Zero-Trust Architecture

A Key Ingredient in the Recipe for Supply Chain Resilience

What is Zero-Trust Architecture?

Zero-Trust Architecture (ZTA) is a cybersecurity model based on the absence of implicit trust. Zero Trust assumes distrust among assets, accounts, individuals, or organizations despite physical or network proximities, shared locations, or common ownership.

Zero Trust assumes breaches will occur or have already occurred. ZTA is a practice to defend against threats that exist both inside and outside of traditional network boundaries.

National Institute of Standards and Technology Special Publication NIST SP 800-207 (2020) offers the following definition of zero trust and ZTA:

> *Zero trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. ZTA is an enterprise's cybersecurity plan that uses zero trust concepts and encompasses component relationships, workflow planning, and access policies.*

Supply Chain Benefits of Zero-Trust Architecture

A ZTA is a valuable tool for protecting against supply chains attacks that achieve access by exploiting third-party suppliers. ZTA limits the reach a malign actor can achieve through a compromised supplier.

A 2013 supply chain cyber attack against one of the largest retail companies in the United States resulted in the theft of financial and personal information from 110 million customers. Thieves used vendor credentials to access other parts of the retailer's computer networks. In 2020, attackers infiltrated the network of a hospitality giant using stolen staff credentials, resulting in a data breach impacting 339 million guests. In both of these cases, ZTA could have mitigated or prevented damage that perimeter-based security models failed to stop.

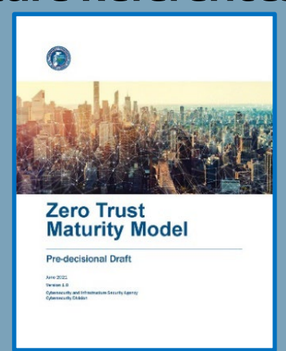
Implementing a Zero-Trust Architecture requires mapping the digital attack surface. Because this process includes identifying all cyber assets, it confers greater oversight and a better understanding of at-risk elements within a supply chain. Consequently, Zero-Trust Architectures provide better opportunities to detect attacks on a supply chain. Faster and more reliable detection enables mitigation efforts and can enhance compliance with reporting requirements.

Zero-Trust Architecture Basics

- Always treat the network as hostile; assume breaches are inevitable or have already occurred
- Assume external and internal threats exist on the network at all times; secure all communications regardless of network location
- Limit access to individual enterprise resources on a dynamic, continuously verified, per-session, as-needed basis instead of offering implicit trust; authenticate every device, user, and network flow
- Constantly monitor for suspicious behavior
- If properly implemented, Zero-Trust Architecture contains cyberattacks and limits their damage

Zero-Trust Architecture References

NIST SP 800-207 Zero Trust Architecture (2020)



DHS CISA Zero Trust Maturity Model (2021)

Dated: 7 April 2023