve the way government agencies protect their data and systems is a concept known as **zero trust**.

Zero trust enhances security posture by eliminating the sole reliance on perimeter-based protection. In effect, organizations decrease their reliance on network security — instead securing endpoints and backend applications.

This ensures a level of trust and removes some of the anxiety around securing a remote office. It also reduces the threat of "data leakage," or employees accidentally losing sensitive company data downloaded to personal devices.

Protection and authentication need to be continually applied at the device and user level for each transaction, ensuring continuous and adaptive authorization.

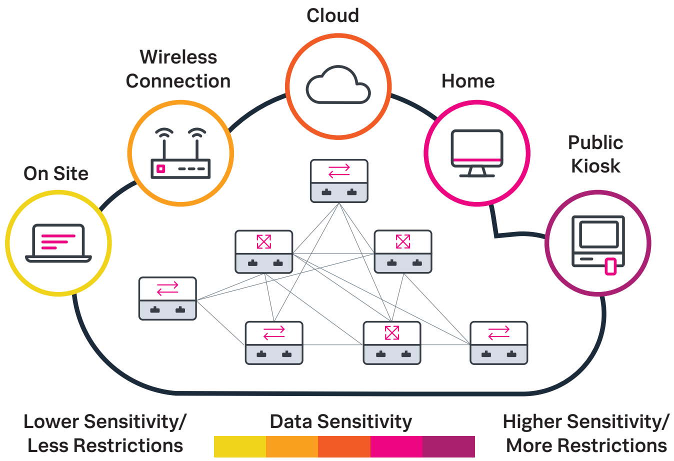
A simplified example of what this looks like in the real world is an employee who accesses an organization's case management system from a managed device. He's granted access.

After some time, he downloads a driver from a website that he feels would be helpful to him in his work. Since his device is continuously monitored in a zero trust strategy, his access to the agency's system would have been revoked since his device now has an unknown component increasing its risk to the enterprise resource.

This example is why a zero trust strategy consists of tying the employees' access to their IT-managed device, and depending on the risk tolerance of the organization, eliminating — or at a minimum, restricting — the amount of sensitive information that can be accessed from personal devices.

Forrester writes that we live in a time where organizations have "to assume you have already been compromised; you simply don't know it yet. That is the necessary mindset in today's hostile environment. 'Trust but verify' leaves you flatfooted and sets you up for crisis management. Zero trust may seem stark, but it is the proactive, architectural approach to align with mission priorities."

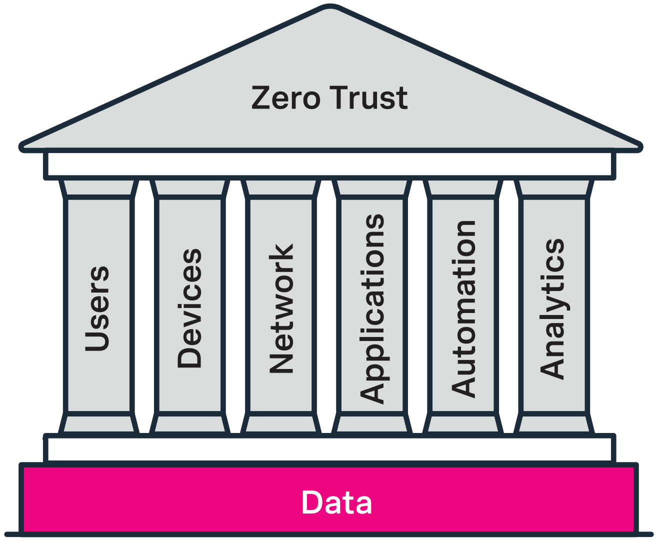
The analyst firm goes further by saying zero trust is "the best path to protecting your firm and brand."


Cloud
Wireless Connection
Home
On Site
Public Kiosk
Lower Sensitivity/ Less Restrictions
Data Sensitivity
Higher Sensitivity/ More Restrictions

Building a zero trust model

Industry and security experts have embraced the zero trust model as a good approach to securing organizations during, and even after, the COVID-19 pandemic.

For instance, ACT-IAC wrote that zero trust could be thought of "as a strategic initiative that, together with an organizing framework, enables decision makers and security leaders to achieve pragmatic and effective security implementations."



Source: Zero Trust Cybersecurity Current Trends, April 18, 2019, ACT-IAC

ACT-IAC lays out the six pillars of a zero trust security model that are built upon a foundation of data summarized as:

Users	The ongoing authentication of trusted users, the continuous monitoring and validating of user trustworthiness to govern their access and privileges.
Devices	Measuring the real-time cybersecurity posture and trustworthiness of devices.
Network	The ability to segment, isolate and control the network, including software-defined networks, software-defined wide area networks and internet-based technologies.
Applications	Securing and properly managing the application layer as well as containers and virtual machines.
Automation	Security automation, orchestration and response (SOAR) allows organizations to automate tasks across products through workflows and for interactive end-user oversight.
Analytics	Visibility and analytics are tools like security information and event management (SIEM), advanced security analytics platforms, user and entity behavior analytics (UEBA) enable security experts to observe what is happening and orient defenses more intelligently.

By definition, a successful zero trust security program must:

- Assume the network is always hostile.
- External and internal threats are always on the network.
- The location of a network locality is not enough to decide to trust in a network.
- Every device, user and network flow must be authenticated and authorized.
- Policies must be dynamic and calculated from as many data sources as possible.
- Risk scores for entities requesting access can be dynamic based on a variety of conditions and attributes and continuous information would serve to ensure trust is always maintained.

NIST similarly *provides its own guidelines* for implementing a successful zero trust strategy:

- All data sources and computing services need to be considered resources.
- All communication needs to be secured regardless of where a network is.
- Access to individual enterprise resources is granted on a per-session basis.
- Access to resources is determined by dynamic policy — including the observable state of client identity, application and the requesting asset — and may include other behavioral attributes.
- The enterprise ensures that all owned and associated devices are in the most secure state possible and monitors assets to ensure that they remain in the most secure state possible.
- All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
- The enterprise collects as much information as possible about the current state of network infrastructure and communications and uses it to improve its security posture.

Source: Zero trust cybersecurity current trends, ACT-IAC, April 2019

All these reports highlight that zero trust is a natural evolution in an organization's cybersecurity mindset that moves from a defense-based approach that focuses on network defenses and static perimeters to focusing on users, assets and the resources available to them. Especially in the time of COVID-19, this has become a global imperative.

To be effective, the zero trust approach requires organizations to focus on leveraging agency-wide data as its foundation and understanding that all data is security-relevant. Once data is being monitored and secured, the organization's defense can expand to include all its assets such as devices, infrastructure and users.

Legacy	Modern
Static, Perimeter-based	Protect Assets, Users, Resources
Implicit Trust within Perimeter	Assumption of Compromise / Continuous Evaluation
Comply to Connect to Network	Comply to Connect to Resource
Product/Tool Based	'Agency-wide' Approach

Splunk and the zero trust model

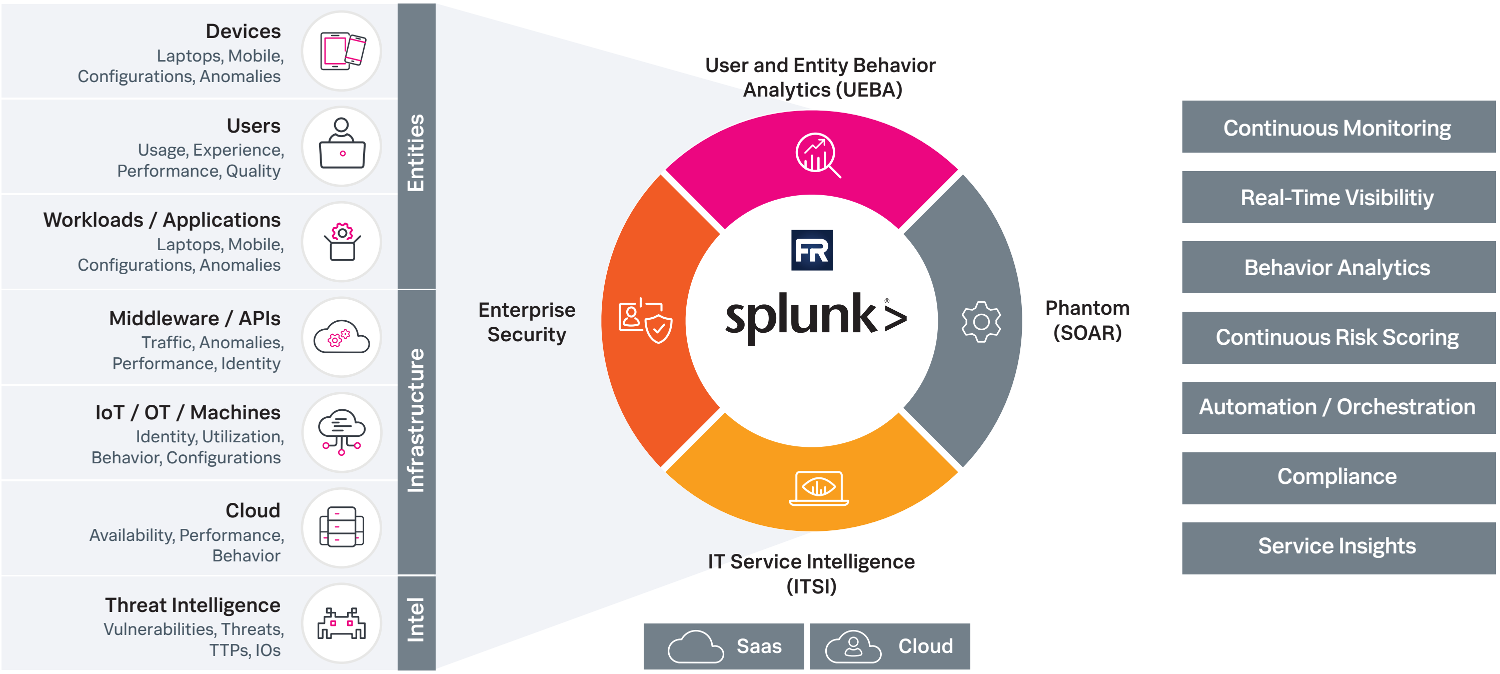
The Splunk platform offers a continuous monitoring and analytics solution for chief information security officers (CISOs) and security professionals who need to ensure secure access to their data and applications in the modern, perimeter-less enterprise.

The platform helps drive confidence and ongoing trust in access decisions, while ensuring component performance, policy adherence and availability across the zero trust ecosystem.

The Splunk platform helps organizations ingest data from almost any source, monitor its infrastructure end-to-end, and helps optimize and increase effectiveness of the zero trust ecosystem.

Splunk specifically maps to the zero trust model in three ways:

1. Splunk increases confidence and trust in access permissions to enterprise resources by continuously monitoring user, asset or service trustworthiness.
2. Splunk delivers full-stack visibility into service health, component relationships and infrastructure, ensuring performance and availability, and predicting issues before they happen with machine learning.
3. Splunk helps reduce manual effort, analyst fatigue and costs by enforcing zero trust policies by automating tasks and orchestrating workflows.



Devices
Laptops, Mobile, Configurations, Anomalies

Users
Usage, Experience, Performance, Quality

Workloads / Applications
Laptops, Mobile, Configurations, Anomalies

Middleware / APIs
Traffic, Anomalies, Performance, Identity

IoT / OT / Machines
Identity, Utilization, Behavior, Configurations

Cloud
Availability, Performance, Behavior

Threat Intelligence
Vulnerabilities, Threats, TTPs, IOs

Continuous Monitoring

Real-Time Visibilitiy

Behavior Analytics

Continuous Risk Scoring

Automation / Orchestration

Compliance

Service Insights

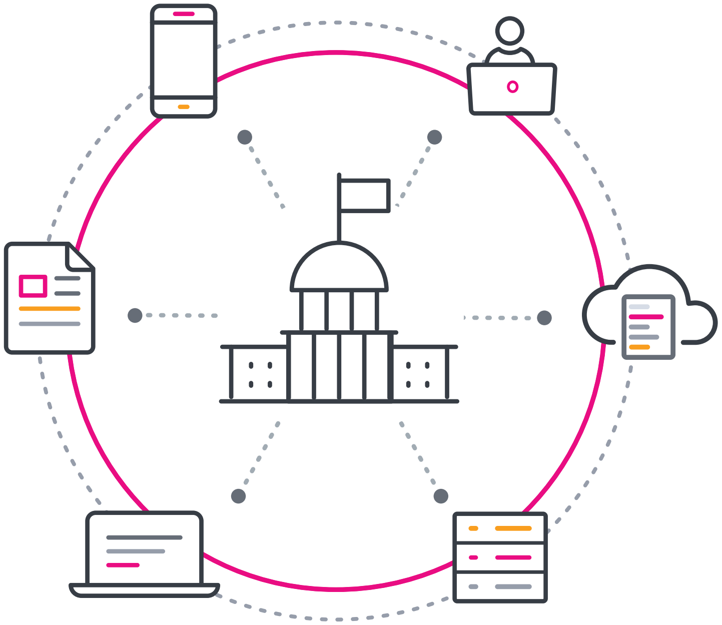
Increasing confidence, reducing risk

The fundamental premise of zero trust is to secure an organization's data — wherever it might live — while allowing legitimate access to entities that need them. The Splunk platform increases confidence and trust in user authorization to enterprise resources by continuously monitoring all users, devices, services and infrastructure. This information helps the policy engine validate user, asset, and service trustworthiness and govern their access and privileges at each step dictated by an organization's security policy.

Government agencies can rely on Splunk software for rich, contextual details on any user, asset or service requesting access to enterprise resources, at intervals dictated by agency policies, for fast and informed decisions.

By combining a sophisticated set of event management and advanced security and behavior analytics capabilities, augmented with machine learning, the solution enables the policy engine to determine trustworthiness and risk posed by the entity requesting access to enterprise data at any given time.

We'll next take a deep dive into the specific Splunk solutions that help build a successful zero trust model.



Feeling secure with Splunk

Splunk's security suite acts as an organization's security nerve center, turning data into insights and insights into actions. The software helps organizations leverage data — both security and non-security related — across the agency to enhance threat detection and response, and serves as a critical integration layer in the continuous diagnostics and mitigation (CDM) architecture.

Splunk's software provides context and streamlines security operations by helping organizations collect, aggregate, de-duplicate and prioritize threat intelligence from multiple sources. The software is continually augmented with actionable use case content to help protect against the latest cybersecurity threats and assess risk profiles and activity status and communicate them across the agency.

The core security solution consists of Splunk Enterprise Security (ES), Splunk User Behavior Analytics (UBA), and Splunk Phantom. Additional applications are available to extend functionality and shorten time to value (TTV).

Splunk Enterprise Security is an industry-leading SIEM solution that delivers an end-to-end view of an organizations' security posture with actionable intelligence to prioritize incidents and respond appropriately.

Splunk ES has comprehensive security-specific views of data, which helps security teams detect cyberthreats faster and optimize incident response. It also provides rapid investigation capabilities, making it possible to determine malicious activities, breach detection, and investigate the scope of a threat or an attack. Splunk ES also provides continuous risk assessment providing granular visibility and real-time insights on information assurance and adherence to controls.

Splunk UBA is a user and entity behavior analytics (UEBA) solution that provides advanced and insider threat detection using unsupervised machine learning. This helps organizations find unknown threats and anomalous behavior across devices, users and applications.

Splunk UBA extends the power of Splunk ES by allowing organizations to act on high-fidelity threats, while optimizing threat detection and enabling targeted incident response. It delivers dynamic risk evaluation capabilities by continuously monitoring access control and user behaviors — internal and external — to detect any abnormal or unauthorized activities. It can automatically stitch together multiple anomalies across multiple entities — users, accounts, devices and applications — into a single threat, simplifying analysis and accelerating actions.

830+ Security Apps
PCI
Splunk Enterprise Security
Splunk User Behavior Analytics
Splunk Phantom
Splunk App for PCI Compliance

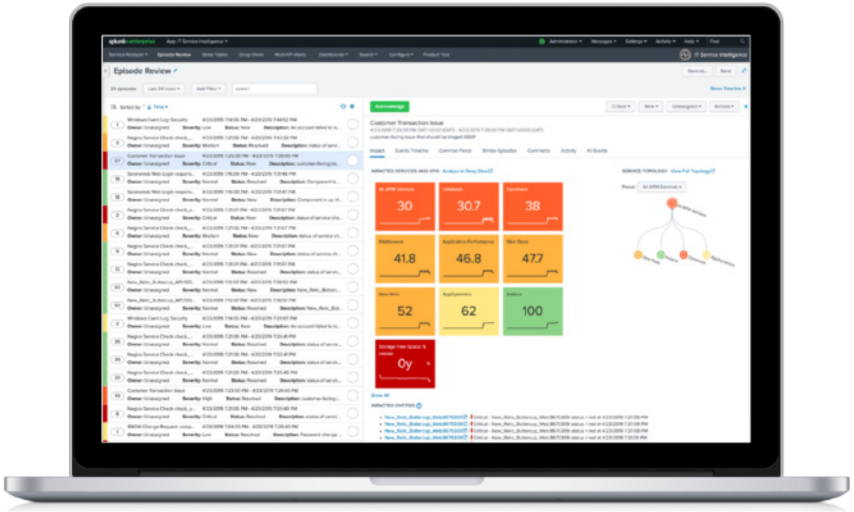
More uptime, less stress time

Splunk also helps optimize and increase the effectiveness of the entire zero trust ecosystem. It delivers continuous, full-stack visibility into service health, component relationships and infrastructure, ensuring performance and availability, and predicting issues before they happen with machine learning. If a component goes down or does not perform as expected, IT and security staff are alerted quickly and the issue is pinpointed, potentially saving them hours in troubleshooting and helping recover lost data.

Additionally, organizations can gain real-time granular visibility across their network, endpoints and application stack to ensure compliance, faster audits and orchestrate any remediations of configuration drifts. They can continuously monitor components of the zero-trust infrastructure to ensure assessments are conducted per policy and assets remain in the most secure state possible.

Splunk IT Service Intelligence (ITSI) is the solution that helps organizations prevent service disruptions incidents before they occur, applying machine learning to data for full-service monitoring, predictive analytics and streamlined incident management. It can predict service degradations and get ahead of investigations by empowering teams to take action quickly before any impact.

ITSI correlates and applies machine learning to metric, log and trace data, and integrates monitoring, event management and incident response into one platform. ITSI's alert management and analytic capabilities provide near real-time, predictive performance dashboards to monitor service health. This can integrate with IT service management (ITSM) and orchestration tools like VictorOps and Splunk Phantom, so teams can monitor, detect, respond and resolve incidents all from one place.



Reduce analyst fatigue and manual effort, go home early

Finally, the Splunk platform automates tasks and orchestrates workflows to help enforce zero trust policies. With a complex security infrastructure, stretched resources can be relieved by automating repetitive tasks — like patching a system and orchestrating workflows — to determine the risk of a personal device requesting access to a resource.

Automation and orchestration help organizations significantly reduce the manual effort to stay ahead of threats, security operations center (SOC) analyst fatigue, and event reaction times. This reduces costs for organizations and frees up analysts to proactively hunt for cyberthreats and address anomalies.

Splunk Phantom is a leading SOAR solution. Phantom's extensible automation and orchestration capabilities helps organizations work smarter, respond to threats faster and strengthen cyberdefenses. Phantom's flexible application model supports hundreds of tools and thousands of unique APIs, enabling organizations to connect and coordinate complex workflows across your team and tools.

It enables you to execute a series of actions — from detonating files to quarantining devices — across your security infrastructure in seconds, versus hours or more if performed manually. Organizations can use Phantom to integrate their teams, processes and existing security tools to support a broad range of security operational functions, including event and case management, collaboration and reporting.

Implementing zero trust principles goes beyond technology. It must be embraced within the processes and teams supporting the organization. Phantom can increase consistency with these standard operating procedures which can be codified into reusable templates, orchestrate human and machine tasks, and keep all related data and activity in one centralized location.

Splunk + Zero Trust Pillars

<table>
<tr><th>People/Identity</th><th>Devices</th><th>Workloads</th><th>Network</th><th></th></tr>
<tr><td colspan="4">Splunk Enterprise</td><td rowspan="4">Visibility and Analytics</td></tr>
<tr><td colspan="4">Splunk Enterprise Security (ES)</td></tr>
<tr><td></td><td colspan="3">Splunk IT Service Intelligence (ITSI)</td></tr>
<tr><td colspan="3">Splunk User Behavior Analytics (UBA)</td><td></td></tr>
<tr><td colspan="4">Splunk Phantom / Splunk Enterprise Security (ES)</td><td>Orchestration and Automation</td></tr>
<tr><td colspan="4">Splunk Compliance Analytics</td><td></td></tr>
</table>

Turn Data Into Doing

Data is at the center of any successful zero trust strategy — regardless of its source or type. The biggest barriers to unlocking the full potential of data are the systems and structures trapping its value.

Removing those barriers unleashes a potential gold mine for public sector organizations. It allows for seemingly disconnected data to come together to drive action in real time across an entire organization and to form the solid foundation needed for a successful zero trust strategy.

Splunk has built the world's first Data-Into-Doing platform designed to remove the barriers between data and action. The Splunk platform is empowering public sector organizations to bring data to every question, every decision and every action.

The Splunk platform is the only integrated suite with industry-leading SIEM, UEBA and SOAR software solutions that utilize a market-proven, scalable big data platform, continually augmented with actionable use case content.

Learn More

Ready to explore how the Splunk Data-Into-Doing platform can help you build a zero trust policy?

Learn more about our new Government Logging Modernization Program and how Splunk's zero trust architecture tools can help you meet the Biden Administration's new requirements for cyber incident response (OMB M-21-31).

Or speak with a Splunk expert to discuss your environment and assess your requirements and how Splunk can help you navigate these challenging times.