MeriTalk splunk>

Time to Zero-In on Zero-Trust

The SolarWinds Orion breach sent powerful shockwaves through the public sector IT community already on heightened alert throughout the pandemic. The event was a powerful reminder of continued escalation of the threat landscape. It also, however, presents an ideal opportunity to rethink public sector cybersecurity strategies and accelerate the adoption of zero-trust architectures across the enterprise.

Modernization Domino Effect

Government's commitment to digital transformation is driving the need for modernization in the way that agencies think about and approach cybersecurity. As agencies embrace various cloud models, continue to telework at scale, expand digital service delivery, and commit to making the most of their data, the move to a zero-trust architecture is not only prudent, but logical.

Traditionally, security strategy has been very reactionary, driven by compliance or based on legacy security architecture principles that don't necessarily fit with modern agile or cloud approaches. As a result, security has often been at odds with the rest of IT and the organization's broader transformation objectives.

It doesn't have to be this way.

Zero trust provides a different way to think about security—one that agencies can balance with their broader transformational needs. This is an important consideration as many perceive zero trust to be an all-or-nothing proposition. Instead, it's more of a mindset that guides security strategy across the lifecycle and supports adoption of a risk-prioritized approach.

For example, when developing a strategy for an initiative such as remote work, the concept of zero trust should be applied throughout the lifecycle—not something built in isolation or bolted on after the fact. Thinking about zero trust in a remote work environment, an agency needs to enable access to protected resources for authorized users in a way that not only ensures the right level of security but is also seamless for the user. Further, decision-makers should think about the operational impacts of such an approach and avoid introducing needless complexity for IT or security teams.

Where Do We Start?

Zero trust tenets dictate that one always assumes a breach and that no one and no asset or identity should be implicitly trusted without being first verified and validated for security compliance. Sounds paranoid, but it's exactly the posture needed for more effective cybersecurity.

Not a new concept by any measure, zero trust has been underrepresented and sometimes misunderstood. Agencies are at various points in adopting zero trust fundamentals, and progress has been slow and inconsistent. There's new interest, however, in accelerating adoption and a number of resources to help. For example, the Advanced Technology Academic Research Center (ATARC) has a working group—including more than 15 Federal agencies—focused on producing an actionable plan that agencies can use as a guideline to implement zero trust. The guidance is expected to help drive greater consensus around how to adopt zero trust, which, in turn, would allow agencies to advance more rapidly.

The zero-trust journey, like any type of cybersecurity approach, is ongoing and must continue to evolve with an agency's needs. It also should incorporate a risk-prioritized strategy that allows agencies to focus on their most critical systems first and iterate from there.

Since zero trust is an evolution of past approaches, it should build on—versus abandon—existing strategies, controls, and tools. The first steps should be to establish a baseline of the agency's critical systems, assets, and data, and then understand who needs access, how systems are accessed, from where, and when. Another approach gaining traction is to begin with identity, credential, and access management (ICAM). Agencies should then build an understanding of the associated threats so they can pursue a targeted approach, starting with the most critical systems and priorities. Agencies must pursue both a tactical approach—applying zero trust to traditional systems—and a strategic approach—incorporating zero trust natively as part of modern IT systems.

No Better Time to Start

An advantage for many agencies starting to consider zero trust now is that the methodology, architectures, and technologies that support and enable the approach have had several years to evolve and improve. There have also been dramatic shifts in technology, more generally with the emergence of cloud-based solutions that provide advanced automation capabilities and extensive interoperability via APIs, for example. These technologies, coupled with the latest generation of zero-trust technologies, enable a dramatically different approach to security.

For example, before zero trust, many organizations attempted to implement network segmentation architectures but based them on traditional networking and security technologies. This approach resulted in massive complexity, and operational overhead as these tools only supported configuration at a network level. Zero-trust solutions and security controls, in contrast, more generally support security policy that agencies can define at a higher level, more closely align to mission requirements, and are dynamically enforced via the various controls.

By using an iterative, risk-based approach, organizations can develop a strategy that best suits their needs and then implement accordingly. Once an agency has a strategy, is applying it to existing systems, and is

Zero Trust in Action: The U.S. 2020 Decennial Census

The 2020 Decennial Census is a high-profile example of the use of a zero-trust architecture. The 2020 Census was the first to leverage online data collection, a strategy fortuitously planned well before the pandemic. To ensure the security of data collection, the U.S. Census Bureau adopted many zero-trust fundamentals as part of its risk-based approach to cybersecurity. This strategy enabled the architecture, use cases, and technology to support the Decennial Census using a common theme. It also allowed the Bureau to adapt—from a technology and security perspective—to threat actors and the pandemic.

incorporating it into its approach for new projects, it is well on its way to embracing zero trust.

Building Blocks to Zero Trust

No path is the same, but there are several logical steps to jumpstart the journey to zero trust adoption and a risk-based approach.

1. **Identify your critical assets**, systems, applications, and data, and prioritize your efforts accordingly. Once priorities have been defined, iterate the following stages for each system identified, adjusting the order or adding new systems as the need arises.
2. **Understand how these systems are used**, who needs to access them, how they will access them, and from where. Then begin building a picture of potential threats to these systems and data.
3. **Conduct an evaluation of related security controls** that can support a zero-trust approach in context with what one needs to secure. Many existing tools can support a zero-trust strategy. For example, Virtual Desktop Infrastructure (VDI) can minimize the scope of access for certain types of users, such as external contractors, and remove the need to manage untrusted devices from third parties.
4. **Build the policy and high-level architecture** that defines the access, authorization, and security controls based on what has been determined from the previous steps.
5. **Determine any additional** technologies and integration required to support the policy and architecture.
6. **Leverage security monitoring and analytics solutions** to augment security controls with security detections that focus on what the agency is trying to prevent and protect with the zero-trust approach. This step has the added benefit of helping to improve overall security operations effectiveness, if done correctly.
7. **Review and adapt** as required.

In pursuing a risk-based approach to zero trust, agencies often find that they already have much of what they need in place to some extent, particularly from a tools perspective. The hardest part of the journey—and often the most incomplete aspect—is answering "what do we need to protect?" Answering this fundamental question requires going back to basics and understanding one's assets, risk, and associated threats to build out a zero-trust architecture correctly.

Creating a Culture Shift—Education is Key

Since zero trust is as much a mindset as a technology initiative, it requires a culture shift. Agencies should not overlook the role of education in jumpstarting change. This should include education around what the concept of zero trust is about—as part of an organizational-wide security training program. When explaining zero trust, it's often useful to compare it to how individuals might personally determine whether they can trust an email they've received. Bottom line: one should always start with zero trust and work from there to validate and determine if it is a legitimate email.

Get There Faster with Splunk

Splunk security suite can support an agency throughout its zero-trust journey—from assets and identity frameworks to understanding what you need to protect to monitoring performance and continually assessing and adapting. It acts as an organization's security nerve center, delivering the visibility and context to make fast decisions and take action. Splunk's platform provides context and streamlines security operations by helping organizations collect, aggregate, de-duplicate, and prioritize threat intelligence from multiple sources.

Components include:

Splunk® Enterprise Security (ES), security information and event management (SIEM) solution that delivers an end-to-end view of an organizations' security posture with actionable intelligence to prioritize incidents and respond appropriately. With Splunk ES and Risk Based Alerting (RBA), we can look across the end-to-end zero-trust architecture and controls to monitor user and device behaviour and detect suspicious activity using a centralized approach.

Splunk® UBA, a user and entity behavior analytics (UEBA) solution that provides advanced and insider threat detection using unsupervise machine learning. This helps agencies find unknown threats and anomalous behavior across devices, users, and applications. Behavior analysis provided by Splunk UBA is an important aspect of security detection and monitoring for zero trust in order to look for anomalous activity of authorized users, specifically in regards to insider threats or situations where there is a compromised user account or device.

Splunk Phantom, a leading security, orchestration, automation, and response (SOAR) solution that helps organizations work smarter, respond to threats faster, and strengthen cyber defenses. Phantom's flexible application model supports hundreds of tools and thousands of unique APIs, enabling organizations to connect and coordinate complex workflows across their team and tools. As a zero-trust approach consists of a range of different technologies and controls, not only do government organizations require centralized monitoring across these controls, they also need to support a coordinated approach to handling incident investigations and response. With Splunk Phantom's extensive integration available across the security ecosystem combined with automation, SOAR supports a centralized approach to incident investigations and response for zero trust.

Splunk® IT Service Intelligence (ITSI), a solution that helps organizations prevent service disruptions and outages 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.

Zero-trust is an intelligent path forward in the quest for more secure public sector organizations. As agencies focus on accelerating adoption, it's important to return to the basics with a risk-based approach, starting with the fundamental question: What is most important to secure?" Agencies can then leverage existing tools as a foundation and build out and iterate from there to deliver a higher level of security to their ever-changing environments.

Start your journey today and learn how Splunk can support you in your mission. Download a copy of Splunk's "Guide to Embracing a Zero Trust Security Model in Government."

MeriTalk splunk>