Zero Trust Architecture Project

Alper Kerman

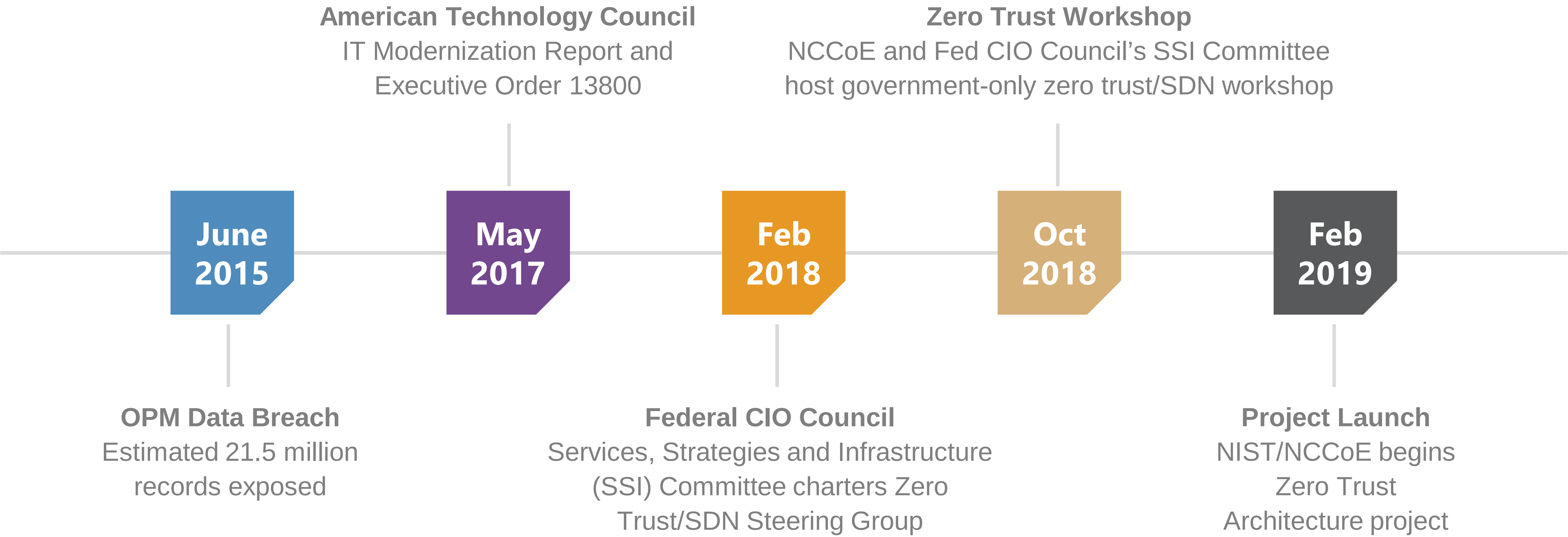
Security Engineer, Project Manager

NIST National Cybersecurity Center of Excellence

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Historical Context



June 2015

OPM Data Breach
Estimated 21.5 million records exposed

May 2017

American Technology Council
IT Modernization Report and Executive Order 13800

Feb 2018

Federal CIO Council
Services, Strategies and Infrastructure (SSI) Committee charters Zero Trust/SDN Steering Group

Oct 2018

Zero Trust Workshop
NCCoE and Fed CIO Council's SSI Committee host government-only zero trust/SDN workshop

Feb 2019

Project Launch
NIST/NCCoE begins Zero Trust Architecture project

Mission: "Adoption of zero trust principles, approaches, and relevant technology to secure Federal information systems"

Project Background, Activities and Scope

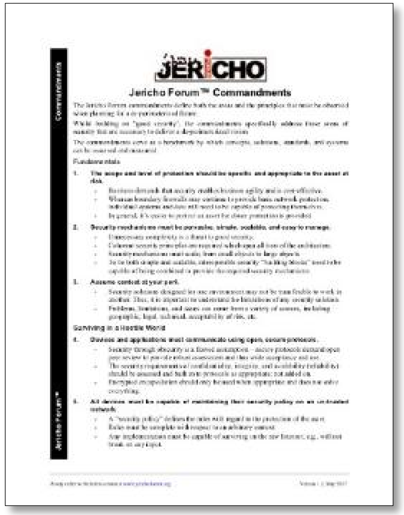
- Federal Initiative for adoption of Zero Trust principles and approaches for securing federal information systems and networks.
- Runs under the authority of Federal CIO Council and NIST is a partner in that effort, leading the research and technical work with volunteers from other agencies.
- Project launch: February, 2019

Project Deliverable

A NIST Special Publication providing general guidance on the adoption of zero trust architectures in federal information systems, including discovered gaps in the current technology, standards, and technical guidance areas

The Evolution of Zero Trust

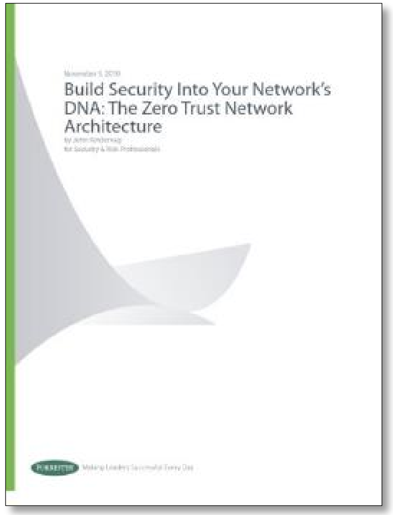
2005: Jericho Forum
De-perimeterization


JERICHO

Jericho Forum™ Commandments

Assume breach and design as if there is no perimeter

2010: Forrester coins "Zero Trust"


Build Security Into Your Network's DNA: The Zero Trust Network Architecture

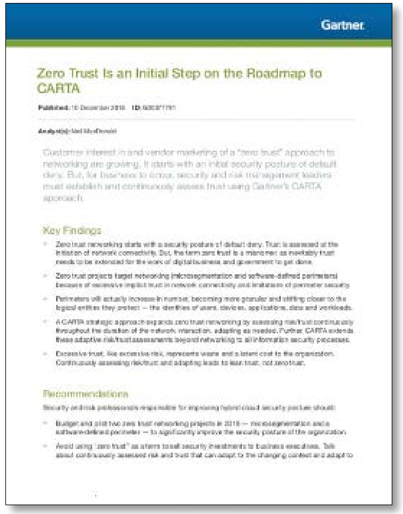
By default, don't trust anything, starting with the network

2014: Google releases "BeyondCorp" papers

BeyondCorp
A New Approach to Enterprise Security

Build trustworthiness and continuously verify

2018: Gartner coins "Lean Trust"


Gartner

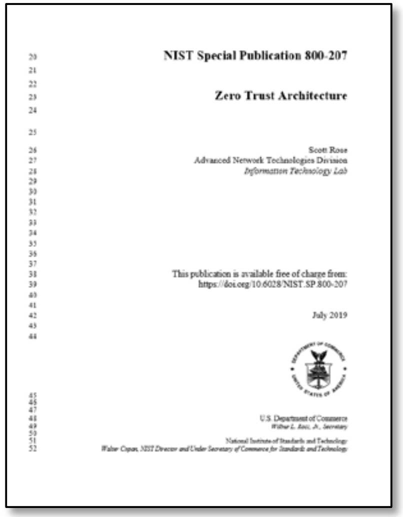
Zero Trust Is an Initial Step on the Roadmap to CARTA

Key Findings

Recommendations

Get just enough risk-optimized trust for the current context

2019: NIST releases draft SP 800-207


NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Advanced Network Technologies Division
Information Technology Lab

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

July 2019

Pull it all together into an architecture with context for USG

Project Deliverable › A NIST Special Pub

NIST Special Publication 800-207, *Zero Trust Architecture*

Scott Rose (Editor)

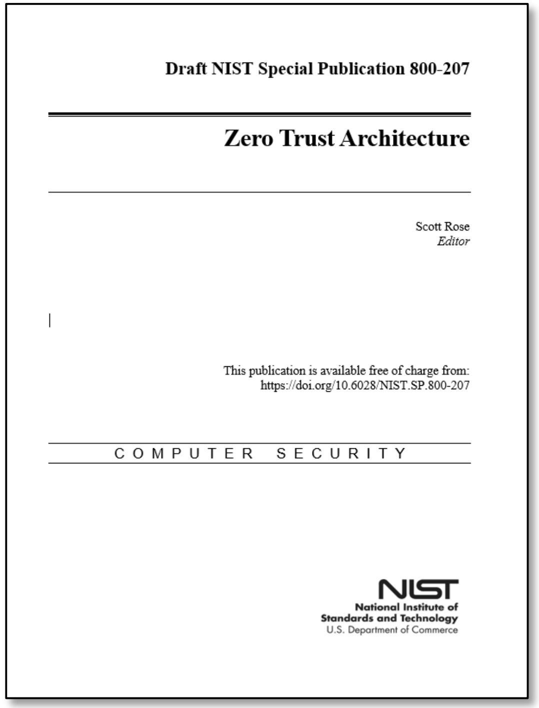
Computer Scientist, Advanced Network Technologies Division
NIST Information Technology Lab

Product of a multi-agency collaboration overseen by the Federal CIO Council

- Describes ZTA strategies for enterprise network architects
- Provides technology neutral set of terms, definitions, and logical components of network infrastructure using a ZTA strategy
- Provides insight into ZTA for civilian unclassified systems
- Provides a roadmap to migrate and deploy ZTA concepts to an enterprise network
- Is not intended to be a single deployment plan for ZTA

Status and availability for public review

- Draft publication, released for public comment period on September 23rd, 2019 and closed on November 22nd, 2019.
- Received comments from over 70 individuals, federal agencies, DoD, industry groups, vendors, and companies.
- https://csrc.nist.gov/News/2019/zero-trust-architecture-draft-sp-800-207



Draft NIST Special Publication 800-207

Zero Trust Architecture

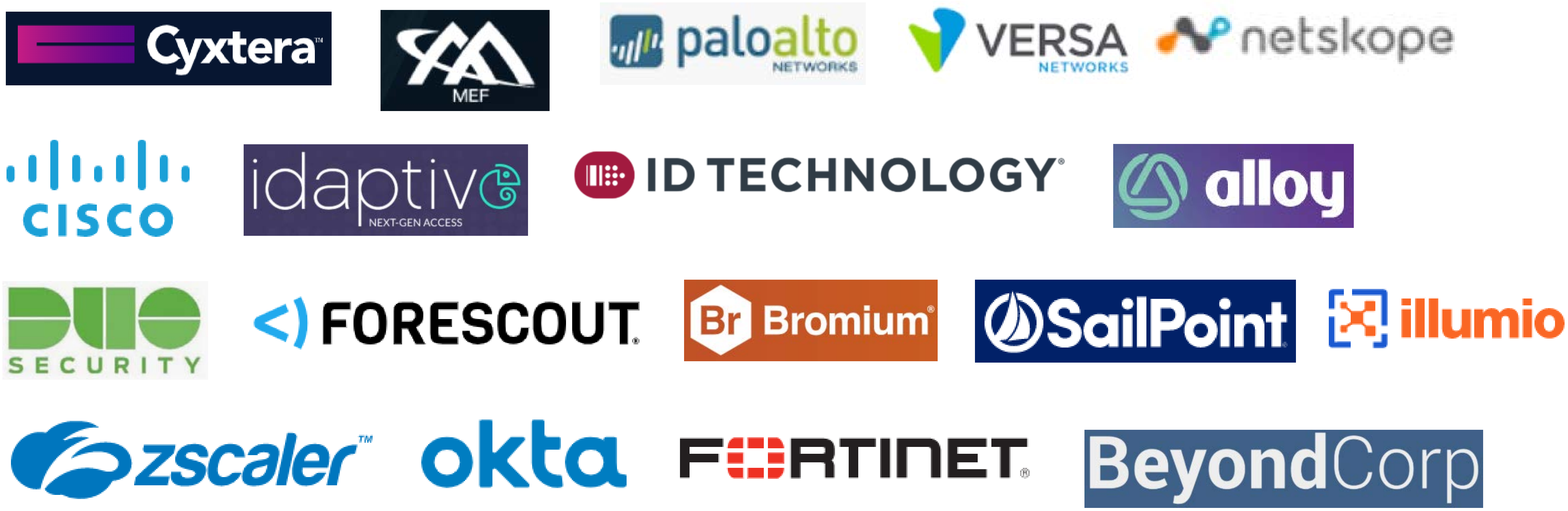
Scott Rose
Editor

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

Zero Trust Technology Demos



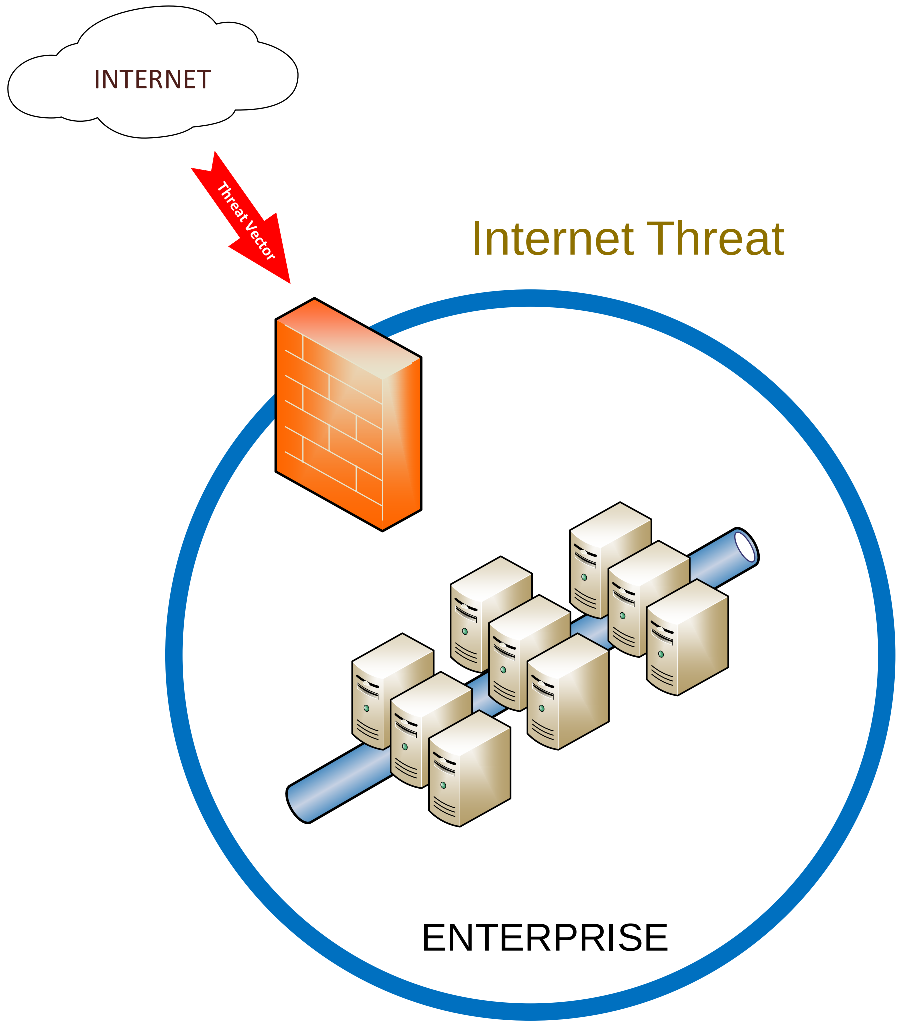
Project Deliverable GAP Analysis

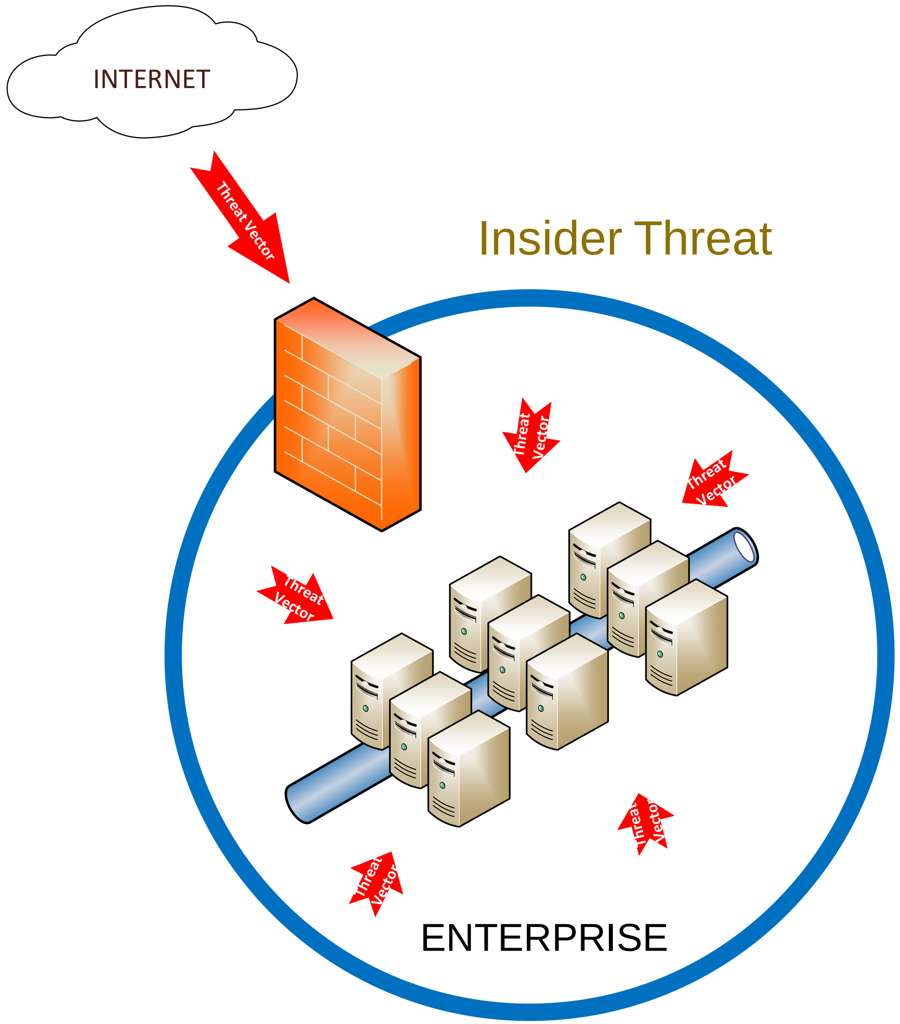
Lab Work – Zero Trust Testbed

- Provision a lab at NCCoE ✓
- Build base level network infrastructure ✓
- Build use case scenarios (1st one built ✓)
- Integrate Zero Trust Technologies
- Conduct technology capabilities tests

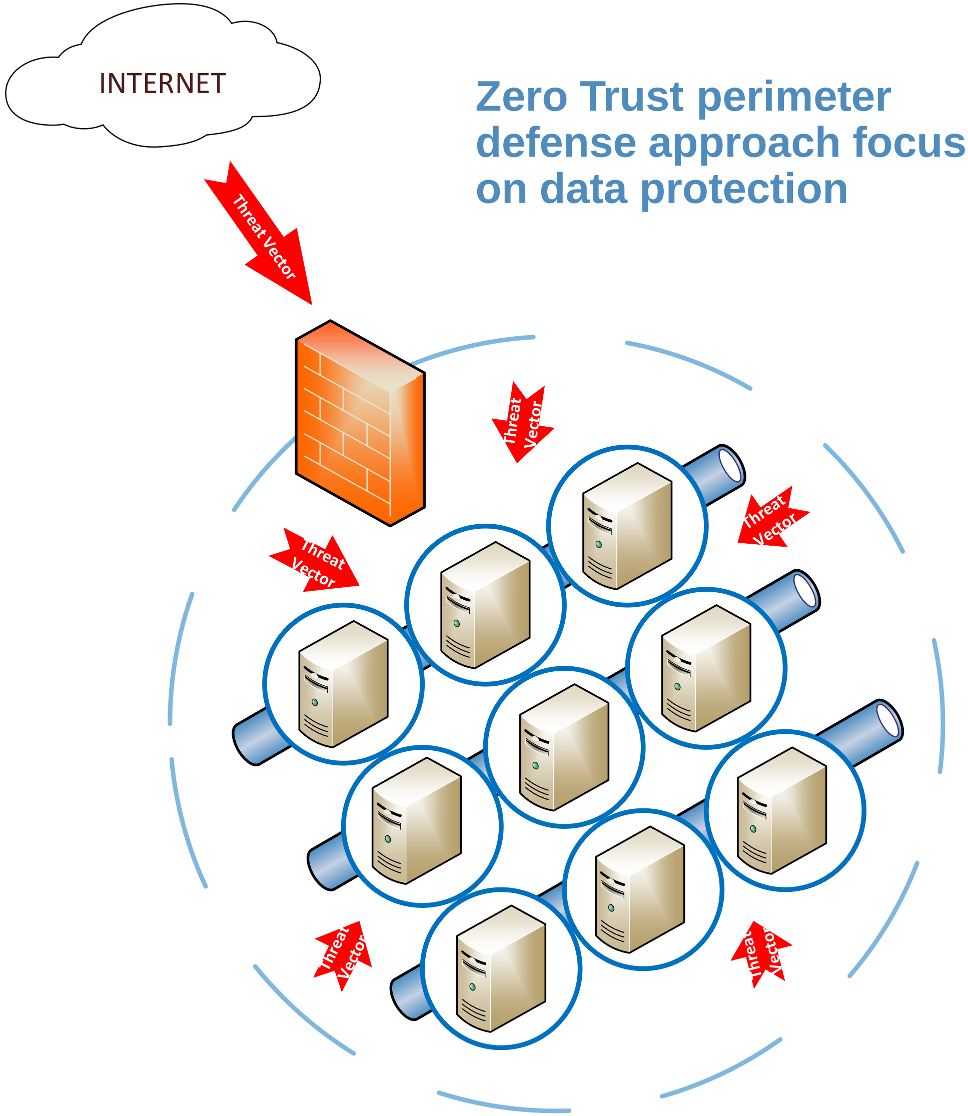
Zero Trust

Traditional Single Perimeter Defense





Zero Trust



Zero Trust perimeter defense approach focuses on data protection

NO IMPLICIT TRUST!

NEVER TRUST, ALWAYS VERIFY!

Tenets of Zero Trust

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-connection basis.
4. Access to resources is determined by dynamic policy, including the observable state of user identity and the requesting system, and may include other behavioral attributes.
5. The enterprise ensures all owned and associated systems are in the most secure state possible and monitors systems to ensure that they remain in the most secure state possible.
6. All resource authentication is dynamic and strictly enforced before authorized access is allowed.

A Zero Trust View of a Network

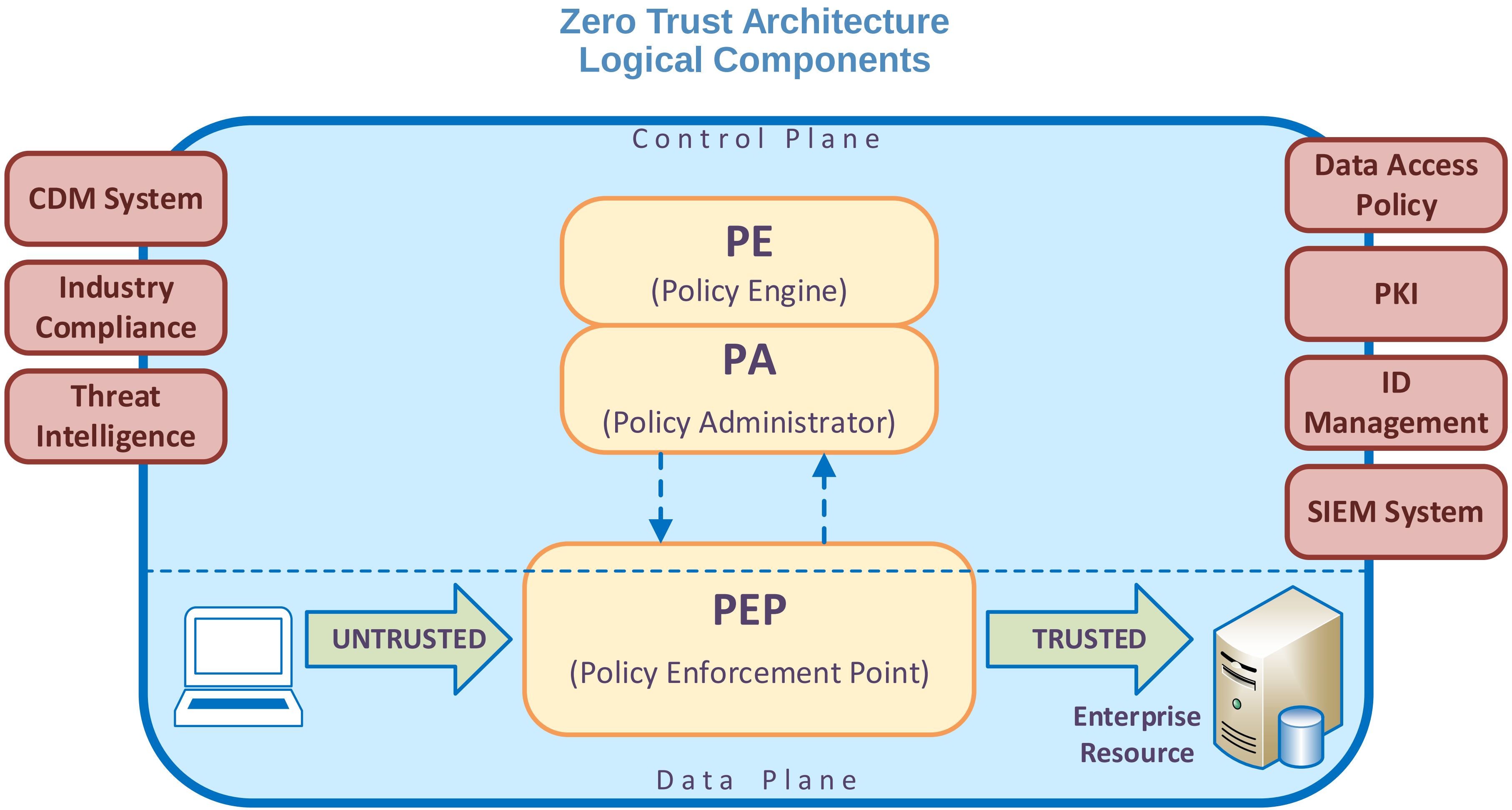
- **Assumptions for Enterprise-Owned Network Infrastructure**

1. The entire enterprise private network is not considered an implicit trust zone.
2. Devices on the network may not be owned or configurable by the enterprise.
3. No device is inherently trusted.

- **Assumptions for Non-Enterprise-Owned Network Infrastructure**

1. Not all enterprise resources are on enterprise-owned infrastructure.
2. Remote enterprise users cannot trust the local network connection.

Zero Trust Architecture

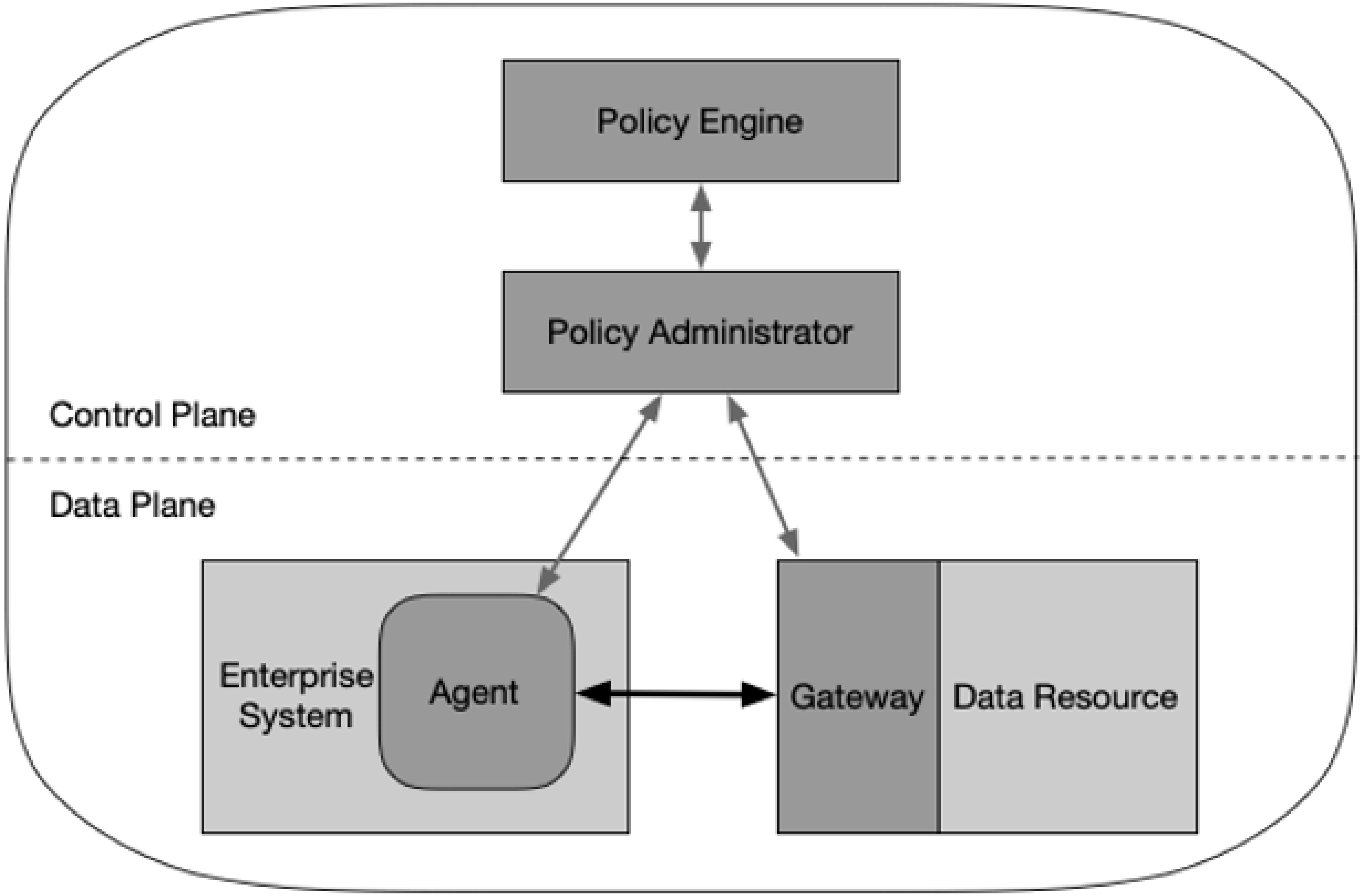


Zero Trust Architecture

- **Continuous Diagnostics and Mitigation (CDM) System(s):** This system(s) gathers information about the enterprise system's current state and applies updates to configuration and software components.
- **Industry Compliance System:** This system ensures that the enterprise remains compliant with any regulatory regime they may fall under (e.g. FISMA, HIPAA, PCI DSS, etc.).
- **Threat Intelligence Feed(s):** This system provides information from outside sources that help the Policy Engine make access decisions.
- **Data Access Policies:** This is the set of attributes, rules, and policies about access to enterprise resources. This set of rules could be encoded in or dynamically generated by the Policy Engine.
- **Enterprise Public Key Infrastructure (PKI):** This system is responsible for generating and logging certificates issued by the enterprise to resources, subjects, and applications.
- **ID Management System:** This system is responsible for creating, storing, and managing enterprise user accounts and identity records.
- **Network and System Activity Logs:** The enterprise system that aggregates system logs, network traffic, resource access actions, and other events that provide real time (or near real time) feedback on the security posture of enterprise information systems.
- **Security Information and Event Management (SIEM) System:** This system collects security centric information for later analysis. This data is then used to refine policies and warn of possible attacks against enterprise systems.

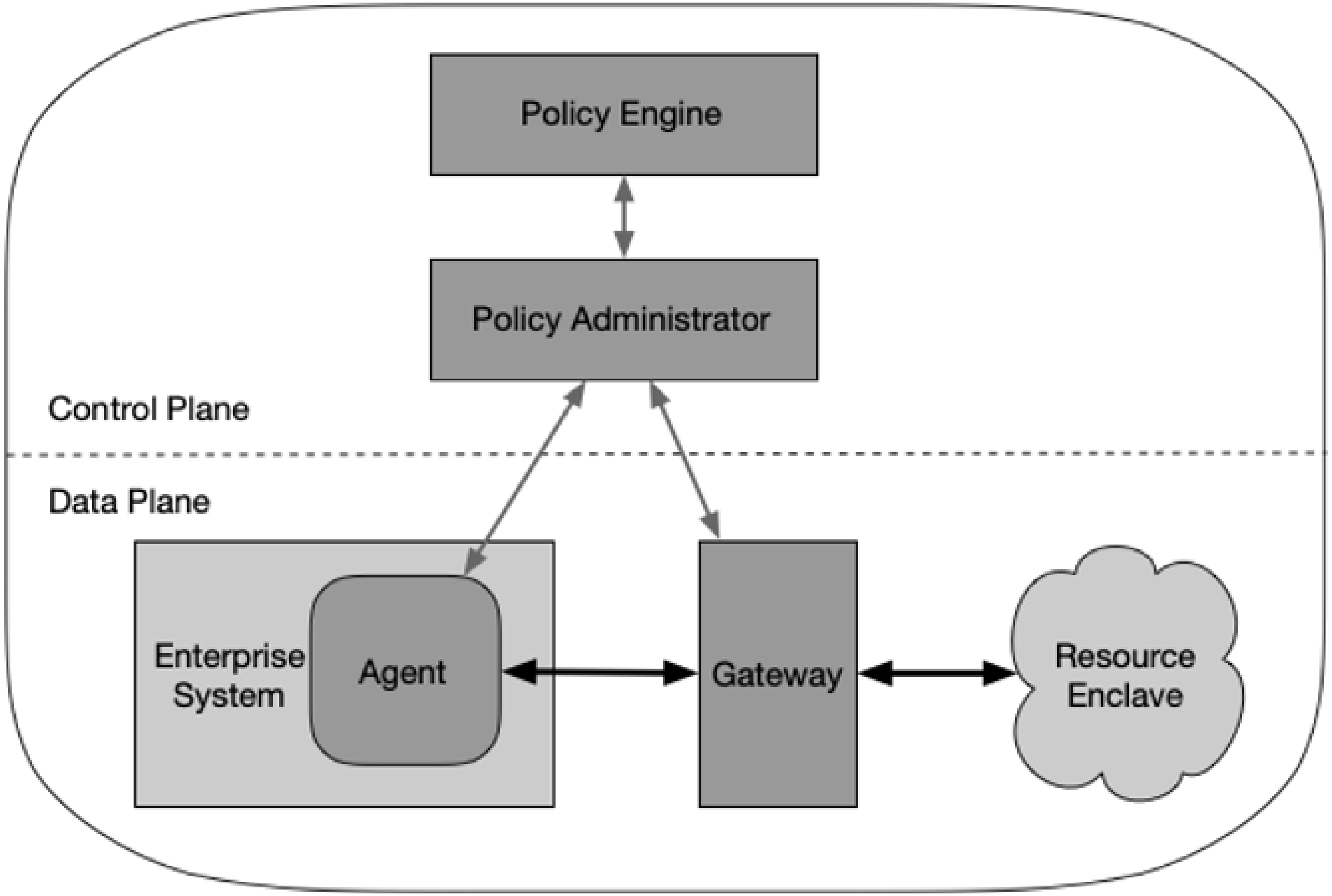
Logical Components Deployment Models

Device Agent/Gateway Model



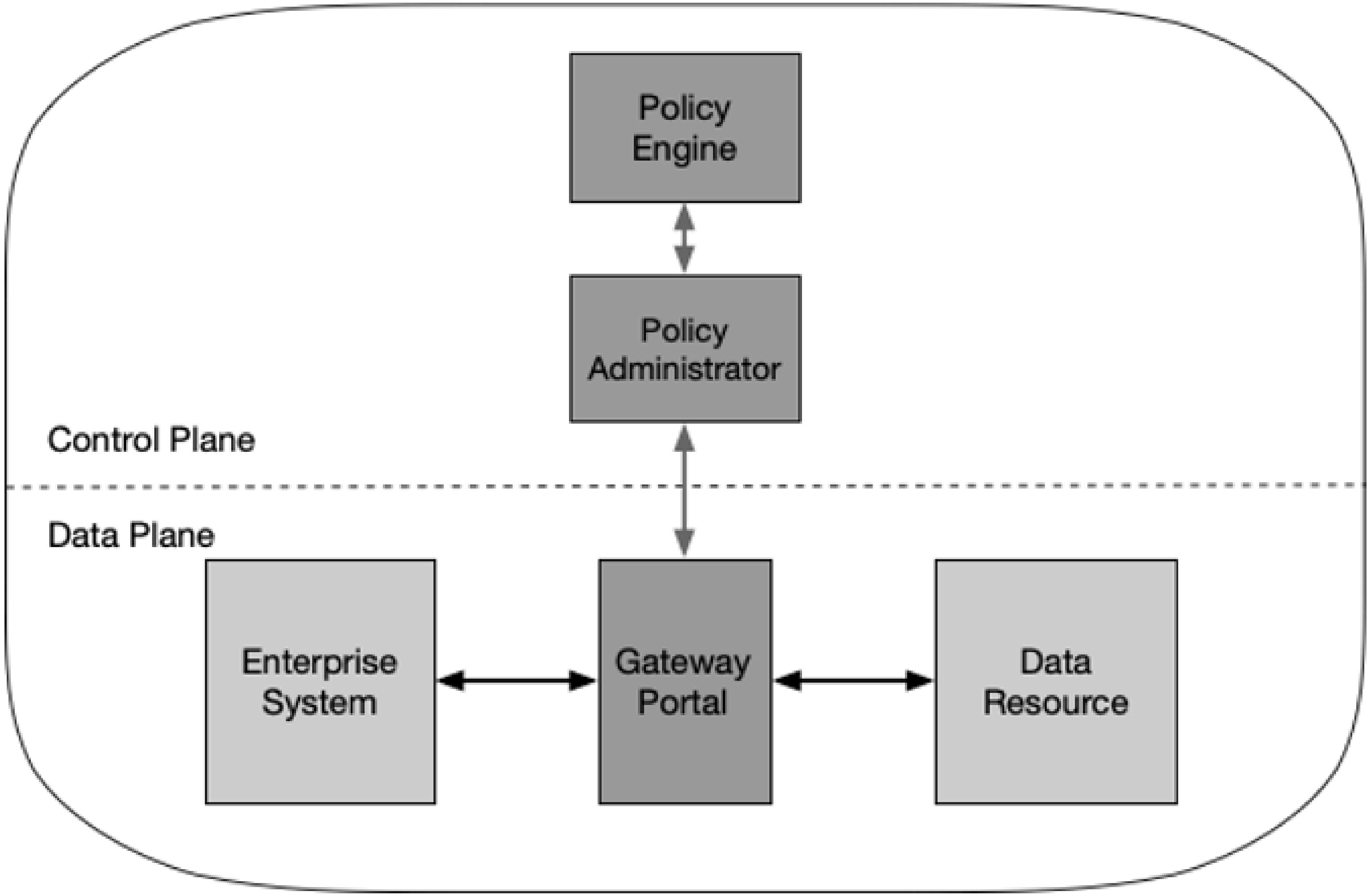
Logical Components Deployment Models

Enclave Gateway Model



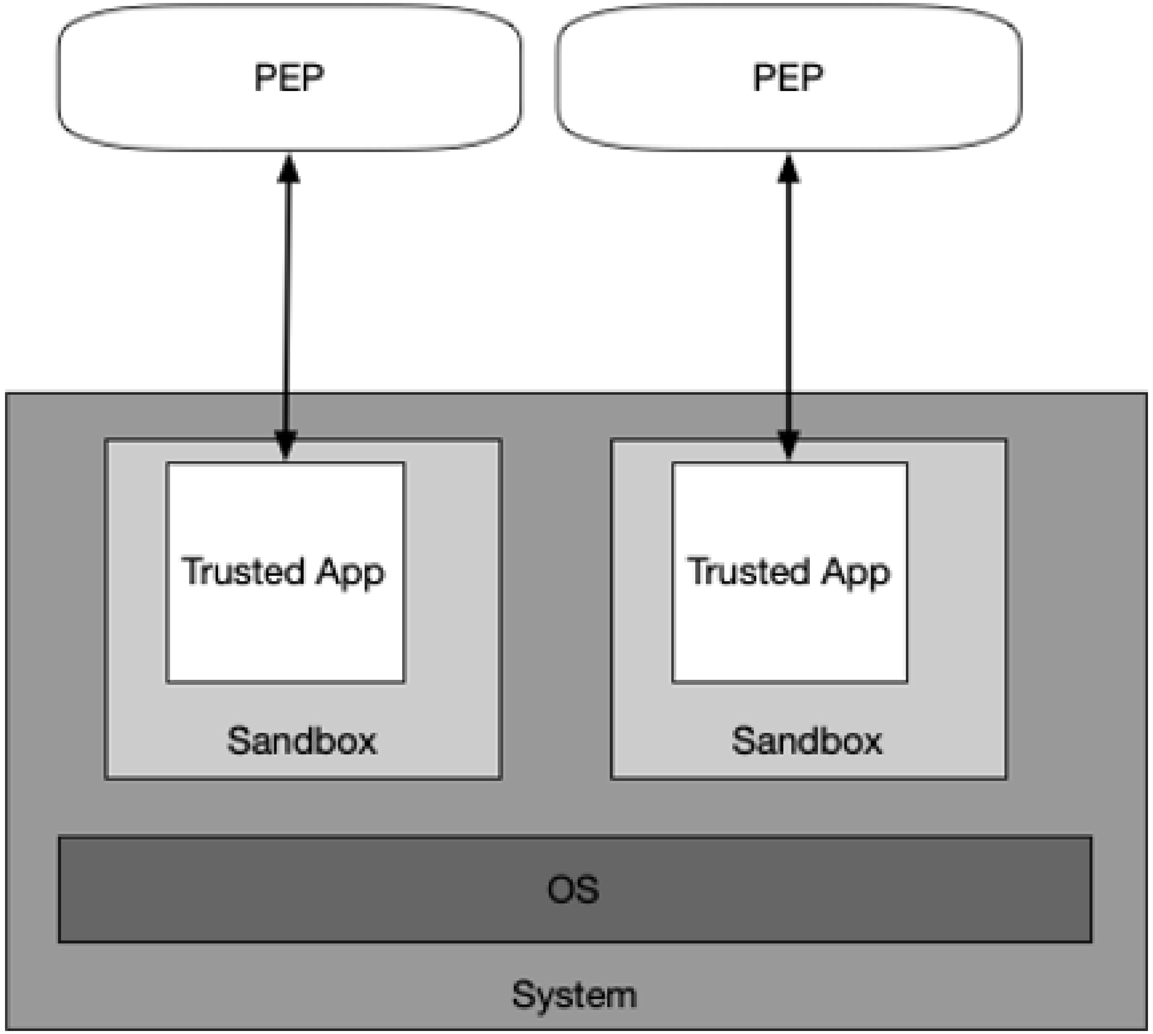
Logical Components Deployment Models

Resource Portal Model



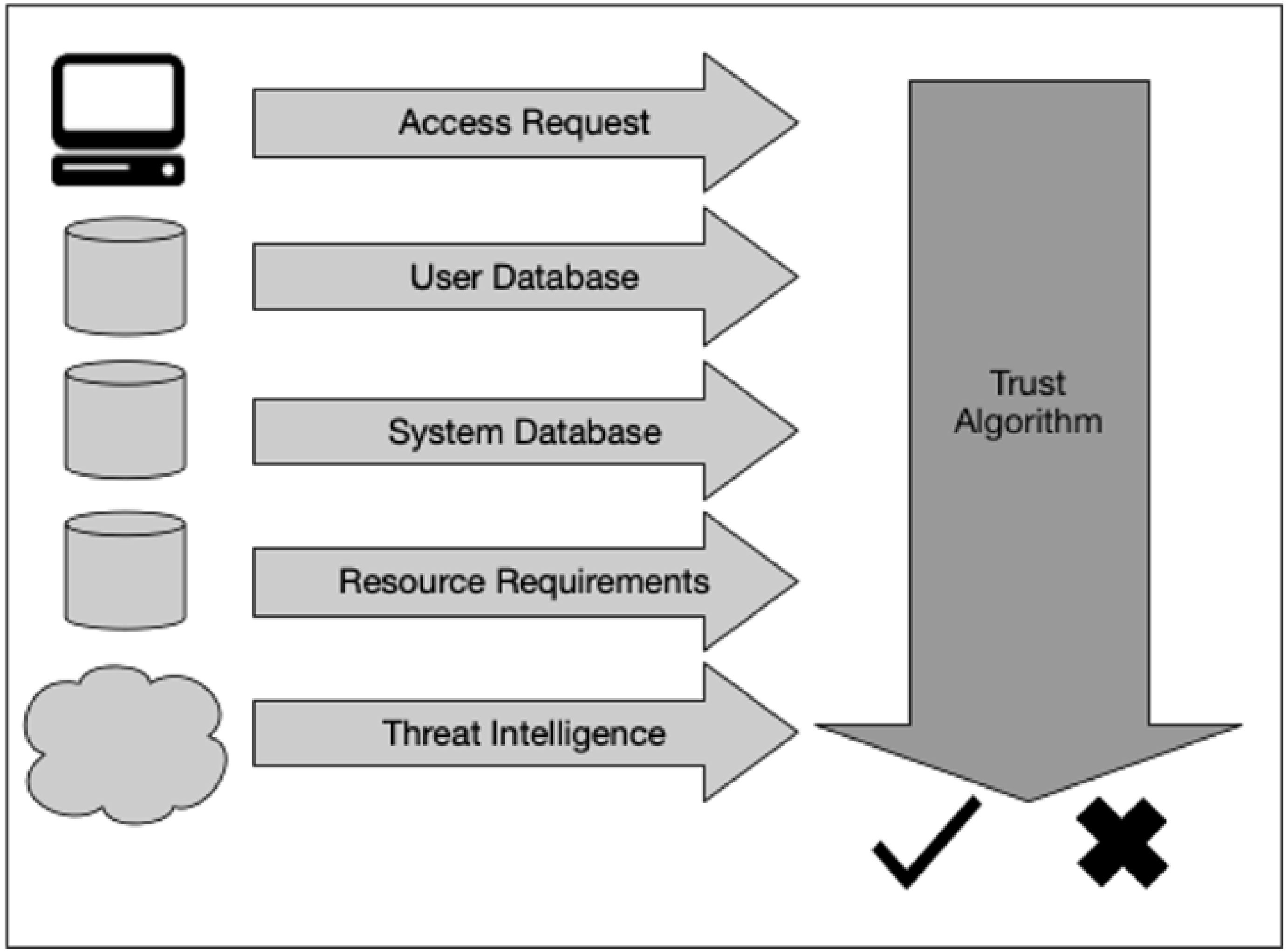
Logical Components Deployment Models

Application Sandboxes



Trust Algorithm

Trust Algorithm Input

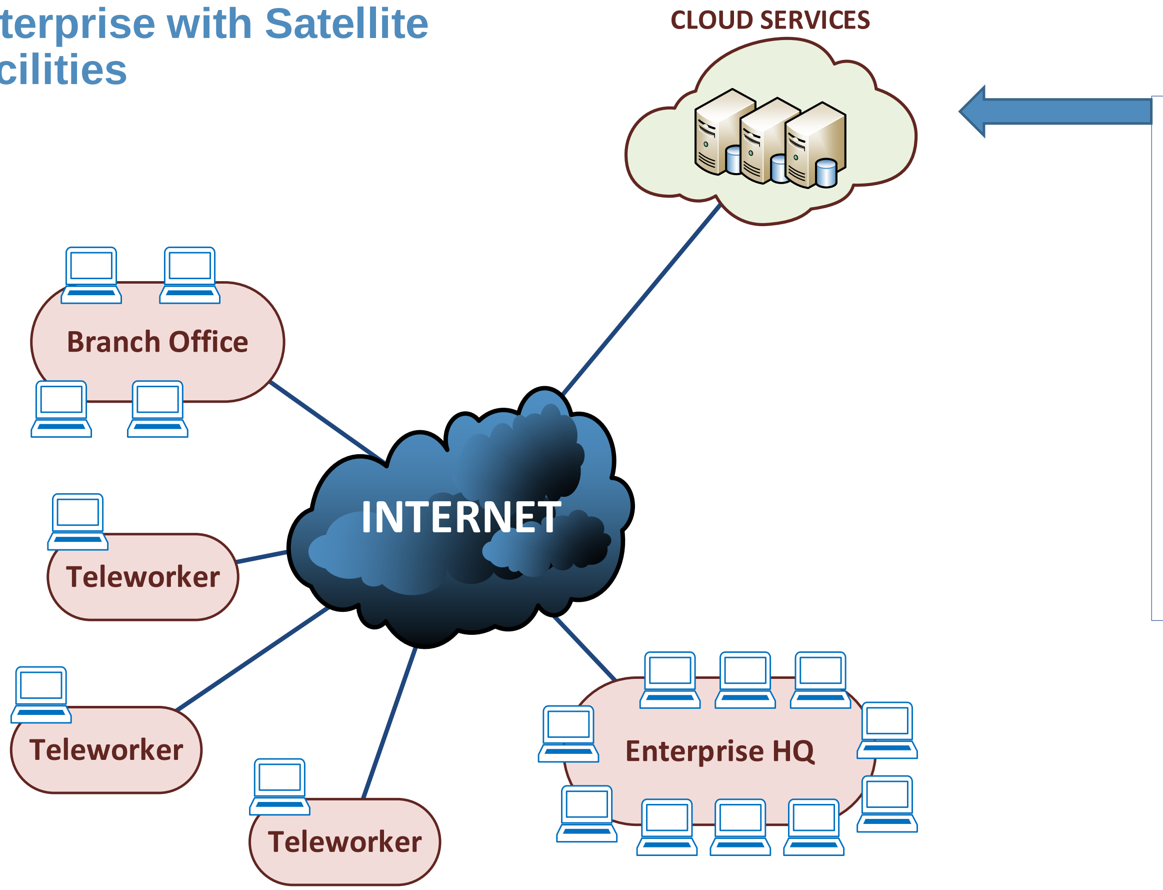


Variations

- Criteria vs Score based
- Singular vs Contextual

Zero Trust Architecture – Example Deployment Scenario

Enterprise with Satellite Facilities

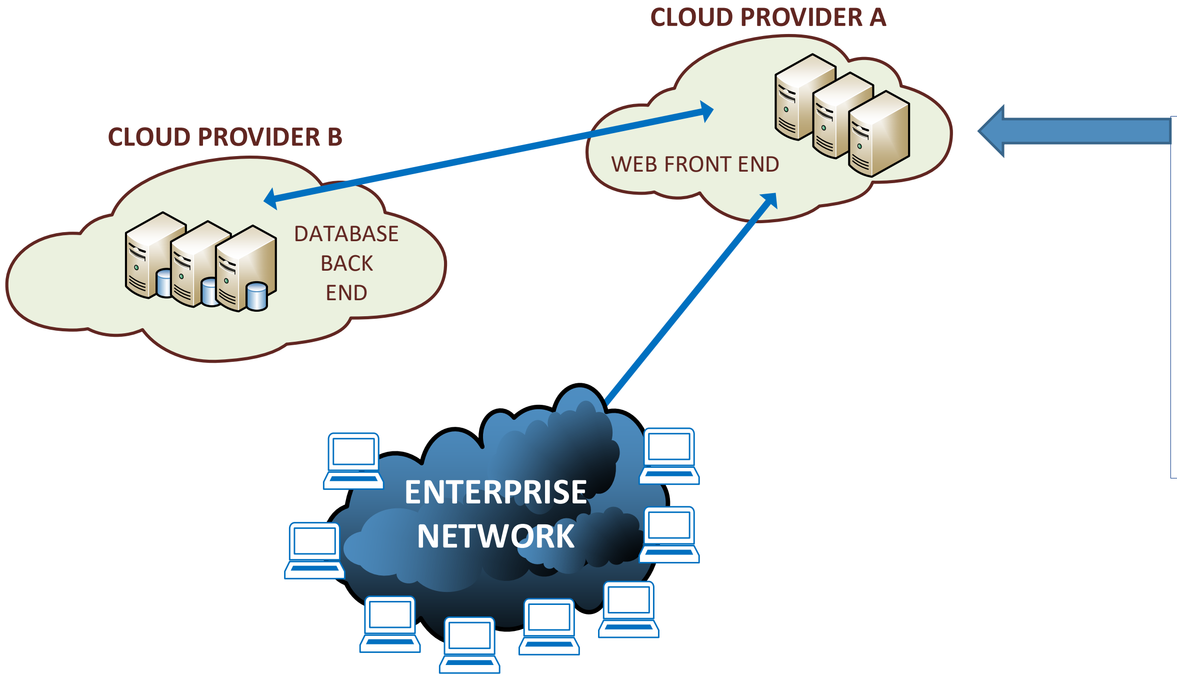


*** In this use case, the **PE/PA** is best hosted as a cloud service, with end systems having a connection agent or accessing a resource portal.

It may not be most responsive to have the PE and/or PA hosted on the enterprise local network, as remote offices and teleworkers must send all traffic back to the enterprise network in order to reach cloud services.

Zero Trust Architecture – Example Deployment Scenario

Multi-Cloud Enterprise



*** In this use case, the zero trust approach is to place **PEPs** at the access points of each application and data sources.

The **PE** and **PA** may be a service located in either cloud, or even a third cloud provider.

Zero Trust Architecture and Existing Guidance

ZTA complements existing Federal guidance and does not replace it

Many existing Federal cybersecurity programs are policy components of a ZTA strategy

- NIST Risk Management Framework (RMF)
- DHS Trusted Internet Connection (TIC), EINSTEIN/ National Cybersecurity Protection System
- DHS Continuous Diagnostics and Mitigation (CDM)
- Federal Identity, Credential, and Access Management (FICAM)
- Cloud Smart and Federal Data Strategy

Zero Trust Architecture Technical Exchange Meeting

Highlights

- Took place on Nov 13th, 14th at NIST/NCCoE
- Organized by NCCoE and FCIO Council
- Highly successful and impactful event where over 150 participants were in attendance (Feds, DoD and industry)
- Various states in their own zero trust journey
- Good mix of presentations from practitioners in the trenches and vendor presentations with Q&A discussions that were informative, influential, and well received.
- “*When will be the next one?*”

Zero Trust Architecture Technical Exchange Meeting

Outcomes – Possible areas for further research and work

- Define a common zero trust lexicon/taxonomy.
- Centralize, orchestrate and communicate activities, results, and lessons learned from Zero Trust pilots and implementations across the federal government.
- Assess challenges associated with TLS and end-to-end encryption and address the need for when to break and inspect traffic.
- Map the Zero Trust Architecture document to Risk Management Framework (RMF) / Cybersecurity Framework (CSF).
- Develop a Zero Trust Maturity model by defining metrics, criteria and standards to use for measuring maturity.
- Define additional use cases and impact on ZT tenets and implementation. Examples include: 5G networks; handling BOTS; IoT and protecting networks and data from IoT.
- Compare the NIST 800-53 security controls against the NIST SP 800-207 ZT framework to identify which controls from 800-53 would be addressed if one were to perfectly institute a ZT reference architecture per 800-207. Identify to what extent 800-53 could be “tailored down” leaving a much smaller set of security controls left unaddressed.
- Define standards for APIs to provide more seamless integration between vendor products; and ease transition between vendor products. Addressing the challenge of vendor lock-in.

NCCoE ZTA Demonstration Project

- Decide on a solution (may be an identity based ZTA?) **TBD**
- Publish a project description
- Publish a FRN
- Team up with ZT vendors for collaboration
- Execute project CY2020

Questions?

Alper Kerman

Security Engineer and Project Manager

Alper.Kerman@nist.gov

301.975.0226

http://www.nccoe.nist.gov

301-975-0200

nccoe@nist.gov