ZERO TRUST ARCHITECTURE PRIMER

This is the first in a series on the topic of Zero Trust (ZT) from AAC. Further topics will include implementing ZT in a net new environment and how an organization can evolve from a legacy environment to a ZT environment.

ZERO TRUST FEDERAL REQUIREMENTS

Following issuance of Executive Order (EO) 14028 Improving the Nation's Cybersecurity, the Office of Management and Budget (OMB) released memo M-22-09 defining an approach to achieve a Federal zero trust architecture (ZTA) strategy and requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024. The EO defines Zero Trust (ZT) as a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both **inside and outside** traditional network boundaries.

According to the Order, the ZT security model eliminates implicit trust in any one element, node, or service. Instead, it requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses.[1] Previously, frameworks commonly referred to as castle and moat models allowed trusted access once you successfully crossed over the defensive perimeter (the "moat"). With ZT, every individual element within the perimeter (application, subnet, web page) requires verification and authentication before granting access.

During the past few years, engineers have recognized and attempted to rectify the shortcomings with existing cybersecurity models. Previously, once a bad actor penetrated the network by successfully breaching the perimeter, they could exploit existing vulnerabilities within that environment. Once "inside", he or she could move across the organization's network, compromising assets and causing irreparable damage. Using a ZT model, if a bad actor were to gain access to the environment, that access would be significantly restricted to only the specific space (user, microservice, API, device…) where access was initially granted. Every subsequent resource the bad actor attempted to access would require additional authentication and verification procedures while continuing to monitor observable behaviors, known assets, and IP addresses.

Previously, when a bad actor was able to breach the enterprise, data, and other resources, their access traditionally would have been based on two factor authentication without consideration of other factors, like time of day, physical location, and sensitivity of the data. In a ZT environment all the above factors and more would come in to play to grant access to the user--restricted to only the data and systems needed based on an extensive set of policies and rules.

Returning to the premise in ZTA that a breach is inevitable or has likely already occurred, the construct limits access to only what is needed while looking for anomalous or malicious activity. A ZTA allows a user full access—but only to the absolute minimum systems needed to perform

[1] Biden, Joseph. "Executive Order on Improving the Nation's Cybersecurity." Whitehouse.gov. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (accessed 2/15/2022)

their job. If a device is compromised, ZT ensures damage is contained and minimized through access compartmentalization.

Illustrated in **Figure 1**, ZT at a very basic level has two zones—untrusted and trusted—with a decision process to grant only the access needed to accomplish a request made to a trusted asset.

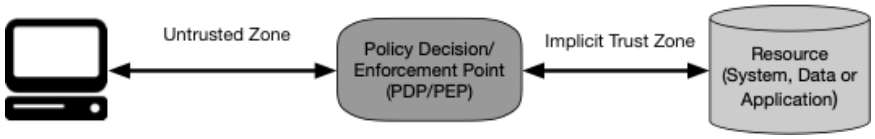

Figure 1: Basic Concept of Zero trust*[2]

The ZTA's comprehensive security environment includes the following features: monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting data in real-time within a dynamic threat environment.

This data-centric security model allows the concept of least-privileged access to be applied for every access decision, where the answers to the questions of who, what, when, where, and how are critical for appropriately allowing or denying access to resources based on the combination of the above factors

From a practical perspective zero trust moves us from the legacy security models of the last few decades where access is granted by roles and responsibilities to a "need to know" model.

The seven tenets of ZT, defined in NIST SP 800-207[3], are illustrated in **Figure 2** below illustrating the restriction of identity, access, system, and behaviors to deliver a ZT framework.

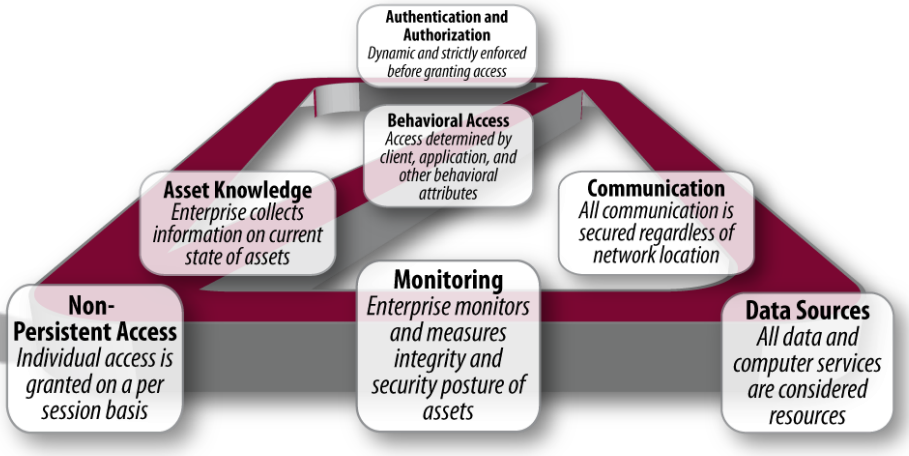

Figure 2: 7 Tenets of a Zero Trust Framework

[2] Rose, Scott, Oliver Borchett, Stu Mitchell, and Sean Connelly. "Zero Trust Architecture." p.5 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf (accessed 2/21/2022)

[3] Rose, Scott, Oliver Borchett, Stu Mitchell, and Sean Connelly. "Zero Trust Architecture." pp.6-7 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf (accessed 2/16/2022)

As organizations engage the 7 Tenets of a ZT framework, they increasingly secure identities, applications devices, data, infrastructure and networks. This process is evolutionary in nature and continually evolves, but by progressing down the ZT path, organizations improve their security posture making it more difficult for bad actors outside and inside the organization to inflict damage.

In the next article on this topic, we will discuss how we can move from the legacy world to a ZT world including assessing what components are already in place and what will need to be added.

HOW AAC CAN HELP

Are you a federal organization looking to comply with the EO and OMB Zero Trust mandates? Not sure where to begin? Let us know. AAC has been delivering enterprise IT solutions including cyber security architectures like Zero Trust for over 39 years for federal customers. Let our cyber experts help you implement and integrate a Zero Trust Architecture in your environment.

For more information or to learn how AAC can support your agency's Zero Trust evolution, please contact us at aacbd@aac.com

*Content in this article is based on NIST 800-207

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf