Preparing Federal IT for a Zero Trust Architecture

Highlights from the "Zero Trust for the Hybrid Workforce" Roundtable hosted by ATARC on June 29, 2021

If the overwhelming threat of the coronavirus pandemic temporarily reduced the mindshare of cybersecurity in the mind of the public, a spate of recent cyberattacks have brought issues around cybersecurity back to the forefront. Particularly jarring was the May 2021 Colonial Pipeline attack, which disrupted the operations of a critical pipeline operator delivering nearly half of the East Coast's fuel.

The Biden Administration's May 2021 Executive Order on Improving the Nation's Cybersecurity, itself a result of the SolarWinds attack uncovered in December 2020, is a bold attempt to address America's vulnerability to cyberattack and the evolving threat landscape. The EO recognizes the need for the "Federal Government to partner with the private sector" and calls on federal agencies "to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life." One of the most impactful of these changes is a requirement that the heads of all federal agencies provide "a report to the Director of OMB and the Assistant to the President and National Security Advisor" detailing their plans to move towards a Zero Trust architecture.

In order to help agencies and their partners in industry respond to the challenge of adopting a Zero Trust model, the Advanced Technology Academic Research Center (ATARC), in partnership with identity provider Okta and IT solutions provider V3Gate, put together a roundtable panel of distinguished participants from both federal agencies and industry to share best practices and chart a path forward. Participants discussed the components of Zero Trust, debated the continued relevance of firewalls, emphasized the importance of "knowing thine network," and spoke about the need to overcome cultural barriers to change.

> “Zero Trust is all about contextual-based access to resources.”

Defining Zero Trust

While the general principle of Zero Trust, that devices should not automatically be trusted whether they are inside or outside of a network, is widely understood, the specifics of how this approach should be applied to an organization are subject to a certain degree of interpretation. One panelist referred to Zero Trust as a "lifestyle choice." This description was met with agreement from other panelists, who emphasized that Zero Trust is not a single solution, or even collection of solutions but rather a series of design principles. As another panelist put it: "Zero Trust is all about contextual-based access to resources."

Looking at Zero Trust in this way helps agencies understand that while moving to a Zero Trust architecture is a significant task, maybe even one that at first feels overwhelming, it is not an insurmountable one. In the words of one panelist, Zero Trust "is really not that much different from any other piece of security architecture that we've had for the past twenty-five years…it's not rocket science." In a point that came up repeatedly over the course of the conversation, panelists emphasized the importance of "taking things one step at a time" and making the necessary effort to understand an agency's risk appetite, legacy applications, and network as critical to getting a Zero Trust strategy right.

To Firewall or Not to Firewall?

The panel experienced its most spirited debate around the question of whether or not a firewall was necessary, or even desirable, in a Zero Trust context. When polled about their plans to return to the office, the vast majority of panel attendees indicated that they planned to either work from home full-time or in a hybrid fashion that mixed remote and in-office work. One panelist pointed out that this new reality represents a major challenge for legacy firewalls, which work by protecting a network's perimeter from outside threats. Today's employees expect to connect from anywhere to anywhere, making legacy firewalls less relevant. Another panelist pointed out that many large businesses are looking to jettison their firewalls precisely because of this fundamental shift in the nature of work.

Other panelists countered that while federal agencies may be able to move away from firewalls in the future, when more data is in the cloud, many agencies still rely on legacy applications located on premises for mission-critical operations. The point was also made that it's difficult to draw generalized conclusions regarding whether or not firewalls are appropriate without a clear understanding of network resources, what needs to be protected, and the agency's risk profile. Furthermore, not all firewalls are created equal. There are a wide variety of commercial firewalls, including stateful and stateless firewalls, web application firewalls, etc. available to federal agencies that may be appropriate in different contexts. Finally, it was noted that Zero Trust doesn’t protect against malware, it simply checks to see if an endpoint, service, or identity is trusted, not whether or what’s being delivered is malicious.

Know Thine Network

No point was more strongly emphasized by panel participants than the importance of learning the ins and outs of their agency’s network, components, and traffic patterns for cybersecurity professionals. Agency networks are often more than twenty years old; cybersecurity professionals need to work closely with network engineers, many of whom have decades of experience, in order to understand where their data lives, where their devices are, which services are supporting which customers, and where their security infrastructure is. Answering these questions can take over a year even for an experienced architect. Yet panelists cautioned attendees to not to skip this important step lest their Zero Trust deployments become “nightmares” due to a lack of preparedness. In the words of one panelist: “you have to know what you’re protecting in order to protect it.”

> ❝You have to know what you’re protecting in order to protect it.❞

Putting this into practice requires a willingness to go through the basics. While many cybersecurity professionals understandably want to focus on the more exciting work of threat hunting, positioning their agency for success with Zero Trust requires them to devote at least part of their time to more mundane tasks, like identity hygiene. Because Zero Trust architectures place so much emphasis on identity verification, it is absolutely critical that cybersecurity professionals periodically review their service accounts, which typically have more expansive privileges than normal user accounts, to delete those no longer in use and ensure that identities are where they should be. For example, only appropriate HR professionals should have access to HR data, developers should not.

Overcoming Cultural Barriers

Panel participants and attendees were also clear that agencies cannot hope to successfully adopt a Zero Trust architecture without an understanding of the “human element” and the potential internal roadblocks to change. In the words of one attendee: “Culture and people are the biggest challenge in enterprise change management. Technology is the easy part.” Many of the internal problems boil down to a culture of silos. The vastness of the federal technology landscape means that agencies, departments, and teams often work in silos with their own data and applications. Panelists encouraged attendees to look into which services could be provided at the department, or even the agency, level and aim to consolidate disparate solutions as much as possible.

> ❝Culture and people are the **biggest challenge** in enterprise change management.
>
> Technology is the easy part.❞

The other human barrier to Zero Trust adoption in the public sector is speed. According to one panelist, “if you’re going through a year of procurement and a year of ATO, that ship has sailed. What you’re building is already outdated.” Another panelist added that if it’s taking a security team a year to approve an application that has already received FedRAMP ATO, the fault lies with the security team, not with the application. However, requiring security teams to be agile and responsive to the needs of the business does not absolve other parts of the organization from their responsibility for maintaining a secure environment. In particular, panelists pointed to the prevalence of phishing attempts, where fraudulent messages are sent in an attempt to get users to divulge sensitive information, as the cause of many breaches and made the case that “everyone in the organization needs to be security-minded” and vigilant.

How Okta Can Help

Okta provides a single platform trusted by over 10,000 organizations to secure every identity. As a remote and Zero Trust cybersecurity company, it can share best practices regarding network security. Contact Okta today to learn more!

How V3Gate Can Help

V3Gate, a recognized IT solutions provider for the US Public Sector, delivers quality and brings a unique focus on the future to keep clients ahead of the technology innovation curve. Contact V3Gate to learn more!

Underwritten by: okta V3GATE DELIVERING THE NEW ERA OF IT