

Advancing Zero Trust in US Government Networks

Highlights from a Roundtable hosted by the Advanced Technology Academic Research Center (ATARC) in partnership with Fortinet Federal, July 2024

US government networks are facing unprecedented cybersecurity challenges as technology advances at breakneck speed. From budget to culture, agencies are facing numerous roadblocks preventing them from advancing Zero Trust. In a recent roundtable discussion, Federal experts explored these challenges while underscoring the ongoing potential of Zero Trust to fortify cybersecurity now and into the future.

Current Status of Zero Trust

“No pillar stands alone.”

For several agencies represented on the panel, the Zero Trust network pillar has been the least challenging pillar to activate. The network is typically more centrally managed compared to other Zero Trust pillars where applications are decentralized, have different system owners, and require significant segmentation.

Other agencies have benefitted from developing their architecture in parallel to the issuance of the Zero Trust mandates, allowing them to incorporate Zero Trust concepts early on. Agencies without this opportunity are in various stages of updating or replacing legacy systems to comply with Zero Trust. Simply determining which Zero Trust capabilities are already in place can take agencies considerable time.

Although there are several maturity models agencies can adopt, several agencies on the panel have adopted the Cybersecurity and Infrastructure Security Agency (CISA) maturity model. Panelists recommend not deviating from a maturity model once established in order to make continued progress. Regardless of the model, many agencies are now determining how to mature the model based on their unique requirements.

Several agencies have established program offices or dedicated Zero Trust Teams to coordinate Zero Trust implementation across the enterprise. Subject matter experts partner with enterprise architect teams while working with cybersecurity and privacy divisions to update and develop Zero Trust processes and procedures.

Due to resource limitations, most agencies are gradually working towards advancing Zero Trust. However, a few have been able to accelerate implementation in a matter of months with the help from Technology Modernization Funding (TMF). With this upfront funding, they've been able to establish a Zero Trust Program Office, PMO team, and working groups, procure a Secure Access Service Edge (SASE) solution, migrate from legacy VPN, refresh firewalls with updated security policies and rules, and deploy endpoint detection response on all laptops and centralized services.

Challenges with Advancing Zero Trust

Culture

“Zero Trust is not just about technology and implementing the pillars. It’s the culture change of ... how we implement security and manage our resources. Our goal is to create a culture where Zero Trust principles are incorporated into everything people do on a daily basis.”

The predominant challenge with advancing Zero Trust is with changing workforce culture. Several panelists discussed specific challenges with their ability to secure funding to secure operational technology and IoT devices. Current leadership often fails to see the long term value of doing so.

Segmentation

As agencies begin to implement Zero Trust, they’re forced to examine the extent to which they must segment their networks. For large organizations, segmentation quickly becomes complex due to the federated nature of the networks.

Agencies are working to map the flow of data within a particular environment, while determining how to best macro segment the environments to control access to information. Agencies are also looking at implementing software-defined networks where necessary.


Roundtable participants are examining segmentation at all levels of operation, from the enterprise to organizational levels, and writing requirements that will aid in future implementation. Some agencies are experiencing challenges with vendors not incorporating Zero Trust principles in their products. This is especially true for smaller vendors with fewer resources. Agencies should consider sharing their Zero Trust requirements with vendors and make the requirements testable, despite added costs to procurement.

Funding

“This may be the first time that we have had IT innovation that’s contributed to a dramatic re-baselining of costs.”

Several on the panel firmly believe the implementation of Zero Trust will realize millions – even billions – in savings. However, most cannot secure the upfront funding required to advance Zero Trust implementation. The government is in a budget crisis, and panelists are extremely concerned about a potential scenario where cybersecurity funding is cut. The general consensus is that agencies cannot fulfill all Zero Trust mandates with current funding levels.

Some panelists are proponents of taking advantage of TMF funding to help offset the upfront investment of Zero Trust. Many are confident in the promise of Zero Trust cost savings, but a few agencies are not willing to take on that risk and are instead strategically implementing Zero Trust.



Agencies are also challenged by obtaining funding for ongoing maintenance costs. IT leaders must consider the costs to maintain capabilities for up to 5 years when submitting funding requests, yet many are finding it difficult to justify these costs to leadership. Even for those agencies that have secured TMF funding, obtaining funds for future maintenance costs is still a concern.

Agencies must also justify the costs of additional skilled personnel to manage both Zero Trust operations and governance processes. However, justifying funds for additional personnel is challenging especially if the agency is making do with existing staff levels. Panelists underscore the importance of having dedicated subject matter experts to manage the complexity of Zero Trust implementation.

Leaders should consider how they are communicating requests for Zero Trust funding. One panelist recommends focusing the requests on the security threats predicated on inaction. They also urge agencies to measure their Zero Trust implementation in order to better articulate the gaps in resources.

Looking Ahead

Panelists are energized by the potential of Zero Trust to transform how cybersecurity is conceptualized and operationalized. The concept of Zero Trust gives agencies control down to the identity and data layer, which indisputably changes how agencies secure networks. As agencies move away from network-centric to data-centric architecture, the concept of 'network' will continue to evolve and advance cybersecurity.



LEARN MORE AT:

[HTTPS://WWW.FORTINETFEDERAL.COM](https://www.fortinetfederal.com)