

SECURING OPERATIONAL TECHNOLOGY ACROSS DECADES OF MISSION READINESS

ZERO TRUST BY DESIGN



Mangaya Sivagnanam
Engineering Leader, Product Security & Compliance
Trane US | Trane Technologies
Mangaya.Sivagnanam@trane.com
LinkedIn: www.linkedin.com/in/mangaya

Mark O'Reilly
Federal Market Team Leader
Trane US | Trane Technologies
Mark.OReilly@tranetechnologies.com
LinkedIn: www.linkedin.com/in/markdoreilly

IMPERATIVE DYNAMICS OF TODAY'S LANDSCAPE

Federal Footprint: ~370M s.f. (1.5K facilities / DoD: 700K s.f.)

DAF Footprint: 21K+ assets at CONUS AFBs (and this is just *Trane* assets!)
59/60 Active AFBs (also ANG, AFRES, JBs)

Device Connectivity: One system incl. >160K connected devices

Decentralized Management

Diverse OEMs and Networks

Connected Systems: 766 systems use OT/IOT across 23 civ agencies (GAO)

Connectivity Issues

Silo'd Requirements



Source: Major AF Installations (U.S. Air Force)

WITH CONVERGENCE COMES RISKS

9 OUT OF 10 ORGANIZATIONS EXPERIENCED AT LEAST ONE INTRUSION IN THE PAST YEAR, AND
78% HAD THREE OR MORE INTRUSIONS



ZERO-DAY EXPLOITATION
HAS INCREASED BY 46%

PUBLISHED
VULNERABILITIES ROSE BY
15%

45% CARRIED HIGH OR
CRITICAL CVSS

A TRANSFORMATIVE APPROACH

INCREASING IMPORTANCE OF **ZERO TRUST** IN OPERATIONAL TECHNOLOGY AND MISSION-CRITICAL SYSTEMS

- ✓ Mission Priorities
- ✓ Memorandum M-22-09
- ✓ Accelerating Adversaries' Capabilities
- ✓ Strategic Alignment
- ✓ Defensible Architecture
- ✓ Resilient Infrastructure



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

January 26, 2022

M-22-09

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director

A handwritten signature in dark ink, reading "Shalanda D. Young".

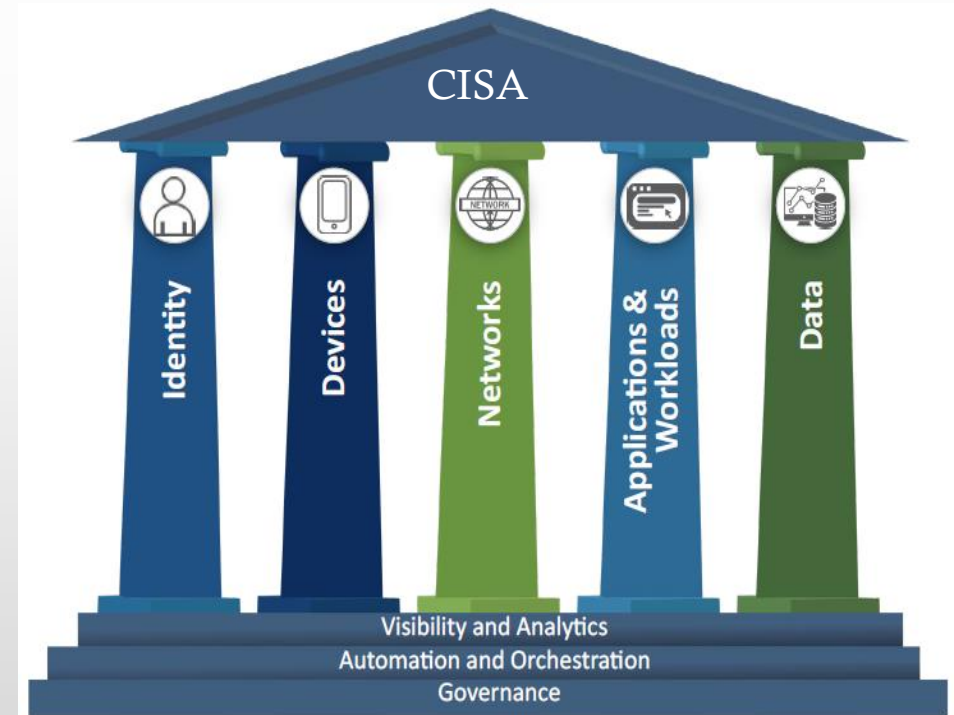
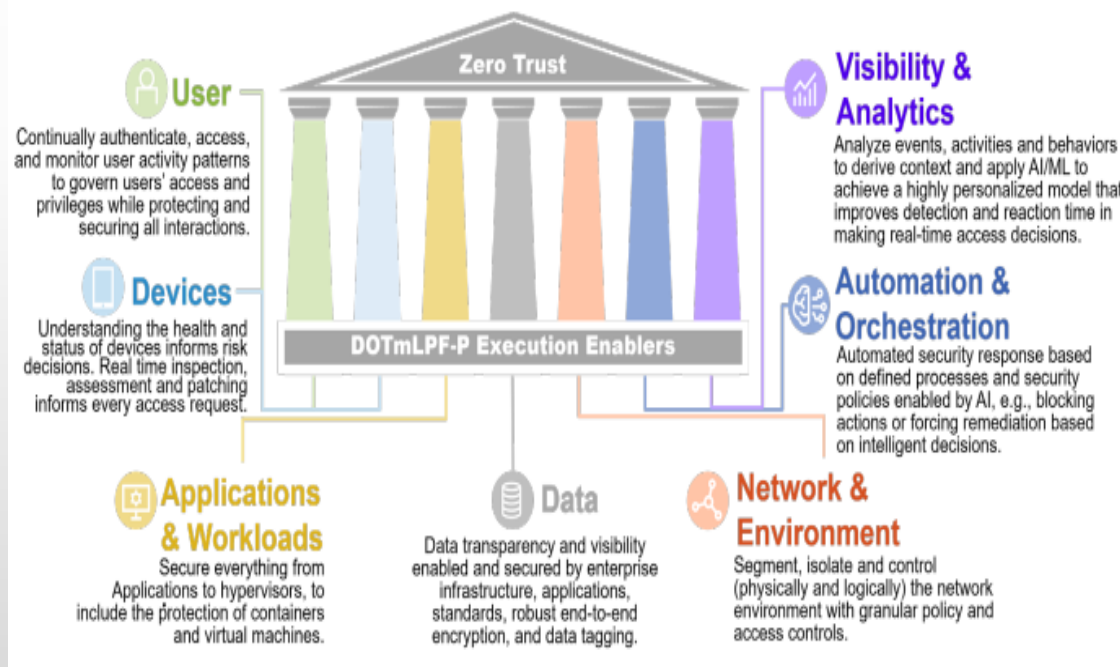
SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

This memorandum sets forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns. Those campaigns target Federal technology infrastructure, threatening public safety and privacy, damaging the American economy, and weakening trust in Government.

ZERO TRUST

- ✓ ZTA (Zero Trust Adoption) Plan
- ✓ Zero Trust Maturity Model Pillars
- ✓ Secure by design vs. secure by operations
- ✓ Network infrastructure (physical and virtual)
- ✓ Operational policies

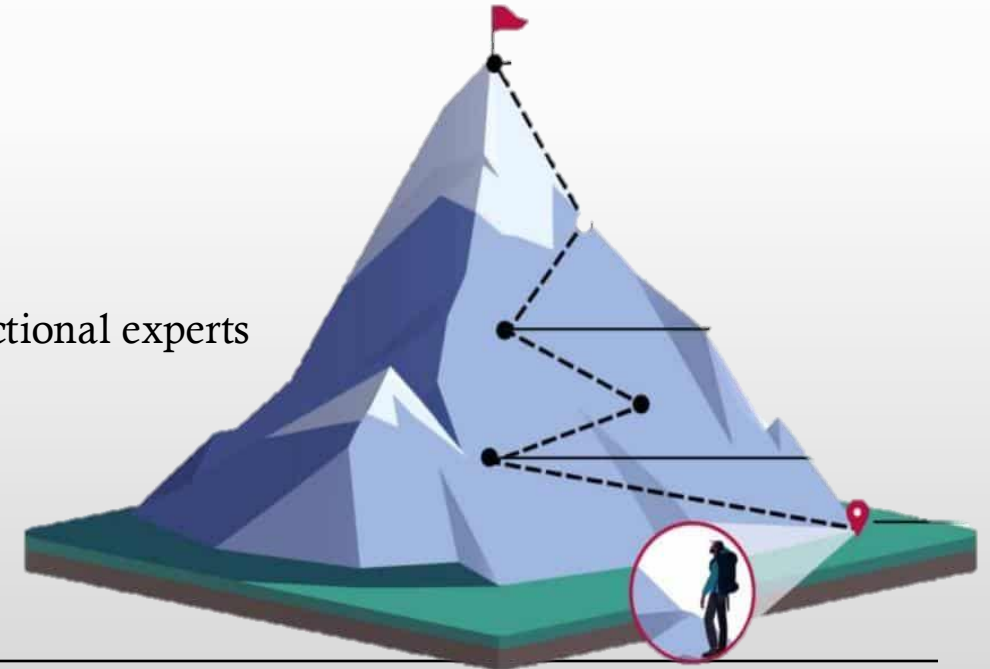
PUBLICLY AVAILABLE MODELS
PILLARS VARY, BUT HAVE A SHARED
COMMITMENT/APPROACH



ADOPTION /CHALLENGES

NAVIGATING THE JOURNEY TO ZERO TRUST

- ✓ Organization Commitments
- ✓ IT Vs. OT Convergence
 - Implicit Trust
 - Aging infrastructure
 - Erosion of Traditional Control Points (procurement)
 - Cloud Services / Digital Supply Chain Vulnerability
- ✓ No Integrated Approach to OT
 - Lack of DOTMLPF Guidance/Solutions
 - OT procured as a “functional” system requires a range of functional experts (ME <> Cyber)
- ✓ Portfolio planning must be integrated
 - Deconflict & Integrate IT/OT portfolios
 - Integrate requirements, incl maintenance
 - Industry Government Alignment



MISSION ENABLERS

ZERO TRUST: FUELING YOUR JOURNEY TO MISSION ACCOMPLISHMENT

- ✓ Reduced Attack Surface
- ✓ Enhanced Data Protection
- ✓ Continuous Compliance
- ✓ Improve Visibility, Detection And Response
- ✓ Capital Planning & OT Asset Management
- ✓ Perimeter Security (Risk-based Approach)
- ✓ Enables Digitalization
- ✓ Adaptability to Hybrid Environments
- ✓ Boosted Third-Party and Supply Chain Security
- ✓ Accelerated Mission Outcomes
- ✓ More Stable Cyber Investments



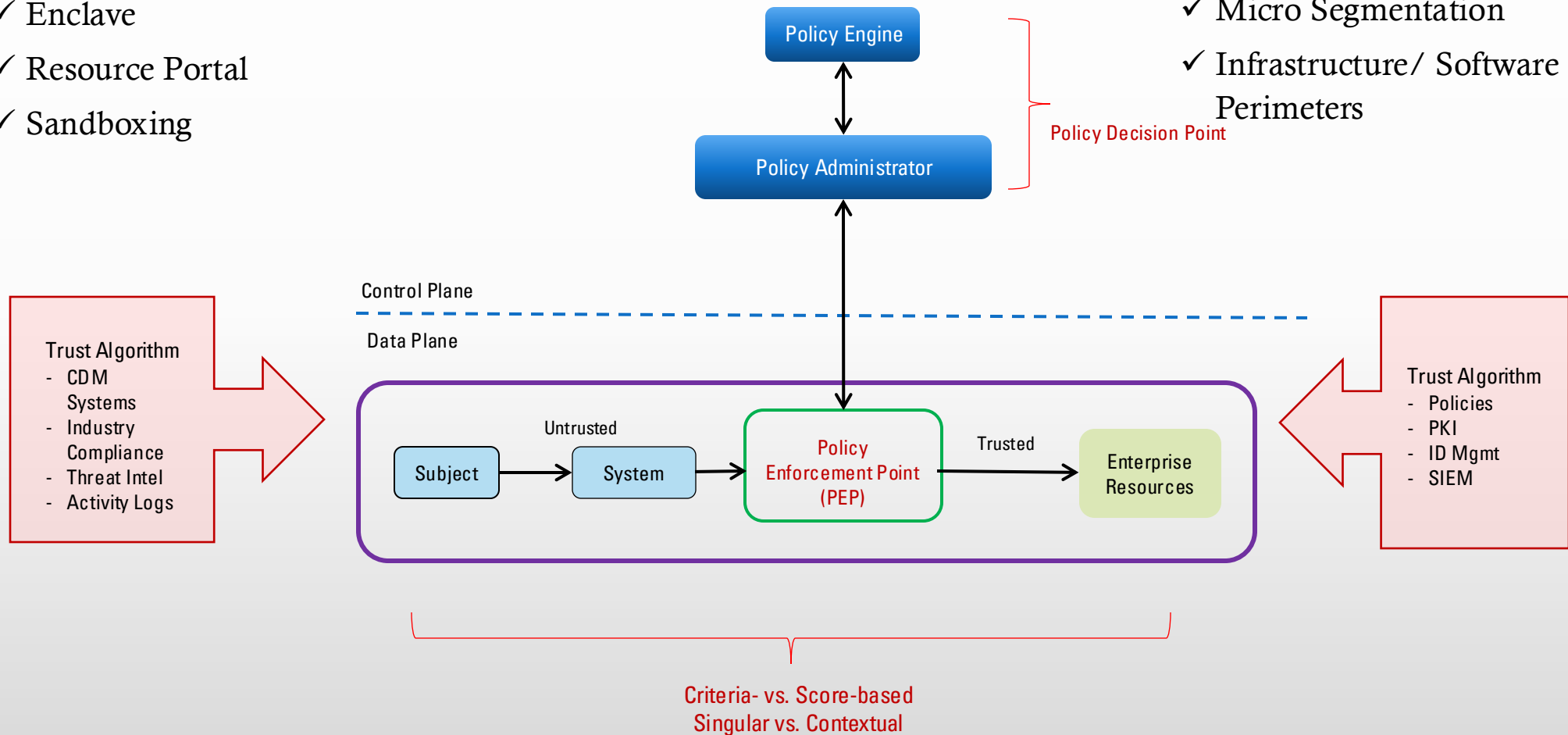
ZERO TRUST ARCHITECTURE

DEPLOYMENT TECHNIQUES

- ✓ Device Agent/Gateway
- ✓ Enclave
- ✓ Resource Portal
- ✓ Sandboxing

APPROACHES

- ✓ Enhanced Identity Approach
- ✓ Micro Segmentation
- ✓ Infrastructure/ Software Defined Perimeters



ZERO TRUST ARCHITECTURE

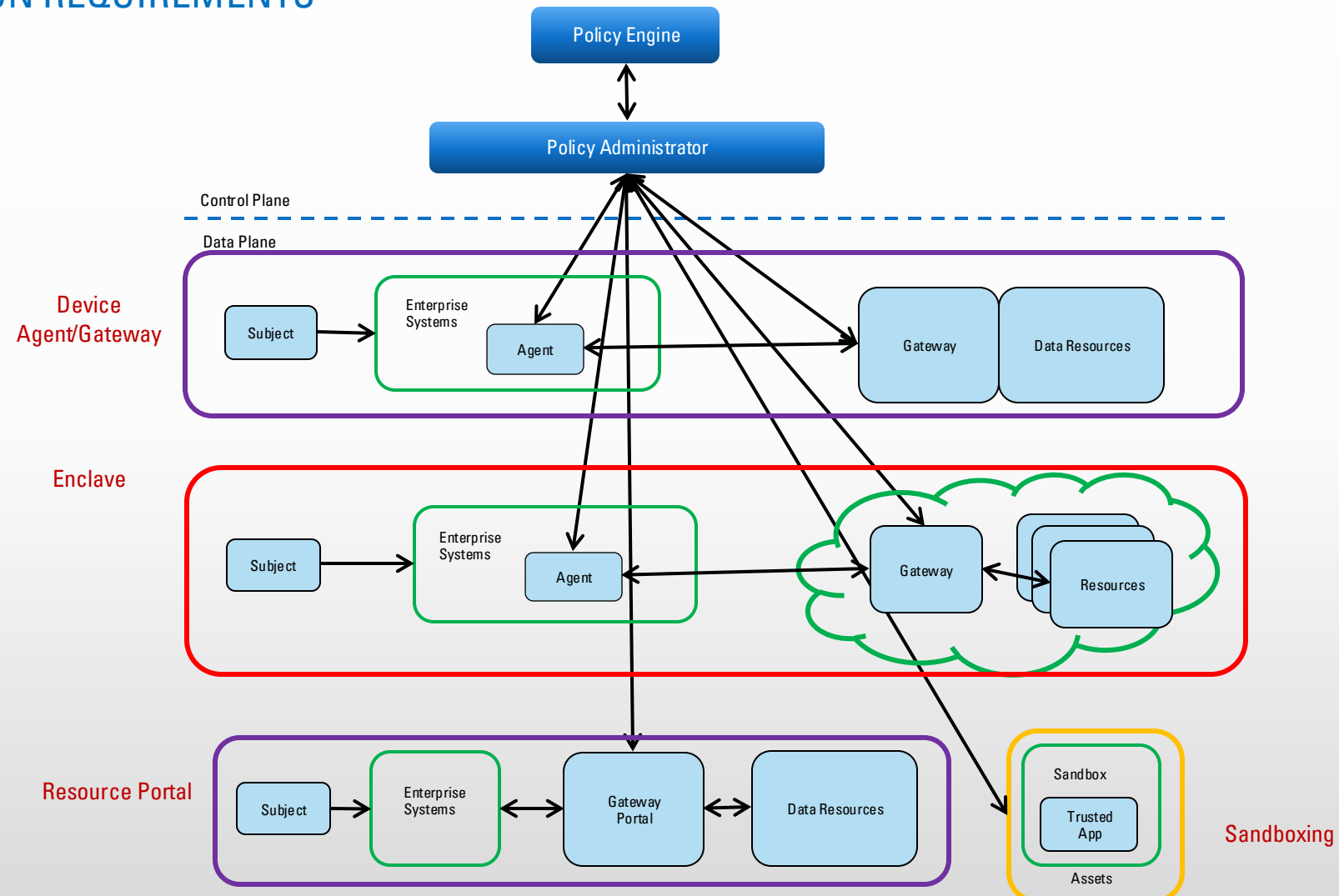
DEPLOYMENT VARIATIONS – MISSION REQUIREMENTS

Robust device management program /
discrete resources that can
communicate with the gateway

Useful for enterprises that use cloud-
based micro-services for a single
business processes

More flexible for BYOD policies and
interorganizational collaboration projects

Advantage here is that individual
applications are segmented from the rest
of the asset





KEYS TO SUCCESS

PRIORITIZE OT ZERO TRUST AS MISSION-ESSENTIAL – BECAUSE IT IS!





Mangaya Sivagnanam
Engineering Leader, Product Security & Compliance
Trane US | Trane Technologies
Mangaya.Sivagnanam@trane.com
LinkedIn: www.linkedin.com/in/mangaya

Mark O'Reilly
Federal Market Team Leader
Trane US | Trane Technologies
Mark.O'Reilly@tranetechnologies.com
LinkedIn: www.linkedin.com/in/markdoreilly
