Zero Trust: A New Frontier in Federal Cyber Resilience

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

Through rigorous access controls and real-time monitoring, zero trust architecture empowers federal agencies to respond to evolving cyber threats with precision and effectiveness. Although there are clear benefits, implementing zero trust in the federal government presents unique challenges.

During a recent roundtable discussion, federal experts explored the topic of zero trust and discussed challenges with data governance, workforce development, and technology integration, while highlighting the potential of AI to enhance zero trust architectures.

Federal Zero Trust Adoption

Agencies at the roundtable discussed their progress with implementing zero trust. While it's common to begin a zero trust journey with identity and access, one agency started with data loss prevention. Throughout the discussion, panelists underscored the criticality of data integrity in successful zero trust implementation.

Regardless where agencies start their zero trust journey, many discover that fundamental security measures are not in place. As agencies modernize with AI, panelists note that the majority of security issues that are emerging are traditional security vulnerabilities rather than issues caused by new technology.

Another roundtable participant started their journey with zero trust from the bottom up by evaluating their existing technologies to determine how best to implement zero trust in each. However, the security rules built from one program do not automatically import into another.

Agencies stress that zero trust is not something you can buy, rather it's the interplay between technology and programs. To implement zero trust effectively, agencies must follow a strategy and lean on the expertise of different teams and vendors.

> **"While we're making progress, it's slowed down by simplicity."**

Some agencies have set up program management offices for zero trust, composed of project and program managers and technical experts. This allows agencies to reinforce foundational security principles and make significant progress towards automation and deploying data prevention and data tagging capabilities.

Data Governance

> **"If we get data wrong, it's all for nothing."**

Perhaps the most important component of zero trust is data. Participants stressed how critical data governance is to successful zero trust implementation. Agencies can have robust network monitoring in place, but if data is not mapped to specific entities then it's not true zero trust.

Agencies must have a firm understanding of how sensitive data is defined and where it is located. Data tagging is not only critical to effectively implement a zero trust strategy, but it also enables agencies to share data more easily. One agency developed their own internal specifications for data governance after facing challenges with properly protecting classified data and separating it from unclassified domains.

As one panelist noted, data governance is not just a problem in government. Organizations across industry are challenged by data governance. Part of the challenge is a lack of proper tools, but panelists agree a bigger impediment to zero trust implementation lies with people.

Workforce Development

Roundtable participants discussed how workforce development and culture are slowing down zero trust implementation. One panelist shared their attempts to hire a zero trust architect, but found it challenging to find a qualified applicant who understands government, zero trust governance, and specific technologies.

Other panelists are roadblocked by agency leaders who cannot make knowledgeable decisions to guide zero trust implementation. For instance, one panelist tried to implement role-based access controls to certain data sets, but leaders did not know what level of access their staff needed. Some agencies on the panel are turning to Chief Data Officers to solve this and other challenges with unstructured data.

Because the speed at which these policies and technologies are changing, successful zero trust implementation hinges on people. While there is a notable skills gap across government, panelists note that agencies should also pay attention to the skills and abilities of vendors and contractors.

As one panelist observed, small businesses typically do not have the capacity to upskill workers at the intensity and pace required of this frenzied tech environment. This can pose implementation challenges that agencies could not have anticipated during the acquisition process. As such, agencies should consider a vendor's capacity to upskill their talent while evaluating solutions.

Panelists also note that vendors often claim to meet specific security controls, but fail to meet them outside of greenfield environments. This underscores the need for more robust security assessments and better education around zero trust implementation requirements for agencies and partners alike.

Implementation Challenges

Further roundtable discussion centered on other challenges surrounding zero trust implementation, such as funding constraints and policy contradictions. Smaller agencies are especially challenged with securing dedicated funding for zero trust initiatives.

Despite numerous memoranda and guidelines, only one mandate mentions funding, which isn't sufficient. With budgets shrinking year over year, agencies are struggling to allocate resources towards zero trust, and often prioritize immediate needs over long-term security goals.

Additionally, the lack of standardized guidance and the abundance of controls from different sources create confusion and make it difficult for agencies - and vendors - to determine the best approach to implementation. While the federal government is pushing for zero trust adoption, agencies are often hindered by outdated security protocols and legacy systems that are not compatible with modern security practices. This creates a conflicting situation where agencies are encouraged to move towards a new security model but are held back by outdated infrastructure and practices.

AI and Zero Trust

> **"AI is a problem for those who don't understand their data."**

Artificial intelligence (AI) has the potential to significantly enhance zero trust architectures by automating processes, improving cross-pillar mapping, and analyzing large amounts of data quickly. However, the integration of AI also introduces new security challenges and risks that agencies must address.

Agencies should pay particular attention to API connections and what type of data is accessible in AI powered machine-to-machine communication. Implementing robust attribute-based controls can help mitigate risk, particularly when accessing unstructured data. While LLMs are especially useful to access unstructured data, agencies must have proper access controls in place. One panelist suggested developing an internal model to access an agency's own data, where access to the model and data are the same.

As AI becomes more embedded into everyday technology, the federal government must move quickly to understand the implications of AI on cybersecurity and take actions to bolster cyber resilience. One panelist indicated a need for AI attestation from vendors, similar to other attestations required during the procurement process.

Ultimately, how AI is used comes down to a business decision. Users are adopting AI whether tools are vetted or not, so it's incumbent on federal leaders to enable safe and controlled access to AI where possible.