

Zero Trust Architecture

U.S. Government Accountability Office
November 22, 2023



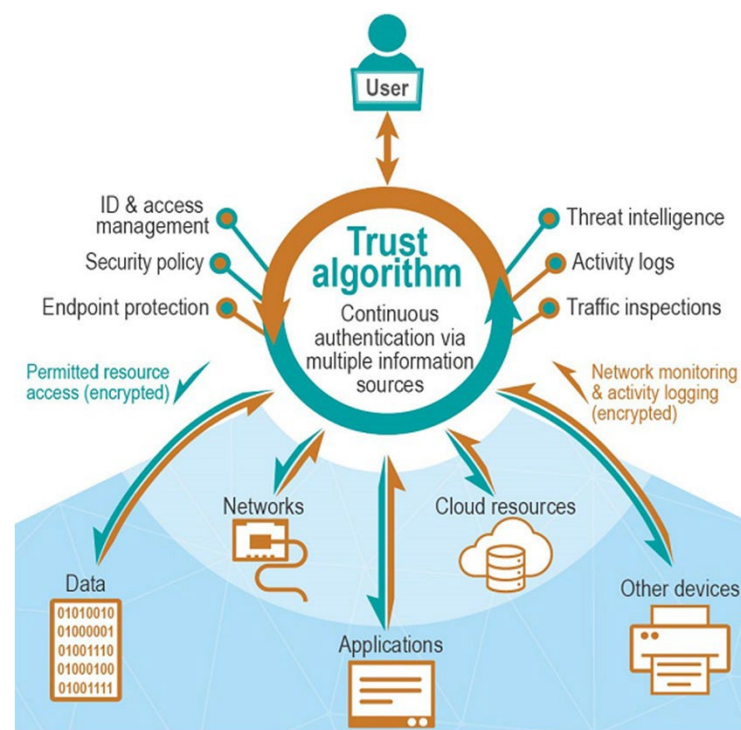
Who We Are

GAO is an **independent, nonpartisan agency** that advises the United States Congress about ways to make government more efficient, effective, ethical, equitable, and responsive.



What is Zero Trust Architecture?

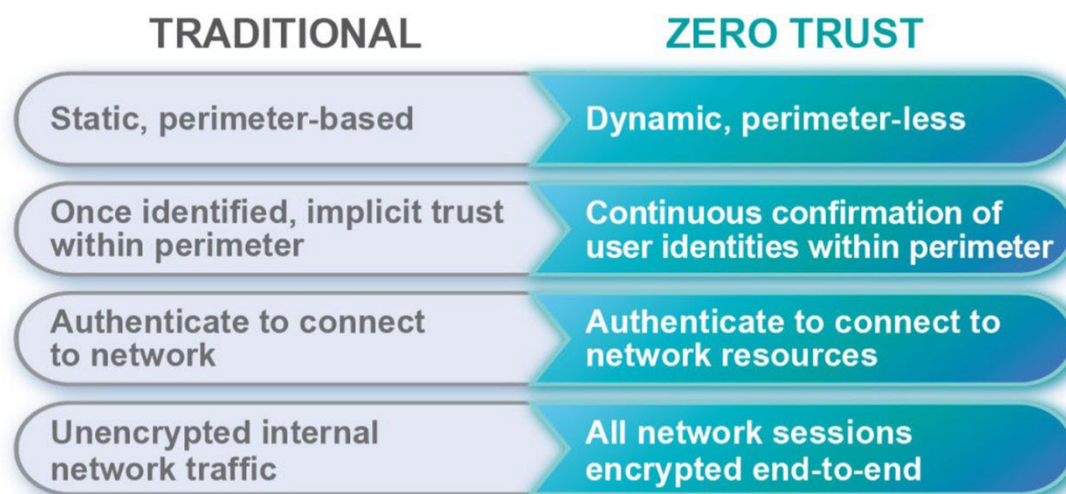
- Zero trust architecture (ZTA) is a cybersecurity approach intended to address rapidly evolving cybersecurity risks.
- A ZTA approach focuses on authenticating and authorizing every interaction between network resources and a user or device, which is different than a traditional, perimeter-based security model.



Source: GAO analysis of NIST documentation. | GAO-23-106065

Why Does ZTA Matter?

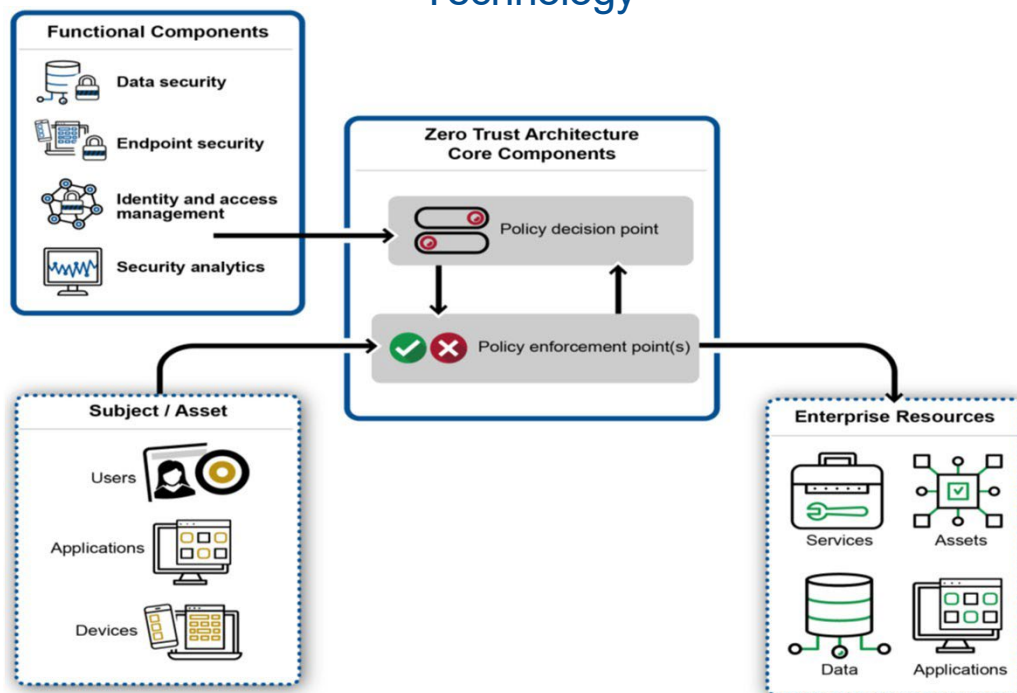
- As IT systems become larger and more complex, they are more susceptible to cyberattacks.
- By moving away from perimeter-based security models, the impact of cyber incidents can be limited.



Source: GAO analysis of industry sources. | GAO-23-106065

How Does ZTA Work?

Basic example of ZTA per the
National Institute of Standards and
Technology








Source: GAO interpretation of National Institute of Standards and Technology zero trust architecture concept; image: lembervector/stock.adobe.com. | GAO-23-105466

- Policy decision point: grant access to a resource for a given subject – uses a “trust algorithm”
- Policy enforcement point: enables, monitors, and terminates connections
- Data sources that provide input and policy rules to the algorithm:
 - Data security
 - Endpoint security
 - Identity, credential, and access management tools
 - Security analytics

Selected U.S. Federal Guidance

- National Institute of Standards and Technology SP 800-207: *Zero Trust Architecture* – August 2020
- Executive Order 14028, *Improving the Nation’s Cybersecurity* – May 2021
- Cybersecurity and Infrastructure Security Agency: *Zero Trust Maturity Model* (version 1.0, draft) – June 2021
- Office of Management and Budget: *Federal Zero Trust Strategy* – January 2022
- Cybersecurity and Infrastructure Security Agency: *Zero Trust Maturity Model* (version 2.0) – April 2023

Cybersecurity and Infrastructure Security Agency ZTA Maturity Model

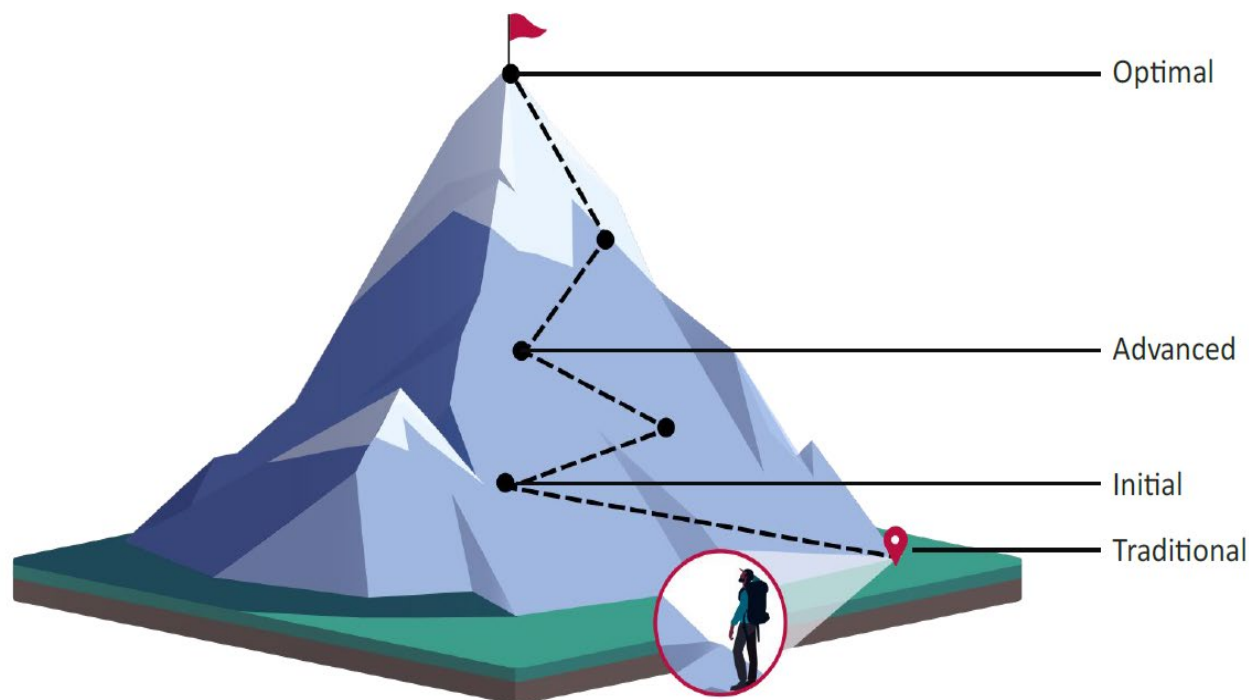
Identity 	Enforcing access controls to confirm the identity of all users. Ensuring that the right users have the right access at the right time.
Device 	Compiling and maintaining ongoing inventories of all devices connected to the network. Ensuring that devices are secure to prevent, detect, and respond to unauthorized access to an enterprise's resources.
Network 	Encrypting open communication channels that are used to transport messages on the network. Segmenting those channels into isolated environments.
Applications and Workloads 	Securing and managing applications by performing rigorous internal and external testing and decreasing reliance on network security.
Data 	Protecting data on devices, networks, and applications by implementing enterprise-wide logging and information sharing.

- Cybersecurity and Infrastructure Security Agency developed guidance based on five "pillars."
- Subsequent Office of Management and Budget guidance used the same pillar structure.
- Both agencies aligned their guidance

Source: GAO analysis of the Cybersecurity and Infrastructure Security Agency's Zero Trust Maturity Model Version 1.0 (draft) and other relevant federal policies and guidance; images: lembervector/stock.adobe.com. | GAO-23-105466

Maturity Model, Continued

Zero Trust Maturity Journey



Source: Cybersecurity and Infrastructure Security Agency,
Zero Trust Maturity Model (version 2.0) – April 2023



Office of Management and Budget Zero Trust Strategy

- Around 20 actions across five pillars for agencies to take
- Emphasis on:
 - Multifactor authentication
 - Device inventory HTTPS/encryption
 - Application security testing
 - Data encryption/backup
- Completion expected by end of September 2024 (although this is a starting point)

Challenges in Implementing ZTA

- Resources needed to transition to ZTA
 - ZTA is a large endeavor for organizations as large and complex as federal entities
 - New tools, practices, and training will be needed
- Interoperability and legacy systems could be difficult to integrate into ZTAs
- Governance frameworks and technical standards are still emerging

GAO Work on ZTA

- GAO-23-105466, *Cybersecurity: Secret Service Has Made Progress Toward Zero Trust Architecture, but Work Remains*
- GAO-23-106065, Science & Tech Spotlight: Zero Trust Architecture

Challenges in Evaluating ZTA

- There is no single ZTA solution
- ZTA implementation is ongoing
- New technologies may be required

Questions to Consider

- What is an appropriate level of oversight to ensure the proper implementation of ZTA?
- What are appropriate performance goals and measures to help justify investments in ZTA?
- What additional standards and frameworks are needed to facilitate ZTA design and implementation?

Questions?

?