Zero Trust 101

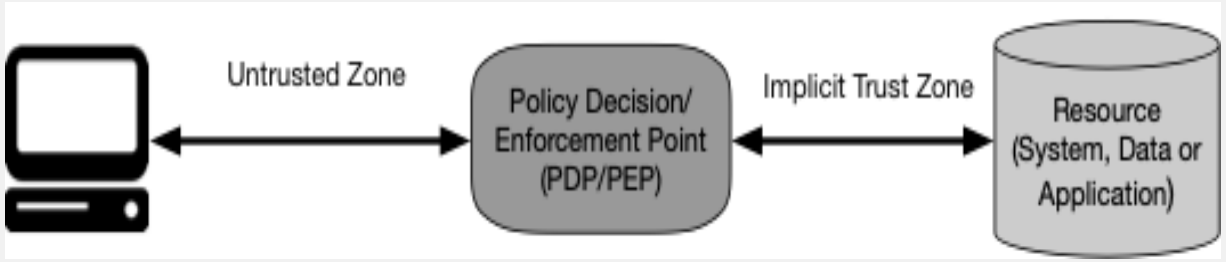
Scott Rose, NIST
scott.rose@nist.gov

A bit of background…

- Information Technology managers are facing an increasing number of cybersecurity breaches
- FCIOC recognized the need to develop guidance that enables the US government to adopt and transition to a Zero Trust Architecture
- Initiative and Steering Group was chartered in February 2019
- Partnering with NIST / NCCoE as the lead technical agency with involvement from a multi-agency project team

What is Zero Trust Architecture?

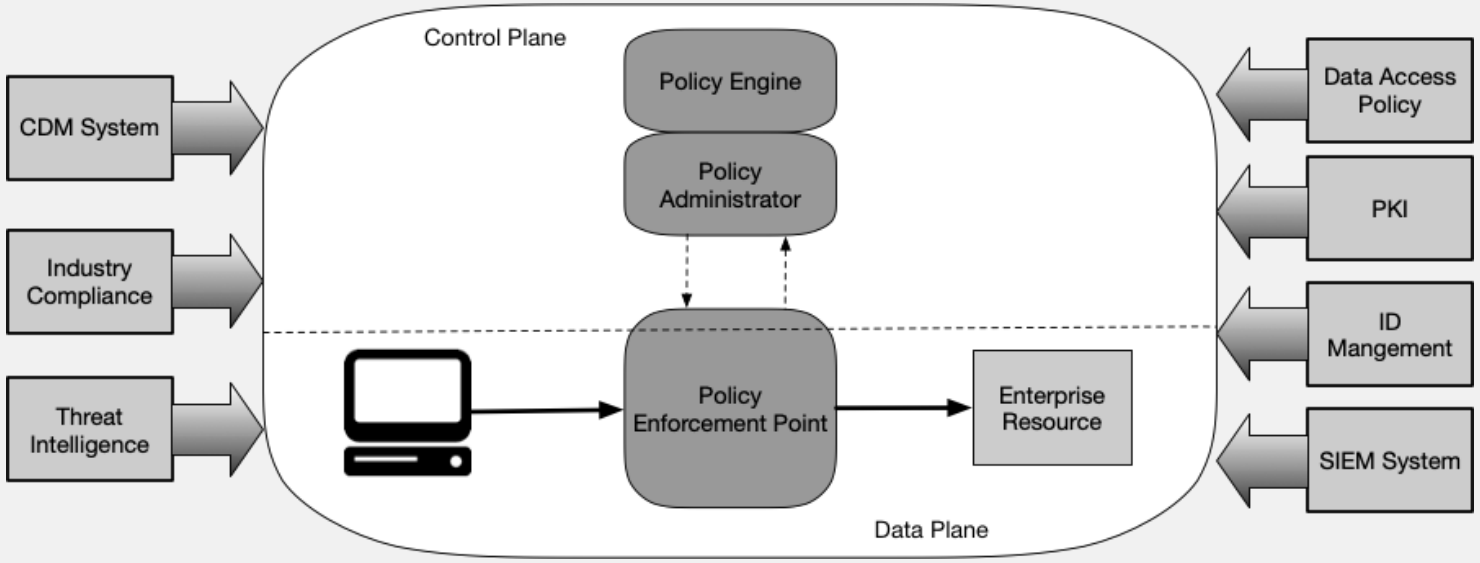
- First off, it's really Zero *Implicit* Trust
- A way of planning a network and work flow
- Moving where policy decisions are made closer to resources.
  - Network location does not grant trust!
  - Access is granted per access, no blanket authentication



Tenets of Zero Trust

- **All enterprise systems are considered resources.**
- **The enterprise ensures all owned systems 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.**
- **Access to resources is determined by policy, including the observable state of user, system, and environment.**

ZTA Logical Architecture



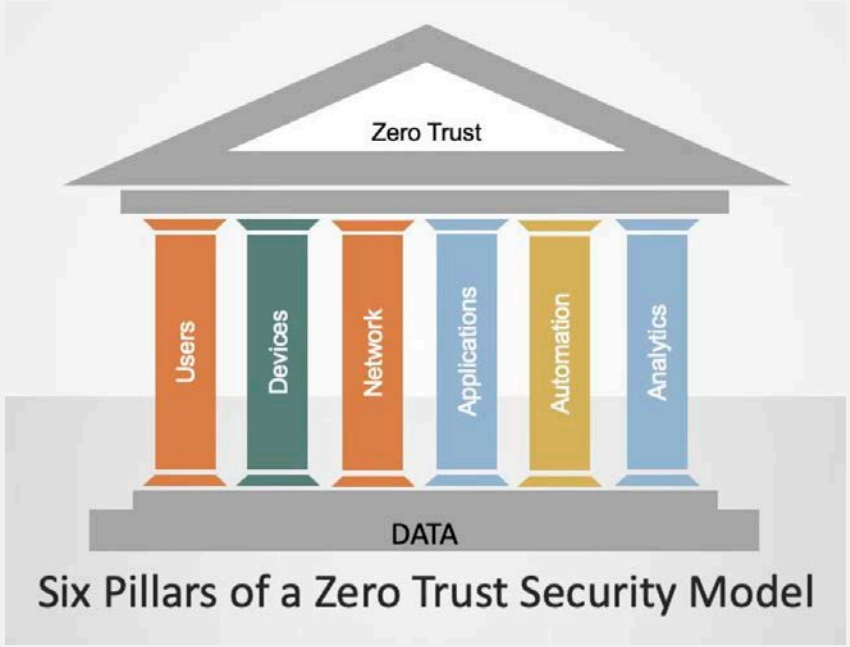
Two separate network planes:

- Control Plane: used by ZT components to set up and manage network
- Data Plane: used by applications for business processes

Roadmap to ZTA

- **Foundation: Identify resources (assets), users (accounts) and workflows**
- **Identify candidate workflow**
  - **Assets, user accounts involved**
  - **Develop access polices around workflow**
- **Deploy and monitor**
  - **Fine tune policies**

Sounds Familiar…



ACT-IAC's "Pillars of Zero Trust"

ZTA Depends on Many Current Federal Cybersecurity Initiatives

- NIST Cybersecurity & Risk Management Framework/FISMA – Planning
- FICAM – Identity Provisioning
- CDM – ID/Device/application management

- Smart Cloud and Data Center Optimization Initiative update (OMB M-19-19)
  - Cloud migration is main driver for ZTA

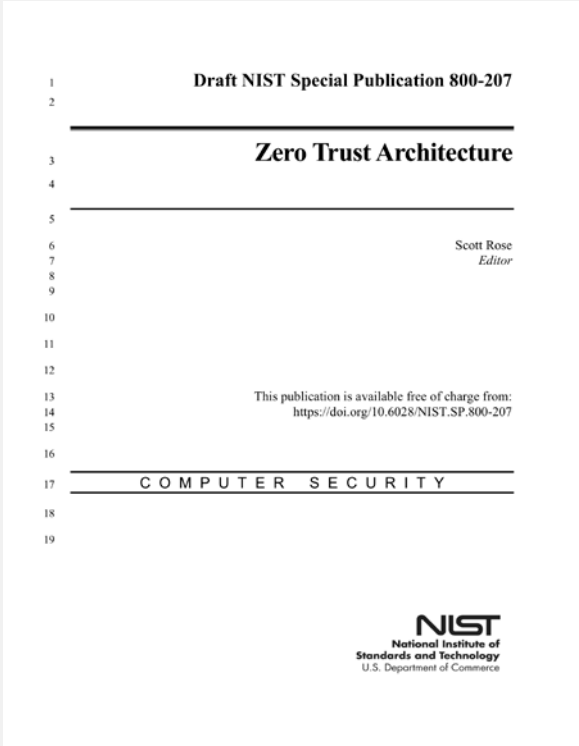
We've been moving to ZTA for years! (without knowing it)

Grey Areas – What's Missing?

- Standardized interfaces between components
  - Risk of vendor lock-in
- What does a successful attack look like?
  - Not enough experience
  - Attackers will eventually figure out how to approach ZTA enterprises
- How will user activity change?
  - Asking for authentication more frequently may impact user behavior
- What about server-server communication?
  - Can't do multifactor authentication between workloads/Automated Tech

Your Input is Welcome

- **NIST SP 800-207 Zero Trust Architecture**
  - **Public comment period ends 11/22/2019**
- **Future NCCoE Demonstration Project**
  - **Winter 2019/Spring 2020**
- **Contact Information**
  - **Alper Kerman (NIST/NCCoE)** – Zero Trust Technical Lead; Alper.Kerman@nist.gov
  - **Scott Rose (NIST)** – Zero-Trust Architecture Sub-team lead; Scott.Rose@nist.gov
  - **Oliver Borchert (NIST)** – Zero-Trust Technology Sub-team Lead; Oliver.Borchert@nist.gov



Draft NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Editor

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

Questions & Feedback