NEWS CIVILIAN AGENCIES HOMELAND SECURITY

Special Report: Zero Trust Necessary for Cloud Security

Zero trust is a simple concept – don't trust anyone; verify everyone; do it continually – with a more complex goal of ensuring the right people have the right level of access to the right resources in the right context. The model has gained traction across industries, with giants like Google declaring that their internal private network is just as dangerous as the internet. The concept is also gaining momentum within Federal agencies.

Shane Barney, Chief Information Security Officer and Chief, Information Security Division at the Department of Homeland Security's U.S. Citizenship and Immigration Services (USCIS) organization, spoke about the importance of zero trust for Federal cloud computing at MeriTalk's recent Cyber Security Brainstorm conference. "Without the notional ideas of zero trust, cloud does not happen. It just can't, because you've now officially blurred any notion of a perimeter," said Barney.

"The idea before was to build a castle, put all of our assets in that castle, put a moat around it, protect it, trust anyone that's in there, don't trust anyone outside of that. But, if someone who is untrusted figures out how to get through the perimeter, they've got unfettered access and horizontal access to all the goods. We saw the huge cost of this model with Equifax, and then with Capital One," explained Ted Girard, VP of Public Sector, Okta.

Cloud connects everyone to everything, dissolving the perimeter in the process. "If you're going to cloud, you're not going to get a choice. You're in a zero trust world already just by going to cloud," Barney commented. He speaks from experience – USCIS IT is 90-95% based on cloud infrastructure today.

Getting there isn't as easy, especially in a multi-cloud, hybrid environment. Barney shared strategic pillars that put USCIS on the path to zero trust.

"Change your culture"

Notably, USCIS didn't intentionally start on a path toward zero trust. Rather, then-CIO Mark Schwartz joined USCIS with the notion that a government agency can run like any other organization. The idea was a reflection of Schwartz's experience in Silicon Valley, and, Barney said, he was right. "We can do full agile development and still stay compliant… it is doable," he said.

The ACT-IAC Zero Trust Project Report released in April listed "moving away from compliance focus" as one of the top challenges to implementing zero trust, citing the tendency to "chase green" in scoring models.

As an example, Continuous Monitoring, Threat Intelligence, and Red Teaming are critical to any cybersecurity strategy, but only the first is reported up, resulting in a skewed focus.

Rather than focusing on compliance, Schwartz advocated a risk model, focusing on fixing problems first, and documenting the issues later.

Getting the developers on board with the new mindset is also important, a Defense Department representative emphasized, and suggested that agencies set up for success by making it as easy as possible to integrate new resources.

Barney shared that he hires Information Security Officers with a more technical background, often offering a higher starting salary compared to other agencies. Infusing fresh talent has helped overcome the "compliance culture," he said. Then as a team, he said, they embraced a risk management model.

IAM is Key to Strategy

Identity and access management (IAM) is key to establishing a zero trust strategy. With this in mind, Barney has driven USCIS to become 99.2% single sign-on (SSO) with the goal of being 100% by September 30. "Knowing with exacting detail who has access to your network is unbelievably important for the adoption of zero trust. If you don't have that, stop. Go home. Focus on identity," he said.

> "To master identity in a multi-cloud or hybrid environment, agencies need an independent, neutral platform."
>
> ***-Ted Girard, VP of Public Sector, Okta***

In addition to identifying and assigning roles to the people on your network, a proper IAM strategy must identify and assign roles to all devices. The ACT-IAC report defines five stages of zero trust, the first three of which focus on this concept of identifying users and devices:

1. Establish User Trust
2. Gain Visibility into Devices & Activity
3. Ensure Device Trustworthiness
4. Enforce Adaptive Policies
5. Zero Trust

After installing agents to take a harder look at network devices, Barney described an "earth-shattering" realization that USCIS had 178,000 assets on its network – averaging four IP addresses associated with every employee.

Make it "button easy"

From secrets management to access control, Barney emphasized that the process needs to be simple for developers to implement, so it becomes something they want that makes their lives better.

USCIS can also shut down the entire system with a flip of a switch – a level of control necessary in a cloud-based, Zero Trust world.

Automation takes processes beyond "button easy" and helps USCIS sift through 4 terabytes per day. Automated Security Operation Centers (SOCs) have allowed the agency to discontinue its tier 1 desk and focus analysts on analytics, while maintaining a watchful eye over three different cloud environments, two data centers, 4,000 developers with broad access, and thousands of telework employees worldwide.

Accelerating the move to zero trust

The pull toward zero trust is strong. Girard said, "Getting the identity management part of zero trust right can accelerate most, if not all, other modernization initiatives by significantly reducing maintenance costs." With 80% of Federal IT spend devoted to maintaining legacy systems, agencies need these opportunities to reduce technical debt.

Draft updates to the Trusted Internet Connection (TIC) policy (TIC 3.0) provide additional momentum for zero trust in government, making the guidelines more accommodating for zero trust-based security models. Agencies are encouraged to focus on reducing risk, and have greater flexibility on the implementation side with TIC 3.0.

USCIS may be leading the path toward zero trust, but other agencies are likewise making progress.

A Federal Emergency Management Agency (FEMA) official shared that the agency is beginning the process, and USCIS's lessons learned may help other DHS component agencies accelerate progress.

DoD's recently released Digital Modernization Strategy highlights zero trust security on a list of innovative technologies it will leverage in its future environment.

Jason Martin, acting director of DoD's Defense Information Systems Agency (DISA) cyber directorate, spoke at the *FCW* Cybersecurity Summit and shared plans to open a DISA lab for researchers to test different strategies for building zero trust network architectures across the Pentagon.

Along with that progress, Federal agencies face challenges as they implement zero trust including a lack of standardized IT capabilities, and for some – a lack of network visibility. Shared network connections and interdependencies add another layer of complexity.

But, as agencies implement more cloud and hybrid environments, they are increasingly considering a zero trust strategy to protect massive amounts of data in environments without a clear perimeter.