Decoding Zero Trust: Unveiling Its Role in Modern Cybersecurity

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

In a recent roundtable discussion, Federal experts discussed the critical role of Zero Trust in modern cybersecurity operational technology (OT). The discussion highlighted various factors that foster Zero Trust implementation, including cultural changes, proactive engineering approaches, effective identity management, and collaboration across agencies.

While budget constraints and legacy systems pose challenges, the overarching consensus among roundtable participants is that Zero Trust is achievable, potentially cost-effective, and essential for modern cybersecurity. The future integration of AI further underscores the need for a solid foundation in Zero Trust principles today.

Zero Trust is Now Mainstream

Roundtable participants note there's a growing understanding of Zero Trust principles across government agencies. Vendors are spending less time educating federal clients on the merits of Zero Trust, which allows them to more effectively implement solutions.

Implementation of Zero Trust has also become less complicated and a much faster process. Some agencies are able to implement Zero Trust at a microsegmented level in a few as 90 days. Some agencies are able to implement Zero Trust relatively inexpensively by using existing infrastructure.

Importance of Cultural and Organizational Change

Although more achievable than ever before, implementing Zero Trust at scale requires a significant cultural shift within all levels of an agency. Panelists noted that Zero Trust does not start and stop with IT professionals. In particular, acquisition professionals, engineers, and agency leaders must be knowledgeable about Zero Trust since they have a direct role in making Zero Trust a reality.

> **"We need awareness of as many people as possible. People who are on the outside, not necessarily in the middle of the implementation of Zero Trust."**

Some agencies represented at the roundtable host educational initiatives, such as Zero Trust days or town halls, to spread awareness of Zero Trust throughout the agency. Panelists note that these events are very well attended, since so many people are interested in learning about Zero Trust.

Panelists also emphasized the foundational role of infrastructure architecture and engineering in successful Zero Trust implementation. The patchwork approach agencies are taking to architect cybersecurity systems lacks strategic direction. Effectively implementing Zero Trust requires some strategy rather than layering controls piecemeal.

Roundtable participants are concerned that most agencies remain in a reactive security posture. There's a need for agencies to take a proactive stance by prioritizing the continuous improvement of infrastructure. As one panelist noted, Zero Trust is not merely a plug-in to a product; rather, achieving Zero Trust requires a fundamental shift in engineering cybersecurity.

"Cybersecurity is all about engineering and architecture. What Zero Trust is doing is exposing issues with architecture and engineering in general."

Funding and Acquisition Challenges

Panelists also discussed challenges with adequately funding and procuring solutions that support Zero Trust implementation and follow Zero Trust standards. Obtaining buy-in from both political and executive leadership is critical to successful Zero Trust implementation, which is the foundation of modern, robust cybersecurity.

Roundtable participants emphasized the importance of prioritizing cybersecurity in future budget cycles and to strongly advocate for cybersecurity funding now. Panelists emphasized the need to prioritize Zero Trust in immediate budget cycles, as waiting until 2026 or 2027 will be too late and put agencies at a significant disadvantage as technology accelerates at record pace. In general, panelists do not see cybersecurity as a partisan issue, but can foresee budgets tightening further as national debt continues to rise.

Despite strained budgets, some panelists argue that the cost of cybersecurity and Zero Trust implementation will stabilize as legacy systems are replaced and more efficient systems are strategically developed from the outset.

Panelists also noted that the nature of cybersecurity has changed as the price of technology continues to fall. Advanced technology was once accessible only to governments and industry. Now, the most advanced technology is available to anyone. Existing legacy systems were developed under this old paradigm, which further underscores the importance of investing in Zero Trust architecture to modernize cybersecurity and keep up with adversaries.

Roundtable participants discussed several ways they are identifying Zero Trust solutions, from working groups to traditional procurements. Many agree that the traditional acquisition process does not consistently include Zero Trust standards. One panelist recommends a FedRAMP-like ranking process where products are certified to meet certain Zero Trust microsegmentation standards.

Some agencies find it challenging to verify if vendors' solutions meet Zero Trust standards and which pillar the solution meets. Developing a catalog of Zero Trust approved products would help agencies understand which solutions have been validated for meeting specific Zero Trust pillars.

Additionally, vendor solutions often claim to 'harden' the network, when in reality the solution simply conceals it from the rest of the network. Other challenges include solutions with embedded Wi-Fi and no option to remove it. Unfortunately, requests for design changes from a single user are unlikely to be met, which is more reason for enterprise-wide Zero Trust acquisition standards. Due to these challenges, panelists recommend engaging with vendors early to ensure Zero Trust requirements are included in procurement.

Role of Identity and Access Management

Panelists consider proper identity and access management the cornerstone of Zero Trust. The shift from role-based to attribute-based access controls is essential for effective Zero Trust implementation and modern cybersecurity. Zero Trust identity and access management enables agencies to secure any network by assigning attributes to non-person entities.

To do this effectively, agencies must prioritize data integrity and data management practices. Without proper data tagging, modernizing cybersecurity, such as broadening Federal access to secure 5G networks, is not possible. Automation and AI are viewed as key enhancers of Zero Trust and modern cybersecurity, but foundational elements like proper data tagging and attribute management must be in place first.

Collaboration and Continuous Improvement

> **"Artificial intelligence is absolutely a game changer, and we can either sit back and let it completely dominate us, or we can actually take advantage of it. We've got to do that with Zero Trust."**

Panelists acknowledge that while there is still plenty of work to do to achieve Zero Trust, progress is being made. Initiatives like program management offices for Zero Trust and integrating Zero Trust principles in governance frameworks are steps in the right direction.

Panelists note there are unprecedented levels of collaboration between agencies that was unheard of a decade ago. Agencies are coming together to share cybersecurity solutions to combat a greater existential threat.

To continuously improve, agencies must start measuring the success of Zero Trust implementations through metrics and verified practices like red team testing. The success of Zero Trust implementations should be measured using metrics and verified through practices like red team testing. Of equal importance is celebrating short-term wins. Demonstrating Zero Trust successes develops greater buy-in and builds positive momentum.