Seven Steps to Achieving Security with Zero Trust

If there are two words federal cybersecurity experts hear most frequently today, they are probably "zero trust." Not only are there plenty of mandates and other requirements to move in that direction, but there are practical reasons as well. It reduces agency risk; provides better control over access, assets and users; and improves the overall cybersecurity posture of the agency.

In a nutshell, zero trust is an approach that assumes that every network is hostile and that every request to access data can come from any user, on any device, from any location. With this "access anywhere" modality, it's important to have a security framework that fits that modality.

It also assumes that we can't keep putting all of the security onus on end users with complex passwords. The framework has to provide the security and be agile enough to adapt to a changing environment with users who may be agency employees, contractors or citizens interacting with government.

While all agencies are working toward zero trust, getting all the way there can seem overwhelming, but it's definitely doable—and it doesn't have to be all-consuming. By approaching the issue systematically and taking the time to do it right, all agencies can get there. Here are some ways to help your agency achieve the goal:

1. **Plan carefully.** Start by taking inventory of your users, devices and data, and see where they may already be compliant with some tenets of zero trust. Focus on resources by identifying and classifying your data. A data inventory should examine the data classification level of all data, as well as who needs access. During this process, make sure to involve data owners. With that information, agencies can determine the best type of security required for different types of data. The goal is to build a "muscle memory" around security so that every time something is moved, added or deleted, it's adhering to the same security policies.

2. **Make identity the foundation of your zero trust approach.** "Nothing happens until somebody or something requests access to something, so identity becomes a fundamental linchpin capability in a zero trust architecture," said Sean Frazier, Federal CSO at Okta. While considering identity management approaches, make sure that they don't diminish the user experience, he added. One way to ensure that identity is front and center is by using the principles of Federal Identity, Credential and Access Management (FICAM), which help agencies manage, monitor, and secure access to their resources.

3. **Bake security into everything.** While legacy systems, applications and approaches often add security after the fact, that approach doesn't work well anymore. In addition to being more expensive, adding security to solutions later means that hackers have more time to exploit security vulnerabilities. Of course, baking security in is easier for newer applications and solutions. There will always be some legacy applications that agencies need to keep, and Frazier suggests dealing with them by putting them in their own "security bubble" with a plan to bring the zero trust framework to them over time.

4. **Consolidate your security stack.** It's not uncommon for an agency to have dozens of different solutions for identity, endpoint management, and other types of cybersecurity solutions. It's expensive and labor-intensive to keep them in sync. Instead, whittle that list down to the essentials, focusing on the solutions that fit your needs best and provide users with the best experience.

5. **Prioritize.** There's no need to try to do everything at once. Frazier recommends starting by modernizing the identity system, and then moving up the stack to devices, applications and network.

6. **Don't make it harder than it has to be.** While mandates and regulations can cause pressure, they are also there to help. There is plenty of zero trust guidance out there to take advantage of, including the recently released Zero Trust Executive Order. Other helpful documents include OMB's M-22-09, CISA's Zero Trust Maturity Model, NIST's SP 800-207, and guidance from the National Cybersecurity Center of Excellence.

7. **Mind the mindset.** Mindset and culture are critical to the success of zero trust initiatives. "Zero trust is a real culture shift internally, because it's a different way of looking at things," Frazier said. That means finding a way to educate the workforce and change the culture to one that puts security first.

Learn More about Okta: okta.com/zero-trust

Iaremenko / iStock

PRODUCED BY FCW | SPONSORED BY carahsoft. okta