Zero Trust: A Primer for Government Agencies

Over the past five to 10 years, the erosion of the traditional perimeter networking model has given rise to the concept of Zero Trust. However, for many agencies, it took the more recent largescale transition to remote work and accelerated adoption of digital transformation initiatives to prompt the move of Zero Trust as a vision to an embraced reality.

Zero Trust is an approach that embodies multiple solutions working together to provide the best defense. The May 2021 Executive Order from the White House accelerated and highlighted the need to improve U.S. cybersecurity and put an emphasis on achieving a Zero Trust strategy.[1] Two important facets of Zero Trust are: enforcing the principle of least privilege everywhere, and never trusting, but always verifying, when it comes to identity.

State and local government agencies wanting to take a Zero Trust approach must verify every attempted access through proper identity controls with location awareness, identity authentication and multi-factor authentication (MFA), and assume every attempt at access is a threat until verified. In addition, no identity, account, application, machine or system should have more privileges or access than absolutely required.

This brief, which draws from a Government Technology webinar sponsored by BeyondTrust and SailPoint, explores the concept of Zero Trust and how it can apply to government agencies looking to bolster security.

Why is Zero Trust Critical Now?

The traditional approach of trusting systems and devices within a perimeter doesn't make as much sense for organizations in today's highly diverse and distributed environments, where users are accessing data from all types of devices and from multiple locations. With governments making more and more processes digital, the mindset must be to never trust and always verify. Systems, devices and users shouldn't be trusted by default, even if they're connected to a managed network and have been previously verified.

In this new environment, a Zero Trust approach can help agencies minimize their attack surface, but they must have a clear understanding of how they plan to move forward with the concept.

A core facet of Zero Trust involves relying on robust identity management and user authentication controls, which includes checking the identity and integrity of devices regardless of location. It also includes providing access to applications and services based on the confidence of device identity in combination with authentication.

Zero Trust is "not just another tool in the box," says Brian Engle, chief operations officer and CISO at CyberDefenses and former CISO for the State of Texas. "It includes how you understand the things that people are accessing, where they're accessing them from and who those people are — which sounds a lot like authentication and includes a lot of the pieces of authentication, but it goes so much further than that." Zero Trust is something "that you should probably consider as a component of your overall security strategy," Engle says.

Remote Work, Digital Transformation Raise the Stakes

The shift to working from home and other remote sites during the pandemic has greatly increased the need for stronger cybersecurity and accelerated the focus on Zero Trust — and in particular identity management.

"When we started allowing people to work from home, we had to increase the confidence of identity account relationships — when they authenticated and when they were

authorized to do activities with on-premises or cloud technologies," says Morey Haber, CTO and CISO at BeyondTrust. "Using a traditional username and password was not necessarily good enough because now we couldn't even trust the network they were operating from."

Identity security and privileged access management (PAM) are key components to explore when building a Zero Trust approach. Almost every attack today involves a stolen identity or privilege to execute and initially compromise an environment, or to move laterally within a network.

The shift to working from home and other remote sites during the pandemic has greatly increased the need for stronger cybersecurity and accelerated the focus on Zero Trust — and in particular identity management.

The Role of Privileged Access Management

A key element of identity security is PAM, which secures the privileged access for sensitive information, resources and systems. PAM is needed not only to secure human identities, but applications and machine identities as well.

Zero Trust encompasses all identity domains, including PAM controls. Privileged accounts are a subset of accounts that provide the highest level of permissions to perform particular tasks and should be treated as special use cases from an identity access management perspective.

Identity and access management solutions help IT teams answer the question of who has access to what. Privileged access management allows agencies to answer questions such as whether particular access is appropriate for certain users and whether this access is being used appropriately.

Applying the principle of least privilege (PoLP) is a powerful and well-recognized way to secure agency systems. It ensures elevated access is only given when contextual parameters are met and is immediately revoked after the activity is performed or the context has changed.

It's important that agencies only grant privileged access for as long as it's necessary and continually monitor access rights, says Frank Briguglio, global public sector strategist at SailPoint. "We need to understand the complete access that someone has, and that all goes with [having] visibility."

Where to Begin — and How to Succeed

Creating and adopting a Zero Trust strategy and architecture can be daunting because it often involves lots of change — in technology, processes and culture. Factors such as legacy architectures can present roadblocks.

A good first step is to assess the current IT infrastructure and understand where challenges might arise. Agencies should look for opportunities to integrate related solutions into existing systems, instead of revamping the whole environment.

The shift to a hybrid work model presents a good opportunity to deploy a Zero Trust approach when creating access entitlements and policies for employees who work both remotely and in agency offices.

Agencies should keep in mind that Zero Trust isn't something that magically happens overnight. It's a journey that might involve many steps and take several years, depending on the size and scope of the organization.

Budgets for financial modernization projects can help agencies pay for Zero Trust security initiatives. They might also be able to tap into cybersecurity funding opportunities available as part of recent recovery legislation.

Security leaders at state and local agencies should closely follow developments with the White House executive order, which could serve as a model for how to incorporate Zero Trust into government operations at all levels.

To learn more about how to take a Zero Trust approach to cybersecurity, listen to the full webinar here.

This piece was written and produced by the Center for Digital Government Content Studio, with information and input from Beyond Trust and Sailpoint.

[1]https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Produced by: CENTER FOR DIGITAL GOVERNMENT

For: BeyondTrust SailPoint

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com.**

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering agencies to secure and manage their entire universe of privileges. The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving agencies the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Learn more at **www.beyondtrust.com/public-sector.**

SailPoint is the leader in identity security for the cloud enterprise. We're committed to protecting government agencies from the inherent risk that comes with providing technology access across today's diverse and remote workforce. Our identity security solutions secure and enable thousands of organizations worldwide, giving our customers unmatched visibility into the entirety of their digital workforce, ensuring that each worker has the right access to do their job – no more, no less. With SailPoint as foundational to the security of their organization, our customers can provision access with confidence, protect business assets at scale and ensure compliance with certainty. **www.sailpoint.com/fed**