Technology Trend Topic: Zero Trust Architecture (ZTA)

Publish Date:
9/23/2020
Published By
Catherine Adams

ITC SMEs: Lawrence Hale, Albert Ingram, Anissa Burley, and Tonya Pruitt

Current ITC Vehicles Highly Adaptive Cybersecurity Services 54151HACS (formerly SIN 132-45), Continuous Diagnostic & Mitigation Tools 541519 CDM (formerly SIN 132-44), Enterprise Infrastructure Solutions (EIS), 8(a) STARS II, Alliant 2

Vehicles to Watch 8(a) STARS III. Expect to see more ZT-specific language in upcoming contract releases and modifications

Overview

Zero Trust (ZT) is a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated. Zero Trust Architecture (ZTA) is an end-to-end approach to enterprise resource and data security that encompasses identity (person and non-person entities), credentials, access management, operations, endpoints, hosting environments, and the interconnecting infrastructure. ZT restricts resources to those with a need to access and grants only the minimum privileges needed to perform the mission. **- NIST SP 800-207**

A ZT approach to cybersecurity requires multi-factor authentication, micro-segmentation, least privilege access control, and continuous monitoring. Automating these techniques reduces the burden on employees, letting them devote more energy and time to their agency's mission. **- GovLoop**

ZT will not only help security posture, but will also help modernize your environment and improve organizational productivity. **- Microsoft**

The proliferation of cloud computing, mobile device use, and the Internet of Things dissolved traditional network boundaries. Hardened network perimeters alone are no longer effective for providing enterprise security in a world of increasingly sophisticated threats. **- NIST**

"ZT" was coined by a Forrester Research analyst in 2010, based on the outdated assumption that everything inside an organization's network should be trusted. **- Palo Alto Networks**

Market Trends

Pivoting toward ZT must prioritize security, practice basic cyber hygiene, modernize assets and retain competent talent. - **Federal News Network**

By 2023, 60% of enterprises will phase out most of their remote access virtual private networks (VPNs) in favor of Zero Trust Network Access (ZTNA). **- Gartner**

The world's data will grow to 175 zettabytes by 2025 from 33 zettabytes in 2018. There are zettabytes of data from nearly every agency, especially as the Internet of Things devices grows. The dependency on data to run missions, serve citizens and protect the nation depends on security and resiliency. **- Federal News Network**

> **"We have to understand our data; we have to understand how our users interact with that data and how important that data is to our mission. If we can't answer that fundamental question, then don't even start down ZT."** - Steven Hernandez, Department of Education

Every ZT initiative must understand hardware and software assets, mapping Phase 1 of the Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) program - automation of hardware and software asset management and configuration settings. **- Gigamom**

Use Cases/Applications

ZTA migration is a journey that will likely operate in a hybrid ZT and legacy mode as agencies continue their IT modernization investments. **- NIST**

In 2015, the Office of Personnel Management (OPM) was attacked with more than 20 million personal records compromised. Once the attackers were inside, they could move freely around the network, gaining more and more access to data. This could have been prevented with a ZT strategy to prevent backdoor access. **- GovLoop**

As federal agencies continue to support large numbers of remote workers, agencies are becoming more comfortable with ZT and are seeking to lay the foundation for deployments. **- FedTech Magazine**

- The **Defense Information Systems Agency (DISA)** is standing up a lab to test different strategies for building ZTNAs across the Pentagon, focusing on: creating a framework for continuously monitoring and checking access on different layers of the network and building out tools to manage identity and access.
- The **Small Business Administration (SBA)** led the effort to use cloud tools to meet the spirit and intent of CDM and Trusted Internet Connections (TIC) TIC policies and is now modernizing its network architecture to incorporate ZT with 5-6 pilots.
- **DoD's Defense Innovation Unit** will launch a pilot for a secure cloud management solution that may lead to granting ZT access to about 500,000 concurrent Defense Department users.
- **Air Force's information warfare wing** launched a small-scale ZT pilot with the goal of establishing a common architecture and framework that allows you to localize customization of security roles and responsibilities across the entire Air Force.

> **"Agencies made good progress on who is on the network, but most still need to improve understanding of why the user is accessing the data and what they are doing with it."** - Suzette Kent, Former Federal CIO

Risks/Challenges/Myths

Lack of cybersecurity maturity is the largest operational challenge to deploying successful ZT solutions government-wide. **- ACT-IAC**

ZT is perceived as costly and complex. However, it is built upon your existing systems; there are no ZT products. **- Palo Alto Networks**

Some organizations are hesitant to implement ZT as SaaS because they might have legacy applications that will either delay, or prevent, cloud deployment. **- Cybersecurity Insiders**

Traditional VPNs are not capable of meeting the growing demands of today's perimeter-less digital business, which inherently puts a hole in the firewall. **- Akamai**

Agencies have a problem with provisioning the right level of access to devices and people. ZT can help strike a balance between carelessness and caution. **- GovLoop**

What You Should Read NOW

1. NIST Special Publication, 800-207, Zero Trust Architecture
2. ACT-IAC Zero Trust Cybersecurity (April 2019)

Federal policies aimed to restrict data and resource access to authorized parties: Federal Information Security Modernization Act **(FISMA);** Federal Identity, Credential, and Access Management **(FICAM);** Trusted Internet Connections **(TIC);** and Continuous Diagnostics and Mitigation **(CDM)** programs

Upcoming Technology Trends Topics

Robotic Process Automation (RPA) and Shared Services Overview

We want to hear from you! Use this **survey link** to share your ideas

Published Technology Trends Topics

Visit the **ITC Resource Center's Tech Corner** for the complete list