GAO | Science, Technology Assessment, and Analytics

SCIENCE & TECH SPOTLIGHT:

ZERO TRUST ARCHITECTURE

NOVEMBER 2022

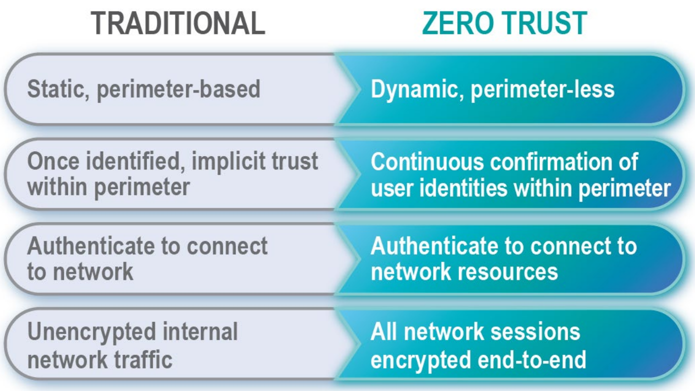
WHY THIS MATTERS

IT systems are vital to the functioning of the federal government, critical infrastructure, and the economy. As IT systems become larger and more complex, they have become more susceptible to cyberattacks. Zero trust architecture is a cybersecurity approach that assumes breaches will occur and uses risk-based access controls to limit the damage from an attack.

/// THE TECHNOLOGY

What is it? Zero trust architecture (ZTA) is a cybersecurity approach intended to address the rapidly evolving security risks faced by IT systems worldwide. These risks include insider threats from employees who either deliberately or unintentionally create a security breach and new, more sophisticated and persistent threats from around the globe. Further, the need to access resources from anywhere, at any time, and with any device has led to increasingly complex IT systems. Because of these and other risks, GAO continues to designate information security as a government-wide high-risk area, including the protection of critical infrastructure from cyber threats and the privacy of personally identifiable information.

The ZTA approach focuses on authenticating and authorizing every interaction between network resources and a user or device. Traditional, perimeter-based cybersecurity models can allow users or devices to move freely within the network once they are granted access. However, building stronger perimeters is no longer sufficient to protect networks, users, applications, and data. In contrast to traditional models, ZTA functions on the principle "never trust, always verify" and assumes that attacks will come from within and outside the network (see fig. 1).



TRADITIONAL	ZERO TRUST
Static, perimeter-based	Dynamic, perimeter-less
Once identified, implicit trust within perimeter	Continuous confirmation of user identities within perimeter
Authenticate to connect to network	Authenticate to connect to network resources
Unencrypted internal network traffic	All network sessions encrypted end-to-end

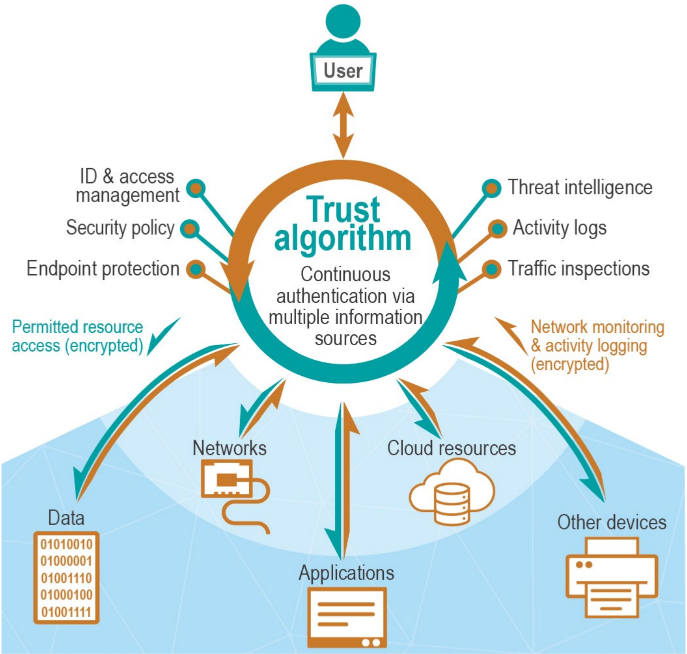
Source: GAO analysis of industry sources. | GAO-23-106065

Figure 1. Comparison of traditional and zero trust cybersecurity architectures.

How does it work? ZTA aims to continuously monitor and protect all activity and resources on an IT network. Given the increasingly complex nature of IT networks, including cloud and hybrid environments, ZTA's goals are to reduce opportunities for attackers by restricting access and to detect attacks by monitoring user behavior and other network activity.

Organizations that use ZTA establish security policies that are applied by a trust algorithm, which ultimately grants or denies access to a resource. The algorithm uses several supporting technologies (see fig. 2), including the following:

- **An identity, credential, and access management (ICAM) system** grants access to certain network resources at certain times based on user information. For example, it may use multi-factor authentication or facial recognition to determine that a specific user is entitled to access.
- **Security analytics** uses threat intelligence, activity logs, traffic inspection, and other information about the network and its resources to detect unusual patterns. For example, data analytics and artificial intelligence techniques identify anomalies that could warrant further investigation.
- **Endpoint protection** ensures that the devices (the endpoints) and their data are protected from threats and attacks. Endpoint protection may include monitoring for intrusions, known vulnerabilities, and malware.
- **Encryption** prevents unauthorized data disclosure, modification, and access.



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

Figure 2. A schematic of how zero trust architecture could control access to network resources.

How mature is it? Commercial products needed for ZTA implementation are largely mature and available. However, ZTA is a systems approach to cybersecurity rather than a technology, and there is no single solution for a mature ZTA. Organizations attempting to implement ZTA have faced difficulties. For example, a National Institute of Standards and Technology (NIST) project to build and demonstrate examples of ZTA using products and technologies from different vendors found that many ICAM and endpoint protection technologies could not be integrated into a functional ZTA.

In addition, some technologies would need to be adapted to implement ZTA. For example, the National Cybersecurity Protection System, which defends the federal government from cyber threats, has intrusion prevention functions that are not compatible with ZTA. According to a NIST publication, the system was originally designed to work on the perimeters of government networks. To be compatible with ZTA, the system would need to be adapted to continuously monitor resources within the network. Further, machine-learning models—which are recommended for automated threat detection—would need to be tailored to each organization's ZTA, a potentially time-consuming process.

The federal government has begun efforts to use ZTA. Since 2020, NIST and the Office of Management and Budget have issued direction and guidance to federal agencies on the use of ZTA. In addition, the Cybersecurity and Infrastructure Security Agency in 2021 issued a draft roadmap on transition to ZTA, and the 2022 National Defense Authorization Act directed the Department of Defense to develop a zero trust strategy and a model architecture.

/// OPPORTUNITIES

- **Confine possible security incidents.** ZTA prevents users, processes, and devices from moving freely throughout a network after gaining access. Damage from any network intrusion will therefore be better contained.
- **Improve situational awareness.** ZTA can provide more visibility into resource usage, which can improve the detection of attacks and lead to more timely responses.
- **Improve data confidentiality.** With improved access controls and encryption, data will be more secure from both internal and external intrusion.

/// CHALLENGES

- **Resources needed to transition to ZTA.** An organization implementing ZTA would need additional resources for computing as well as new tools, practices, and training, which can be expensive and time-consuming. For instance, to establish appropriate access policies, an organization would need to develop and maintain complete information about systems, networks, and data.
- **Interoperability.** Because there is no single ZTA solution, ZTA implementation requires integrating existing technologies with each other and with newer technologies. These technologies may not be designed to work together, particularly in organizations with large investments in traditional technologies.
- **Standards.** Governance frameworks and technical standards for ZTA are still emerging, and there is no consensus on how existing industry standards should be applied to a ZTA implementation.

/// POLICY CONTEXT AND QUESTIONS

- 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?

/// SELECTED GAO WORK

- See GAO's "Cybersecurity" topic website for additional information and products. Washington, D.C., 2022.
- Cybersecurity: Secret Service Has Made Progress Toward Zero Trust Architecture, but Work Remains, GAO-23-105466.
- High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas, GAO-21-119SP.
- Cybersecurity: DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program, GAO-20-598.
- See "Cybersecurity" case study in Artificial Intelligence: Emerging Opportunities, Challenges, and Implications, GAO-18-142SP.

/// SELECTED REFERENCES

Office of Management and Budget, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles Memorandum* M-22-9 (Jan. 26, 2022).

National Institute of Standards and Technology, *Zero Trust Architecture,* NIST Special Publication 800-207 (Aug. 2020).

GAO SUPPORT:

GAO meets congressional information needs in several ways, including by providing oversight, insight, and foresight on science and technology issues. GAO staff are available to brief on completed bodies of work or specific reports and answer follow-up questions. GAO also provides targeted assistance on specific science and technology topics to support congressional oversight activities and provide advice on legislative proposals.

For more information, contact: Brian Bothwell at (202) 512-6888 or BothwellB@gao.gov and Jennifer R. Franks at (404) 679-1831 or FranksJ@gao.gov.

Staff Acknowledgments: Richard Hung (Assistant Director), Nicole Jarvis (Assistant Director), Mike Krafve, Di'Mond Spencer, Kevin R. Smith, Nora Adkins, Cheryl Harris, Matthew Metz, Joe Rando, and Ben Shouse.

This document is not an audit product and is subject to revision based on continued advances in science and technology. It contains information prepared by GAO to provide technical insight to legislative bodies or other external organizations. This document has been reviewed by Timothy M. Persons, PhD, the Chief Scientist of the U.S. Government Accountability Office.