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. This fact sheet provides an overview of the Implementing a Zero Trust Architecture project, including background, goals, potential benefits, and our project collaborators.

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

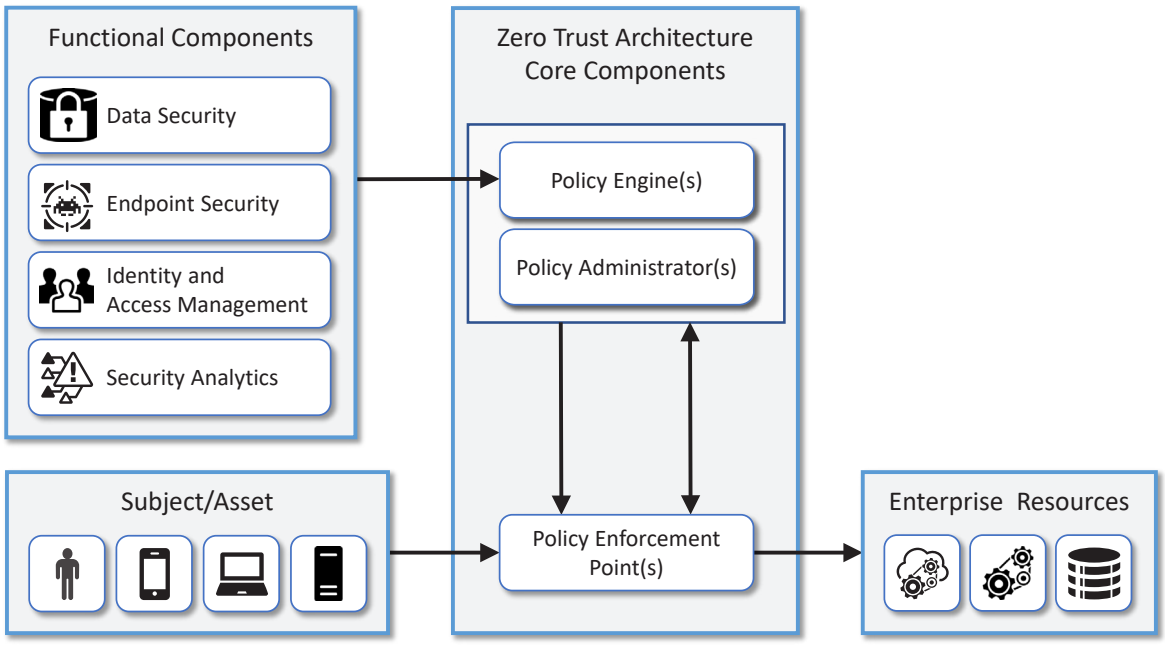
The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges.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

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

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

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 in the 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.

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 for the purpose.

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 have question about this project or would like to join the Zero Trust Architecture Community of Interest, please email nist-nccoe-zta@list.nist.gov.

July 2021