IMPLEMENTING A ZERO TRUST ARCHITECTURE

The National Cybersecurity Center of Excellence (NCCoE) is addressing the challenge of implementing a zero trust architecture (ZTA) through collaborative efforts with industry and the information technology (IT) community, including cybersecurity solutions providers. This fact sheet provides an overview of the Implementing a Zero Trust Architecture project, including background, goal, potential benefits, and project collaborators.

BACKGROUND

The conventional security approach has focused on perimeter defenses. Once inside the network perimeter, users are "trusted" and often given broad access to many corporate resources. But malicious actors can come from inside or outside the perimeter, and several high-profile cyberattacks in recent years have undermined the case for the perimeter- based model. Moreover, the perimeter is becoming less relevant due to several factors, including the growth of cloud computing and mobility, and changes in the modern workforce.

Zero trust is a cybersecurity strategy that focuses on moving perimeter-based defenses from wide, static perimeters to narrow dynamic and risk-based access control for enterprise resources regardless of where they are located. Zero trust access control is based on a number of attributes such as identity and endpoint health.

CHALLENGE

The challenges to implementing a ZTA include:

- Leveraging existing investments and balancing priorities while making progress toward a ZTA via modernization initiatives
- Integrating various types of commercially available technologies of varying maturities, assessing capabilities, and identifying technology gaps to build a complete ZTA
- Concern that ZTA might negatively impact the operation of the environment or end-user experience
- Lack of common understanding of ZTA across the organization, gauging the organization's ZTA maturity, determining which ZTA approach is most suitable for the business, and developing an implementation plan

GOALS

The goal of this NCCoE project is to demonstrate several example ZTA solutions—applied to a conventional, general- purpose enterprise IT infrastructure—that are designed and deployed according to the concepts and tenets documented in NIST Special Publication (SP) 800-207, Zero Trust Architecture.

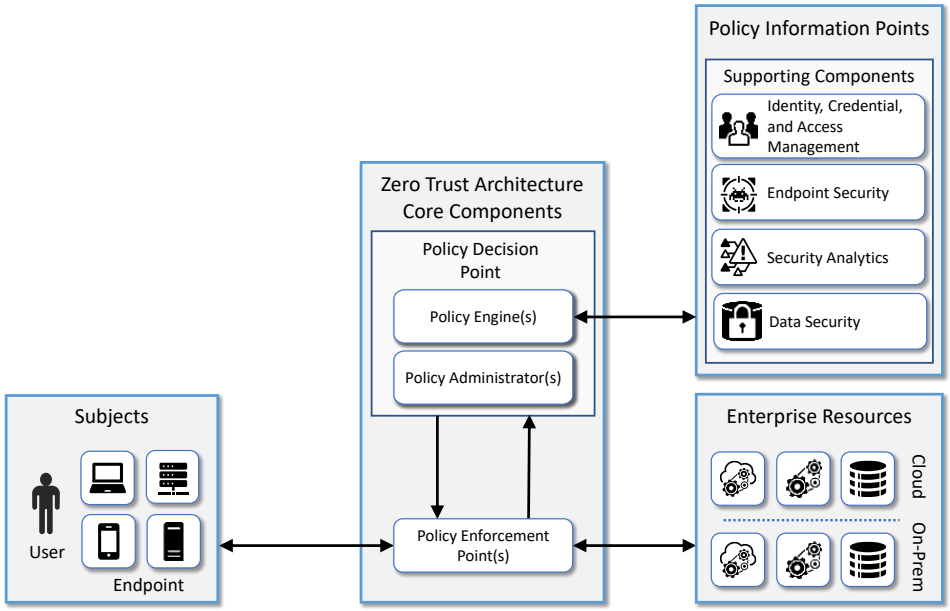
BENEFITS

The potential business benefits of the example solutions include:

- Support user access to resources regardless of user location or user device (managed or unmanaged)
- Protect business assets and processes regardless of their location (on-premises or cloud-based)
- Limit the insider threat (insiders—both users and non-person entities—are not automatically trusted)
- Limit breaches (reduce attackers' ability to move laterally and escalate privilege within the environment)
- Protect sensitive corporate information with data security solutions
- Improve visibility into the inventory of resources, what configurations and controls are implemented, all communications and their specific flows, and how resources are accessed and protected, and then use this understanding to formulate and enforce a useful and complete security policy
- Perform real-time and continuous monitoring and logging, and policy-driven, risk-based assessment and enforcement of resource access policy

HIGH-LEVEL ARCHITECTURE

A ZTA is designed for secure access to enterprise resources. Shown here is a high-level, notional architecture of the core components of a ZTA build for a typical IT enterprise and the functional components to support it. A detailed explanation of each component can be found within the practice guide and project description at https://www.nccoe.nist.gov/zerotrust.



TECHNOLOGY COLLABORATORS

The technology vendors participating in this project submitted their capabilities in response to an open call in the Federal Register. Companies with relevant security capabilities were invited to sign a Cooperative Research and Development Agreement with the National Institute of Standards and Technology (NIST), allowing them to participate in a consortium to build this example solution.

Appgate	F5	Lookout	PC Matic	Tenable
AWS	Forescout	Mandiant	Ping Identity	Trellix
Broadcom (VMWare)	Google Cloud	Microsoft	Radiant Logic	Zimperium
Cisco	IBM	Okta	SailPoint	Zscaler
DigiCert	Ivanti	Palo Alto Networks	Symantec by Broadcom	

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or the NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available.

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE

For more information about this project, visit:
https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture