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 vendors of cybersecurity solutions. As a private-public partnership, we are always seeking insights from businesses, the public, and technology vendors. If you are interested in contributing technology or expertise to this project, please email nccoe-zta-project@list.nist.gov.

BACKGROUND

Conventional network security 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 network, 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, mobility, and changes in the modern workforce.

Zero trust is a cybersecurity strategy that focuses on moving network defenses from wide, static network perimeters to focusing more narrowly on dynamic and risk-based access control to enterprise resources, regardless of where they are located.

CHALLENGE

The challenges to implementing a ZTA include:

- No single solution exists for zero trust, but instead requires integration of many different technologies of varying maturity
- Migrating an existing IT ecosystem, particularly one with legacy applications and systems, requires investments in time, resources, and technical ability to retool them to adhere to zero trust principles
- Security concerns, such as a compromise of the ZTA control plane, must be thoroughly assessed and vulnerabilities identified and mitigated

GOAL

The goal of this NCCoE project is to demonstrate one or more ZTAs—applied to a conventional, general purpose enterprise IT infrastructure—that are designed and deployed according to the concepts and tenets documented in NIST SP 800-207, Zero Trust Architecture.

BENEFITS

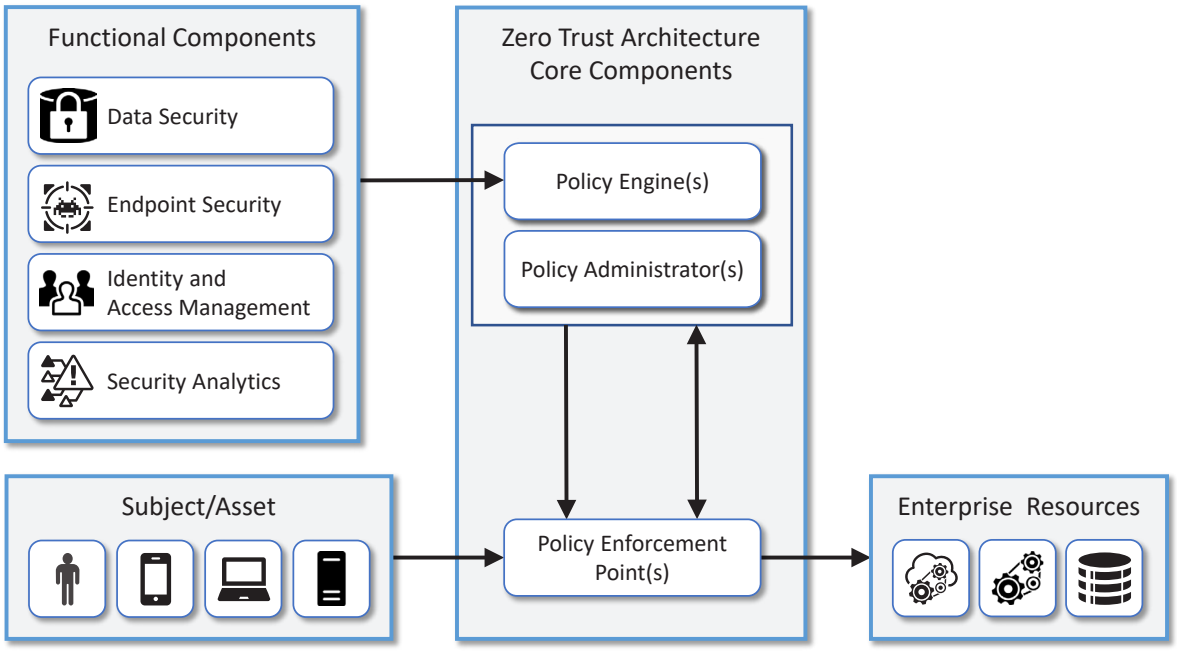
The potential business benefits of the solution explored by this project include:

- supporting telework initiatives by supplying secure and reliable access to your corporate resources anywhere, using any device
- improving visibility and governance over who, what, and how users are accessing your data and applications
- decreasing breach potential and data exfiltration by limiting lateral movement, thus decreasing organizational risk
- limiting the cost for recovery and mitigation if a breach occurs
- protecting the confidentiality of your company's sensitive data

LEARN MORE ABOUT NCCOE
https://www.nccoe.nist.gov.

CONTACT US
nccoe@nist.gov
301-975-0200

HIGH-LEVEL ARCHITECTURE



Core Components:

- The policy engine handles the ultimate decision to grant, deny, or revoke access to a resource for a given subject. The policy engine calculates the trust scores/confidence levels and ultimate access decisions.
- The policy administrator handles establishing/terminating the transaction between a subject and a resource. It generates any session-specific authentication and authentication token or credential used by a client to access an enterprise resource.
- The policy enforcement point handles enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource.

Functional Components:

- The data security component includes all the data access policies and rules that an enterprise develops to secure its information, and the means to protect data at rest and in transit.
- The endpoint security component encompasses the strategy, technology, and governance to protect endpoints (e.g., servers, desktops, mobile phones, IoT devices) from threats and attacks, as well as protect the enterprise from threats from managed and unmanaged devices.
- The identity and access management component includes the strategy, technology, and governance for creating, storing, and managing enterprise user (i.e., subject) accounts and identity records and their access to enterprise resources.
- The security analytics component encompasses all the threat intelligence feeds and traffic/activity monitoring for an IT enterprise. It gathers security and behavior analytics about the current state of enterprise assets and continuously monitors those assets to actively respond to threats or malicious activity. This information could feed the policy engine to help make dynamic access decisions.

DOWNLOAD THE PROJECT DESCRIPTION

This fact sheet provides a high-level overview of the work underway on zero trust cybersecurity. For more details, download the project description at https://www.nccoe.nist.gov/zerotrust

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights from businesses, the public, and technology vendors. If you are interested in contributing technology or expertise to this project, please email nccoe-zta-project@list.nist.gov.