Executive Order (EO) on Improving the Nation's Cybersecurity

The Executive Order (EO) on Improving the Nation's Cybersecurity was signed in May and is now in the process of being implemented. The EO is broad ranging in scope, focusing on key areas of vulnerability, including:

- Removing barriers to threat information sharing between government and the private sector
- Modernizing and implementing stronger cybersecurity standards in the federal government (Zero Trust)
- Improving software supply chain security
- Establishing a cybersecurity safety review board
- Creating a standard playbook for responding to cyber incidents
- Improving detection of cybersecurity incidents on federal government networks
- Improving investigative and remediation capabilities

The principal aim of the EO is to enhance the cybersecurity of government departments and supply chains. However, expect this to have a trickle-down impact on all types of businesses within the private sector, both big and small.

Therefore, small businesses should make themselves aware of the requirements of the EO and determine if they are required to make any changes to remain in compliance, specifically with regards to their vendor relationships.

Executive Order (EO) on Improving the Nation's Cybersecurity

- Sec. 3. Modernizing Federal Government Cybersecurity.
  (a) To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, the Federal Government must take decisive steps to modernize its approach to cybersecurity, including by increasing the Federal Government's visibility into threats, while protecting privacy and civil liberties. The Federal Government must adopt security best practices; advance toward (NIST) Zero Trust Architecture…

- (k) the term "Zero Trust Architecture" means a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries.
- The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses.
  - In essence, a Zero Trust Architecture allows users full access but only to the bare minimum they need to perform their jobs. If a device is compromised, zero trust can ensure that the damage is contained.
  - The Zero Trust Architecture security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity.
  - Zero Trust Architecture embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting data in real-time within a dynamic threat environment.
  - This data-centric security model allows the concept of least-privileged access to be applied for every access decision, where the answers to the questions of who, what, when, where, and how are critical for appropriately allowing or denying access to resources based on the combination of sever.(several factors).

AN OFFERING IN THE BLUE CYBER SERIES:

Demystifying Zero Trust for Small Business

Scott Rose, NIST/CTL

25 January 2022

Blue Cyber Education Series

Demystifying Zero Trust for Small Business

Scott Rose, NIST/CTL

National Institute of Standards and Technology
U.S. Department of Commerce

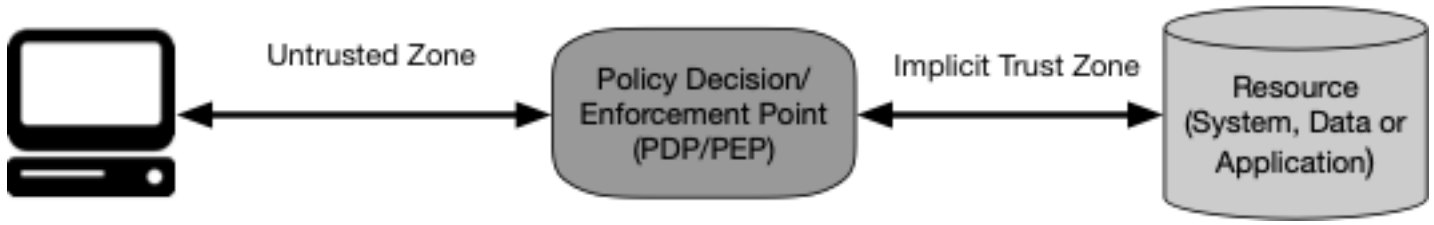
NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

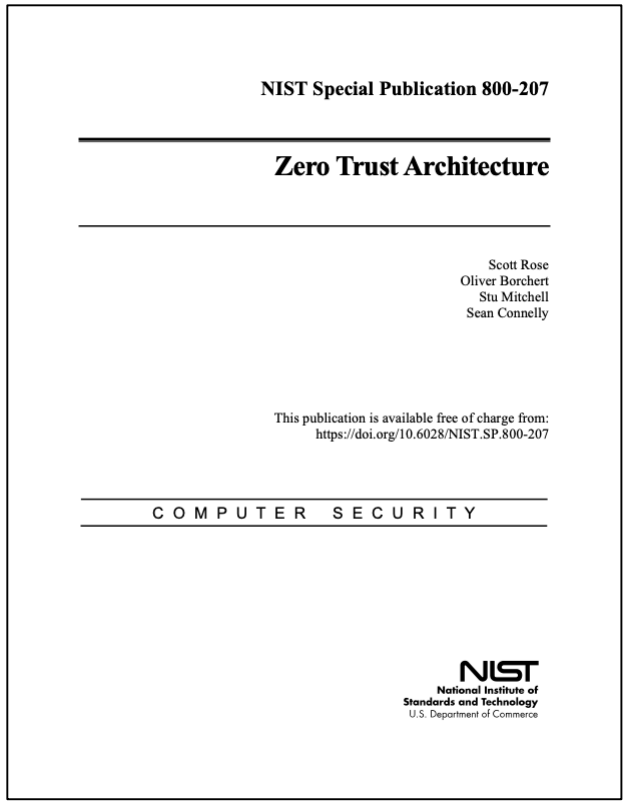
AGENDA

- Zero Trust Definition and Principles
- NIST Special Publication 800-207
- National Cybersecurity Center of Excellence (NCCoE) Zero Trust Architecture Project
- Discussion

WHAT IS ZERO TRUST?

- A way of designing IT systems and networks
- Not a single technology, standard or architecture
- NIST SP 800-207 *Zero Trust Architecture*
  - Conceptual Framework – *Not a standard!*





NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

ZERO TRUST PRINCIPLES

User Centric

- Dynamic and strictly enforced
- Granted per session

Device Centric

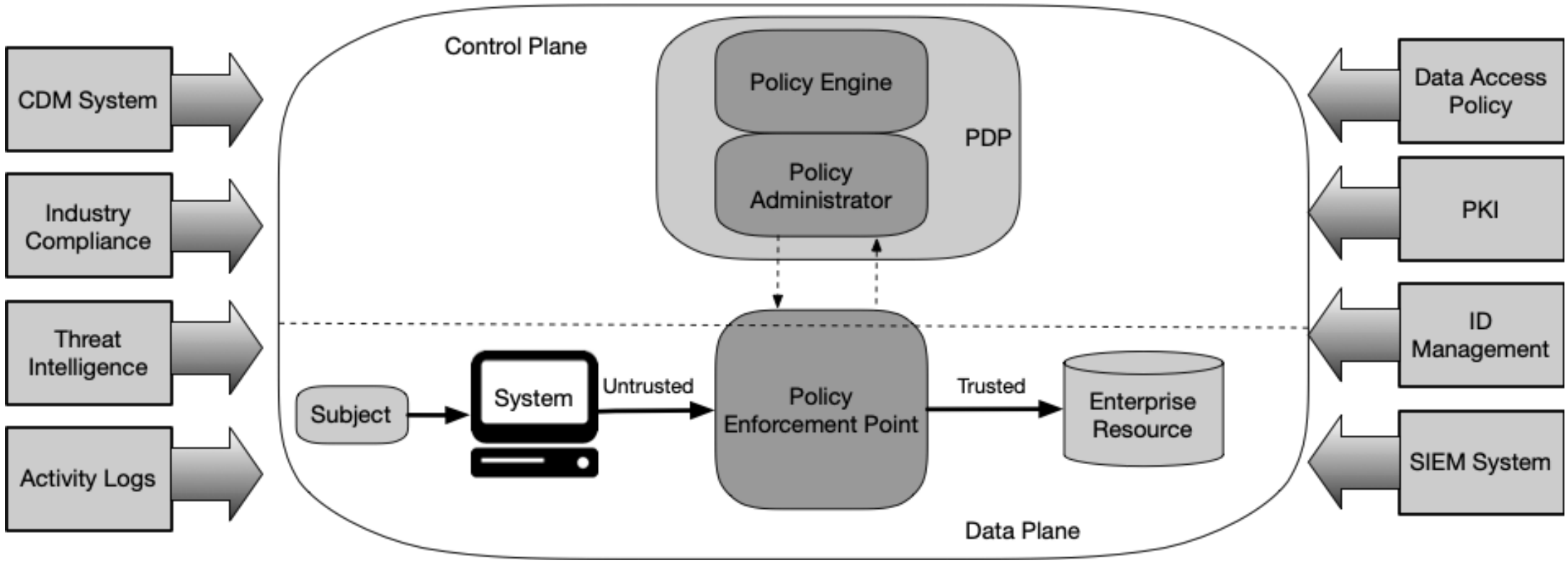
- All systems are considered resources
- Devices maintained in most secure state possible

Data/Network Centric

- All communication secured
- Logs (history) used to refine policy
- Default Deny, grant exceptions

See NIST SP 800-207 for full description: https://csrc.nist.gov/publications/detail/sp/800-207/final

ZERO TRUST ABSTRACT ARCHITECTURE



Control plane used to establish and manage connections between components.
Data plane is used by application traffic (i.e. the actual work).
Many of these roles exist in non-ZT architectures too!

ZTA IN PRACTICE

- Approaches
  - Enhanced identity governance
  - Microsegmentation
  - Software Defined Perimeters

Elements of all three may be present!

- Deployment Models
  - Agent/Gateway
  - Portals
  - App Sandboxes

There may be different models for different workflows!

SO WHERE TO START?

- First, know thyself…
- The (usual) easiest path start with enhanced ID governance
  - How many ID stores exist in the enterprise?
  - Separation of duties or least privilege
  - Playbooks (checklists) for employee onboarding/changes/separation
- Monitoring – you can’t protect what you can’t see
  - Employee endpoint and resources/services

ZERO TRUST AND COMPLIANCE

Zero Trust

- Internal focus, voluntary
- No controls, only principles, changes are self-initiated
- Implementation varies per enterprise

Compliance Regimes

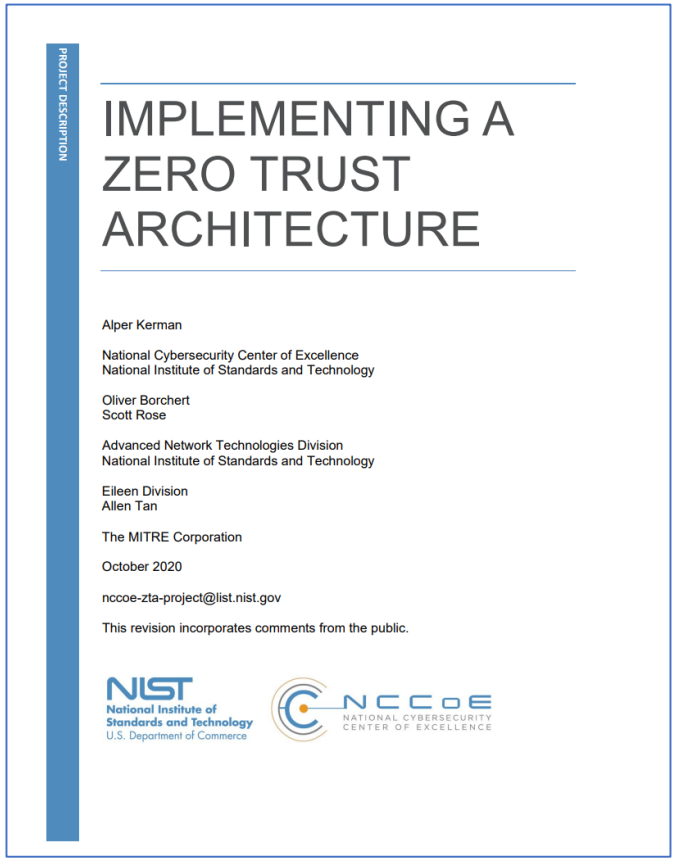
- External focus, mandated
- Control based and changes are announced
- Aims for consistency in outcomes

There is no reason for this to be either/or, zero trust can guide *how* a compliance regime is implemented and compliance controls could also be guided by zero trust principles.

ZTA IN THE LAB

- NCCoE Building Block Project
  Implementing a Zero Trust Architecture
  - Focused on evaluating access requests to resources
  - Kick-off July 2021, expected to run ~18 months
  - Final product: NIST SP 1800 series Practice Guide

https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture


PROJECT DESCRIPTION

IMPLEMENTING A ZERO TRUST ARCHITECTURE

Alper Kerman

National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Oliver Borchert
Scott Rose

Advanced Network Technologies Division
National Institute of Standards and Technology

Eileen Division
Allen Tan

The MITRE Corporation

October 2020

nccoe-zta-project@list.nist.gov

This revision incorporates comments from the public.

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Scott Rose, NIST

nccoe.nist.gov

@NISTcyber

ZERO TRUST TENETS

- All enterprise assets considered resources.
- All enterprise-owned assets are in their most secure state possible.
- All communication is done in a secure manner regardless of network location.
- Access to individual enterprise resources is granted on a per-connection basis.
- User authentication is dynamic and strictly enforced before access.
- All resource authentication and authorization is dynamic and strictly enforced before access is allowed.
- The enterprise collects as much information as possible about the current state of network infrastructure and communications and uses it to improve its security posture.

See NIST SP 800-207 for full description: https://csrc.nist.gov/publications/detail/sp/800-207/final

Any Questions?

- This briefing is not a substitute for reading the FAR and DFARS in your contract.
- This presentation and other presentations in the DAF CISO Blue Cyber Educational Series and be found on the DAF CISO webpage: https://www.safcn.af.mil/Organizations/CISO-Homepage/Small-Business-Cybersecurity-Information/
- Please provide questions, feedback or if you just want to talk about your cyber security /data protection questions to Kelley.Kiernan@us.af.mil
  - Daily Office Hours for answering/researching your questions about DAF Small Business cybersecurity and data protection!
  - Every Tuesday, dial in for the DAF CISO Small Business Cybersecurity Ask-Me-Anything. Register in advance for this Zoom Webinar: https://www.zoomgov.com/webinar/register/WN_CHsGAoWXTJSU5cDvEmQQHQ