RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **ZT-M03**

Inside the Making of a Zero Trust Architecture

Alper Kerman

Security Engineer, Project Manager
NIST NCCoE

Scott Rose

Computer Scientist
NIST/CTL

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Agenda

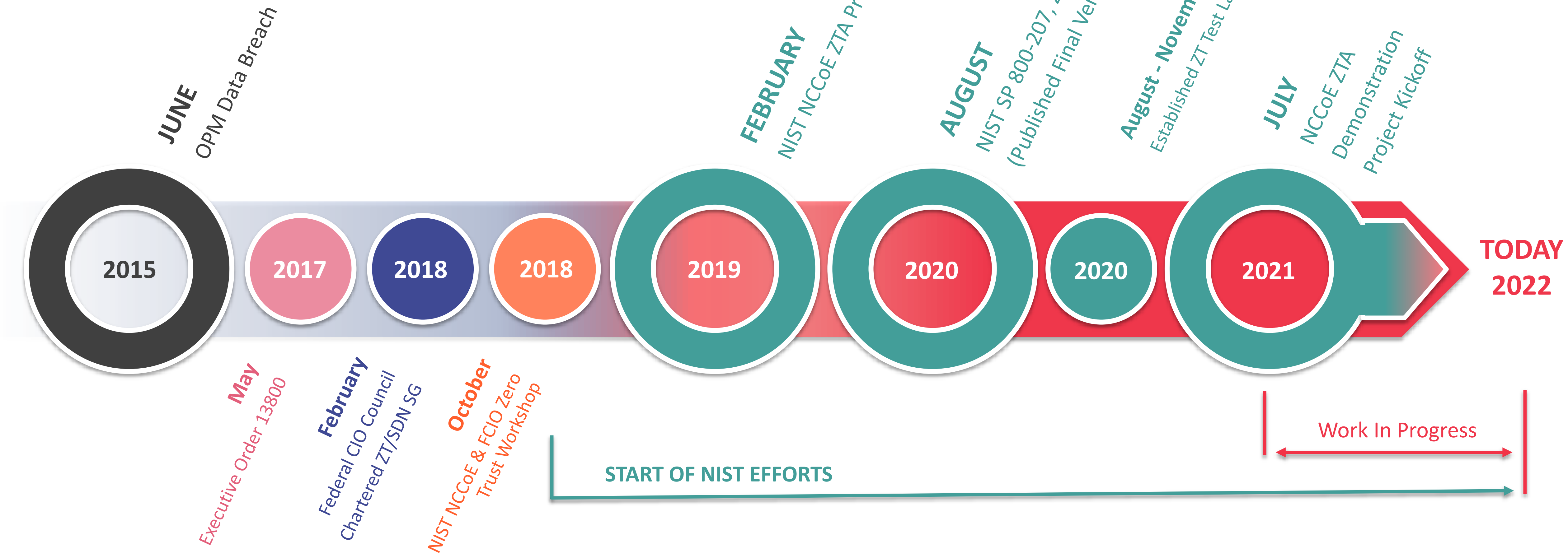
- NIST Zero Trust Efforts (Summary)
- Our View of Zero Trust
  - NIST Special Publication 800-207
- NIST National Cybersecurity Center of Excellence (NCCoE) ZTA Demonstration Project
- Getting Started

RSAConference2022

NIST Zero Trust Efforts

Initial Research and Ensuing Objectives

NIST Zero Trust Efforts



2015
JUNE
OPM Data Breach

2017
May
Executive Order 13800

2018
February
Federal CIO Council
Chartered ZT/SDN SG

2018
October
NIST NCCoE & FCIO Zero
Trust Workshop

2019
FEBRUARY
NIST NCCoE ZTA Project Launch

2020
AUGUST
NIST SP 800-207, ZTA Guidance
(Published Final Version)

2020
August - November
Established ZT Test Lab at NCCoE

2021
JULY
NCCoE ZTA
Demonstration
Project Kickoff

TODAY
2022

Work In Progress

START OF NIST EFFORTS

RSAConference2022

Zero Trust and NIST SP 800-207

Defining Zero Trust and its Principles

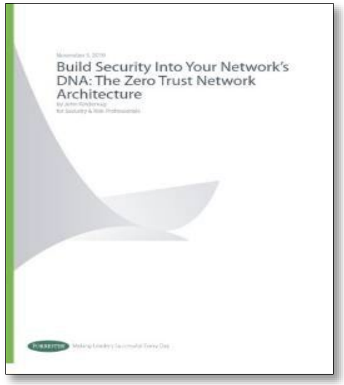
Zero Trust 101

2005: Jericho Forum De-perimeterization

JERICHO

Jericho Forum™ Commandments

2010: Forrester coins “Zero Trust”



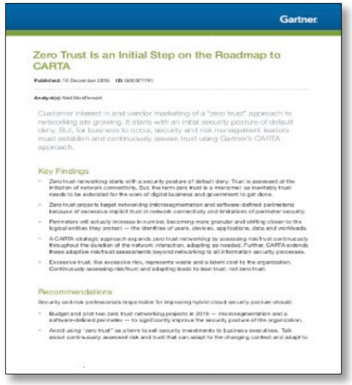
Build Security Into Your Network's DNA: The Zero Trust Network Architecture

2014: Google releases “BeyondCorp” papers

BeyondCorp

A New Approach to Enterprise Security

2018: Gartner coins “Lean Trust”



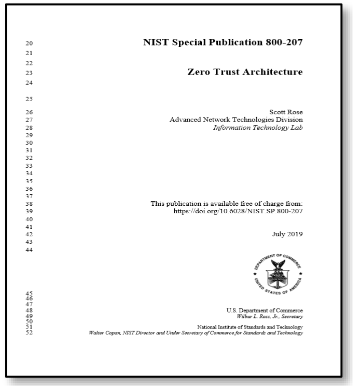
Gartner

Zero Trust Is an Initial Step on the Roadmap to CARTA

Key Findings

Recommendations

2019: NIST releases draft SP 800-207



NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Advanced Network Technologies Division
Information Technology Lab

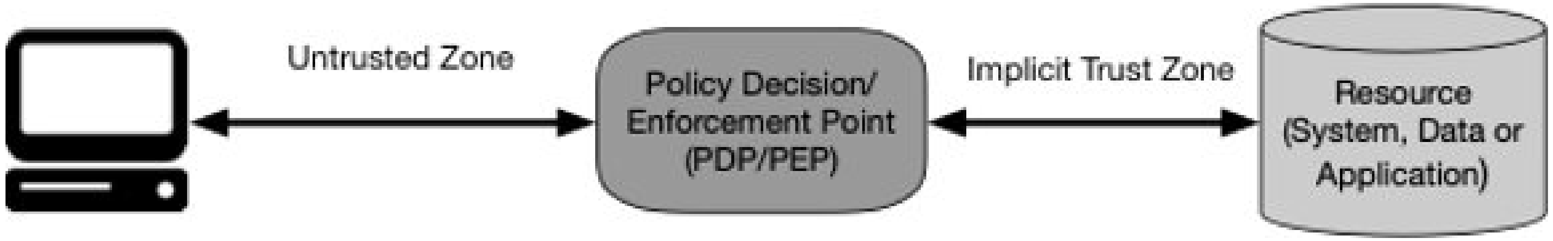
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

July 2019

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

- Zero trust is a set of principles used when designing, implementing and operating an infrastructure
- Want to reduce *implicit* trust between enterprise systems


Untrusted Zone
Policy Decision/ Enforcement Point (PDP/PEP)
Implicit Trust Zone
Resource (System, Data or Application)

NIST SP 800-207: Zero Trust Architecture

- A descriptive document, not prescriptive
- Contains definitions, observed approaches and tenets of zero trust
- Zero trust functional components
  - Policy Engine "The Brains"
  - Policy Administrator "The Executor"
  - Policy Enforcement Point "The Guard"
  - *Policy Information Point(s) "The Advisors"*

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

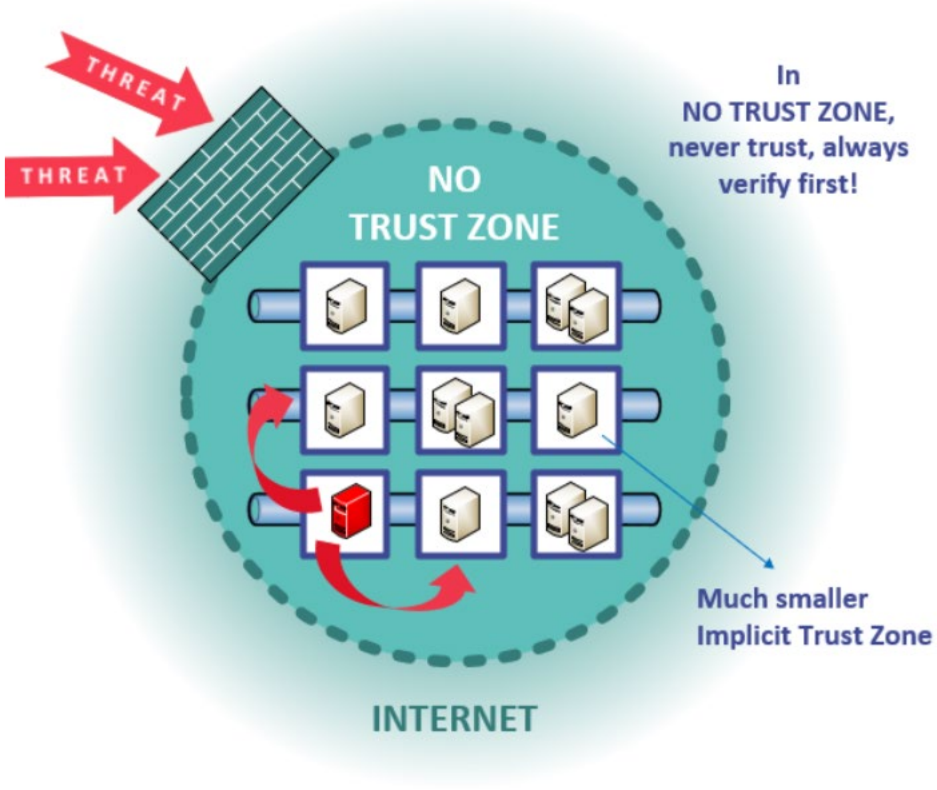
NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NIST SP 800-207 Approaches

Main Technology Used in Enterprise Policies

- Enhanced Identity Governance (EIG)
  - Using network ID as main enforcement point of access policies
- Micro-segmentation
  - Using network segmentation (e.g. firewalls, smart switches, etc.)
- Software Defined Perimeter (SDP)
  - Layer 7 solutions (e.g. overlay network, etc.)

Zero Trust Defense Focuses on Resource Protection


THREAT
THREAT
NO TRUST ZONE
In NO TRUST ZONE, never trust, always verify first!
Much smaller Implicit Trust Zone
INTERNET

"System of Systems" Reality

- Multiple Policy Engines/PEPs each covering a portion of ZT
  - ICAM, endpoint protection, network monitoring, etc.
  - Enterprise policy is overarching management

Pros:

- Mix/Match components (best of breed)
- May be able to keep existing tools
- Less vendor lock-in

Cons:

- Interoperability challenges
- Need centralized logs/SIEM
- May be difficult to diagnose issues

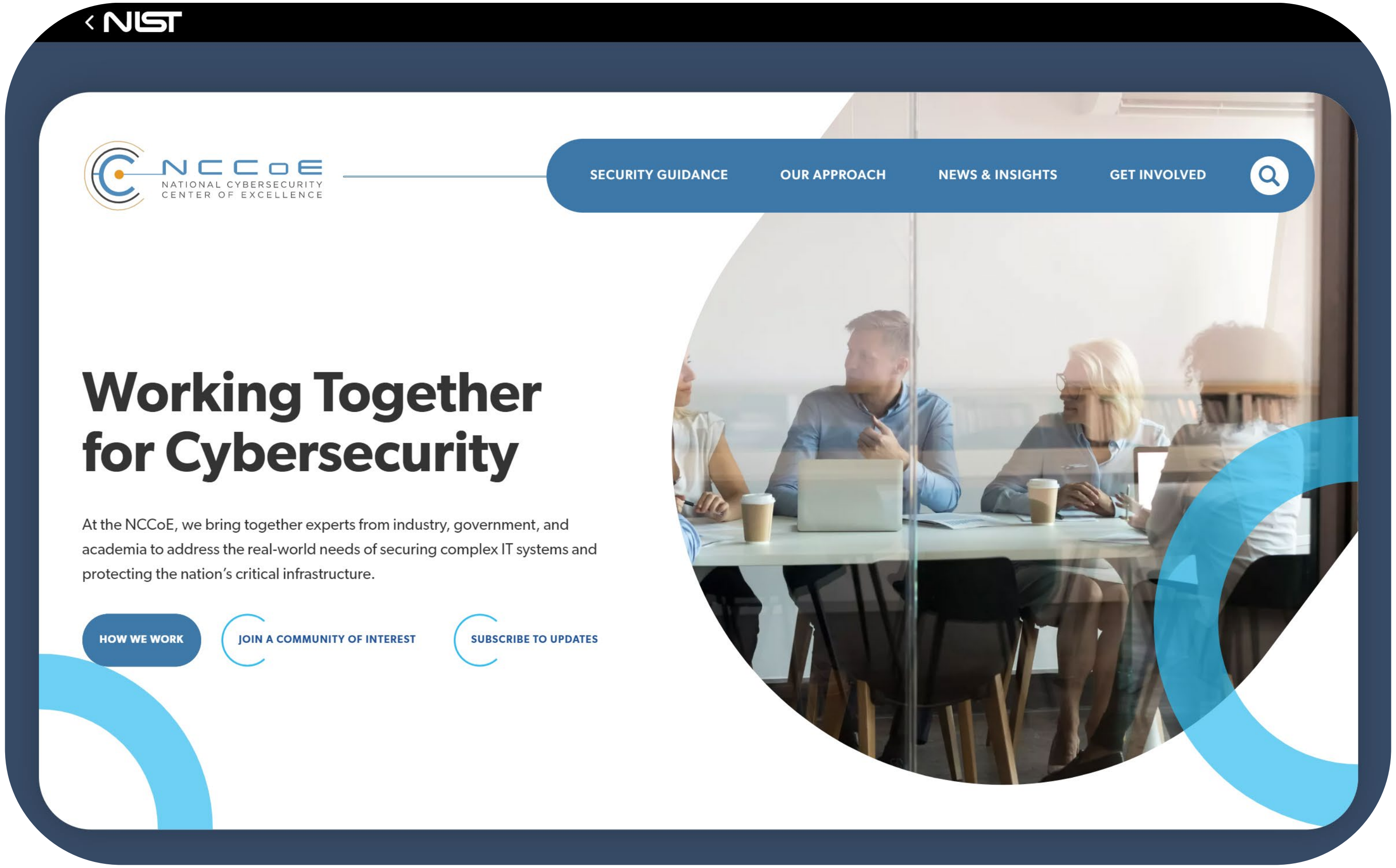
RSA®Conference2022

NCCoE Implementing a Zero Trust Architecture Project

Putting Principles into Practice

National Cybersecurity Center of Excellence (NCCoE)

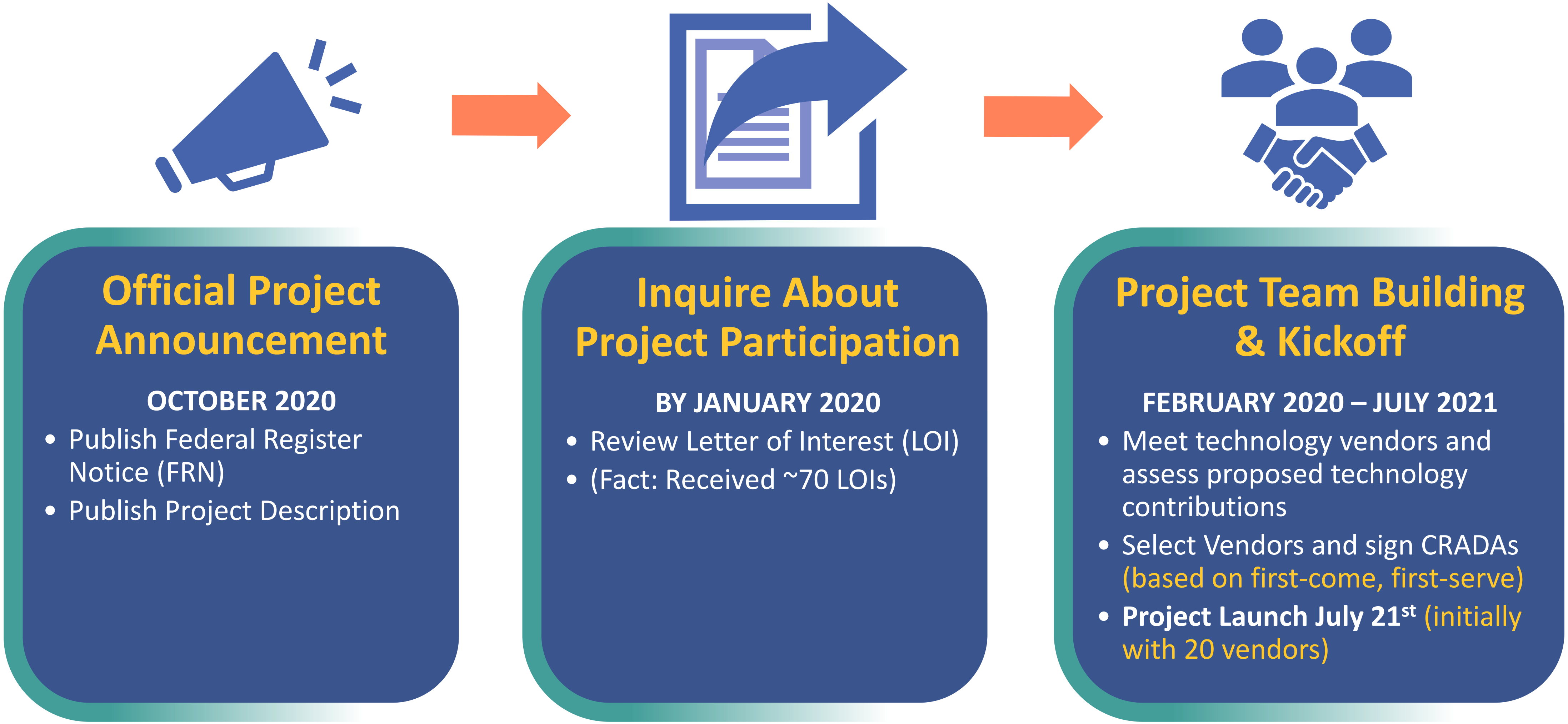
- NCCoE is a component of NIST (Established in 2012)
- Under project specific CRADAs, we work with industry organizations, government agencies and academic institutions to design and build example solutions for most prevalent cybersecurity problems.
- We complement each example solution with NIST 1800 series document (Practice Guide)



Working Together for Cybersecurity

At the NCCoE, we bring together experts from industry, government, and academia to address the real-world needs of securing complex IT systems and protecting the nation's critical infrastructure.

Implementing a ZTA – NCCoE Project Initiation



Official Project Announcement

OCTOBER 2020

- Publish Federal Register Notice (FRN)
- Publish Project Description

Inquire About Project Participation

BY JANUARY 2020

- Review Letter of Interest (LOI)
- (Fact: Received ~70 LOIs)

Project Team Building & Kickoff

FEBRUARY 2020 – JULY 2021

- Meet technology vendors and assess proposed technology contributions
- Select Vendors and sign CRADAs (based on first-come, first-serve)
- **Project Launch July 21st** (initially with 20 vendors)

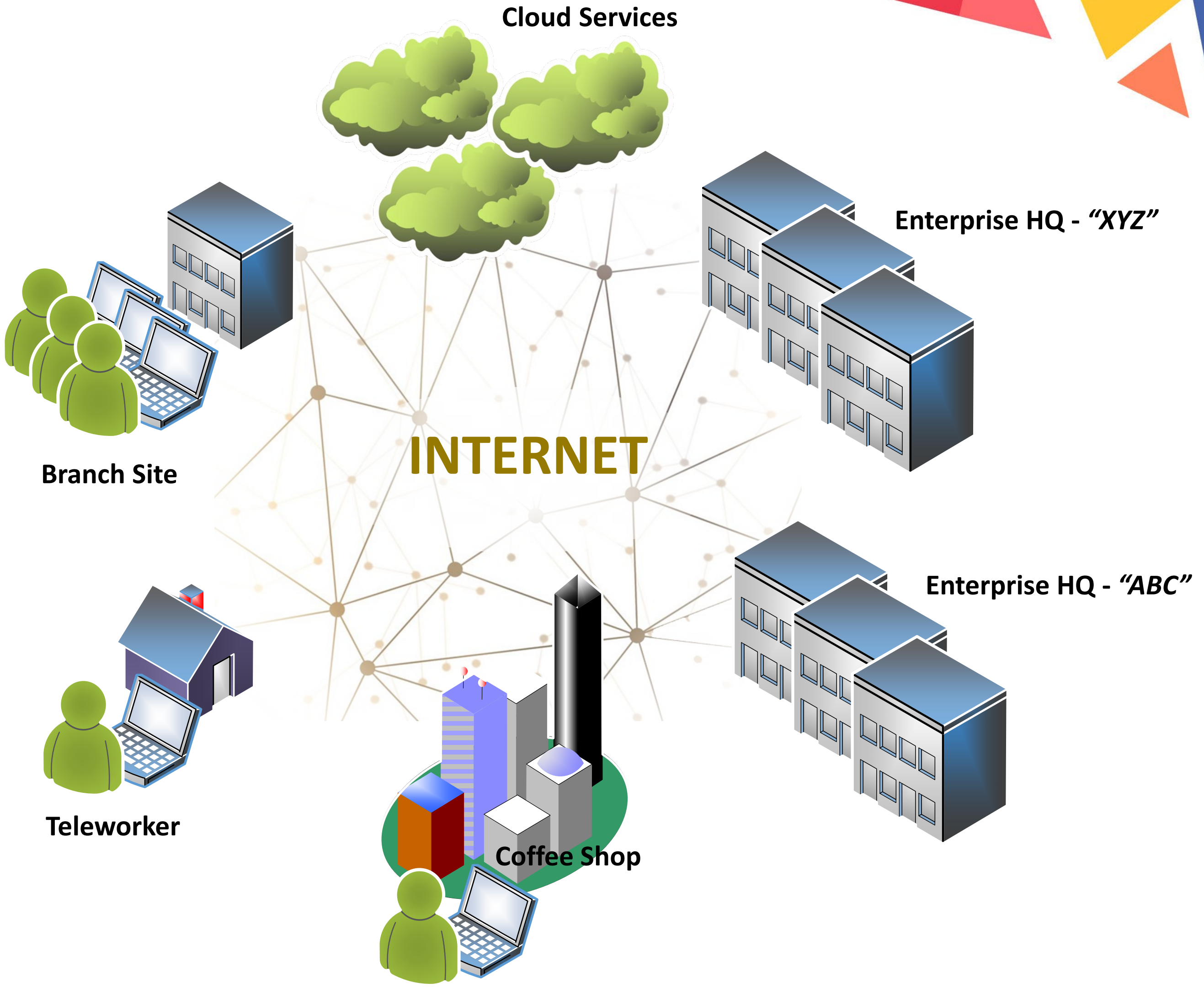
Project Goals and Focus

Deployment Approaches

- Enhanced Identity Governance (EIG)
- Micro-segmentation
- Software Defined Perimeter (SDP)

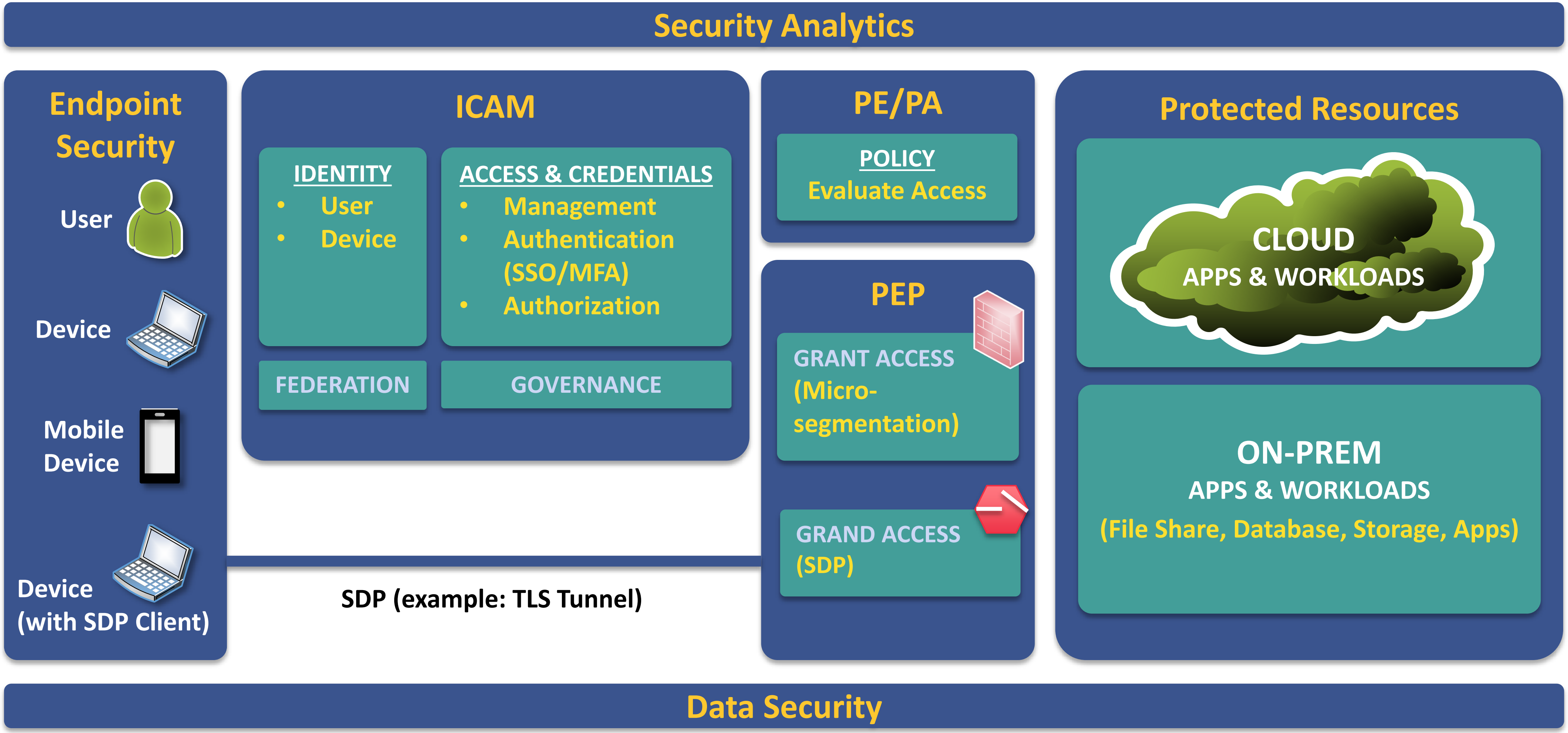
Demonstration Scenarios

- Employee Access to Corporate Resources
- Employee Access to Internet Resources
- Contractor Access to Corporate and Internet Resources
- Inter-server Communication Within the Enterprise
- Cross Enterprise Collaboration with Business Partners
- Develop Trust Score/Confidence Level with Corporate Resources

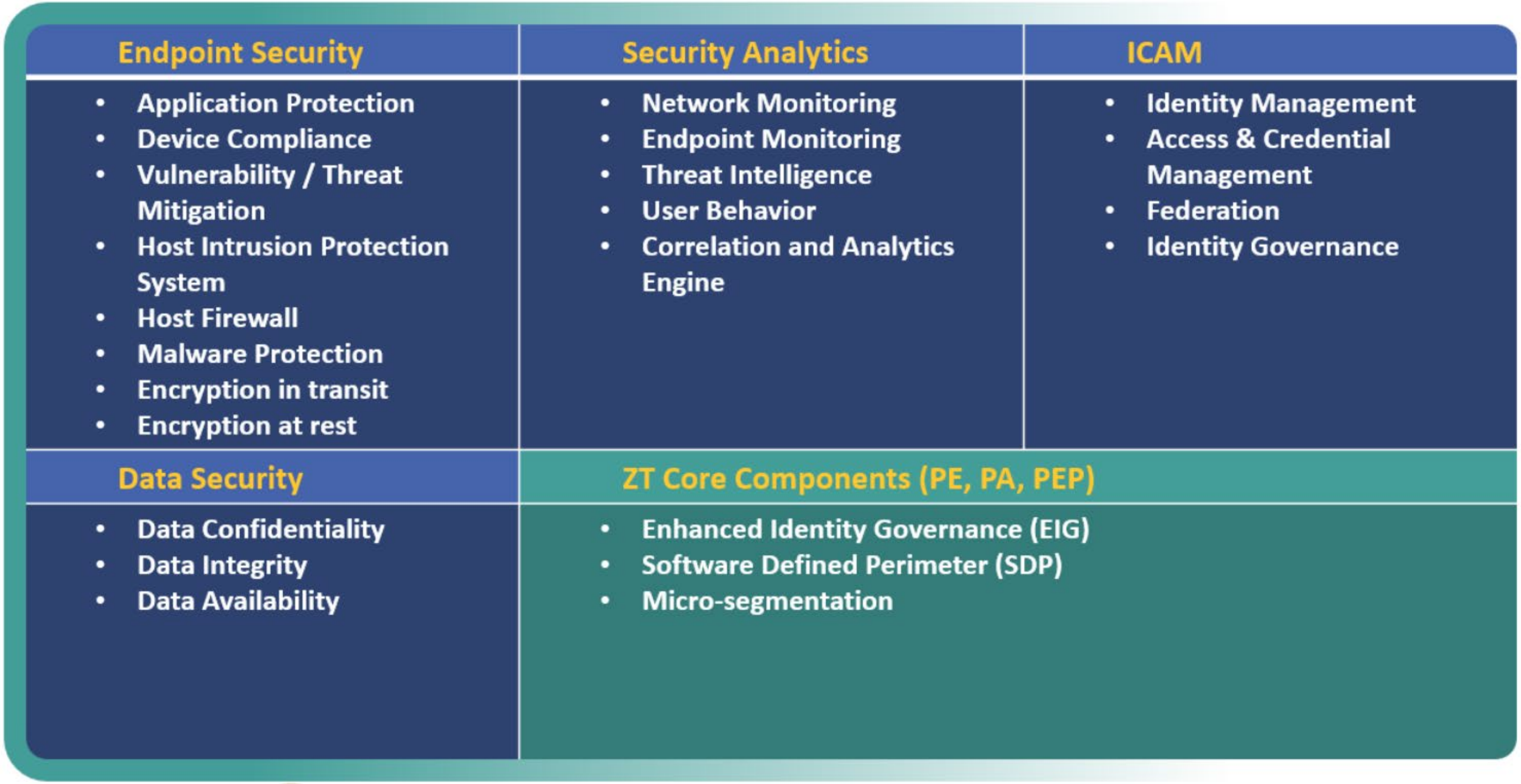


Deployment (Brownfield) Use Case Scenario
"Enterprise with Satellite Facilities"

NOTIONAL ZTA ARCHITECTURE



ZTA Capabilities Groupings



Endpoint Security

- Application Protection
- Device Compliance
- Vulnerability / Threat Mitigation
- Host Intrusion Protection System
- Host Firewall
- Malware Protection
- Encryption in transit
- Encryption at rest

Security Analytics

- Network Monitoring
- Endpoint Monitoring
- Threat Intelligence
- User Behavior
- Correlation and Analytics Engine

ICAM

- Identity Management
- Access & Credential Management
- Federation
- Identity Governance

Data Security

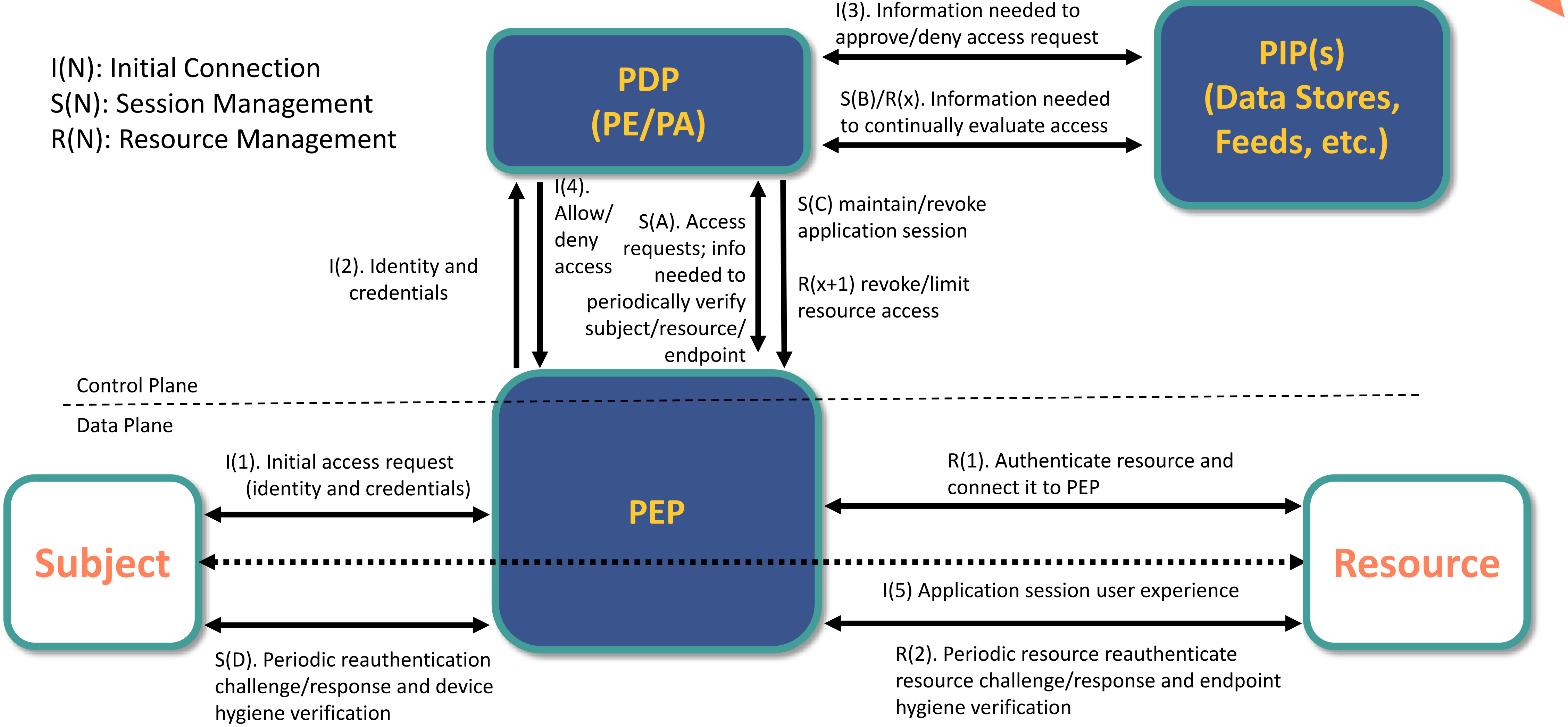
- Data Confidentiality
- Data Integrity
- Data Availability

ZT Core Components (PE, PA, PEP)

- Enhanced Identity Governance (EIG)
- Software Defined Perimeter (SDP)
- Micro-segmentation

Notional Deployment Approach

I(N): Initial Connection
S(N): Session Management
R(N): Resource Management



I(3). Information needed to approve/deny access request

S(B)/R(x). Information needed to continually evaluate access

I(2). Identity and credentials

I(4). Allow/ deny access

S(A). Access requests; info needed to periodically verify subject/resource/ endpoint

S(C) maintain/revoke application session

R(x+1) revoke/limit resource access

I(1). Initial access request (identity and credentials)

R(1). Authenticate resource and connect it to PEP

I(5) Application session user experience

S(D). Periodic reauthentication challenge/response and device hygiene verification

R(2). Periodic resource reauthenticate resource challenge/response and endpoint hygiene verification

Project Implementation Strategy & Focus Areas

- Take on agile approach with each implementation
  - Implement iteratively and incrementally (crawl, walk and run)
    - Implement multiple builds for demonstration of each deployment approach
      - Start with a minimum viable solution when implementing each deployment approach
      - Capture and document the experience and findings toward a more mature ZTA
- Determine use cases for scenarios in:
  - Asset/resource discovery and registration
    - **examples:** enterprise owned, cloud based, etc.
  - Access to resources on-prem, in the cloud, on the internet using different types of IDs
    - **examples:** enterprise ID, federated ID, other ID, etc.
- Determine ZTA capabilities needed for demonstration of each deployment approach
  - Identify capabilities needed for crawl (minimum viable solution), walk and run implementation phases
- Start with Enhanced Identity Governance (EIG) approach
    - Why?
      - Not as complex
      - Identity is essential

Project Status

- Currently focused on implementing builds that demonstrate the EIG deployment approach
  - Close to finishing up
  - Next implementations will focus on micro-segmentation and SDP deployment approaches
- Also focused on publishing a preliminary draft of the Practice Guide (NIST SP 1800-35)
  - Preliminary Draft NIST SP 1800-35A (Published on June 3rd, 2022, Public Comment Period Open until July 5th, 2022)
  - Preliminary Draft NIST SP 1800-35B (Anticipated Publishing Date: End of July)
  - Preliminary Draft NIST SP 1800-35C (Anticipated Publishing Date: Mid August)
- Project Website
  - https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture
- Project COI
  - Request to Join Email: nccoe-zta-coi@list.nist.gov
- NIST ZTA Forum
  - Request to Join Email: nist-nccoe-zta@list.nist.gov
  - Forum Webpage: https://www.nccoe.nist.gov/nist-zero-trust-architecture-forum

Participating Project Collaborators

aws

appgate

CISCO

f5

digicert

FORESCOUT

Google Cloud

IBM

ivanti

Lookout

MANDIANT

McAfee

Microsoft

okta

paloalto NETWORKS

PC Matic

PingIdentity

RADIANT LOGIC

SailPoint

BROADCOM SOFTWARE

tenable

vmware

ZIMPERIUM

zscaler

Getting Started

- Right Now:
  - do a risk analysis on your organization's primary mission
  - Identify resources (including PE/PEPs)
- For the Next Quarter:
  - Begin forming policies for workflows
  - Identify gaps (technology/policy/process)
- For the Next 6-12 months:
  - Focus on “low hanging fruit”
    - Addressing gaps in identity, compliance, and monitoring