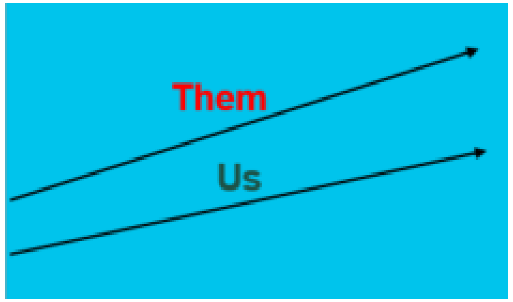
Zero Trust – The Time is Now!

Tim Denman,

DoD Zero Trust Portfolio Management Office (ZT PfMO)

July 20, 2022

We’re Getting Better at Cybersecurity, BUT …



Government Accountability Office (GAO)

- While around 80% of over 3,000 identified cyber problems have been documented as being fully addressed, the problems continue to mount, with some signs of progress, but not enough to keep up with the advances of our cyber adversaries.
- Until cyber shortcomings are addressed, information and systems will be increasingly susceptible to the multitude of cyber-related threats.

(GAO High Risk Series, July 2018, GAO 18-645T, “Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation”)

Director, Operational Test & Evaluation (DOT&E)

- Cybersecurity was the most common survivability problem. Despite ongoing cybersecurity improvements, multiple programs were shown as not survivable in a cyber-contested environment.
- A suite of cybersecurity capabilities intended to protect the Department of Defense Information Network (DODIN) was not effective in defending against the threat. As a result, the capabilities were not deployed and a Zero Trust security architecture was recommended for deployment as quickly as possible.

(Director, Operational Test & Evaluation (DOT&E) FY 2021 Annual Report, January 2022, DOT&E)

DoD Cybersecurity improvements are NOT keeping up with adversaries

Why Zero Trust?

Legacy cybersecurity approaches, such as Perimeter Defense, have never worked:

- Network boundaries have become increasingly fluid, VPN'd, or nonexistent
- "Break and Inspect" as a practice is increasingly incapable and ineffective at providing protection

Defining a critical mission "protection surface" is possible, but the "attack surface" is much harder to identify:

- Exploitation can happen anywhere – unpatched systems, zero-day exploits, supply-chain exploits, inadequate security awareness program for policies and employees, etc.
- Implicit trust to "authenticated" users enterprise-wide can lead to total network infiltration

Network cybersecurity must be focused on the practice of continually verifying the identity, authorization, and authentication of data, users, and devices at all times.

Zero Trust is a cybersecurity paradigm focused on users, assets, and resources

What is Zero Trust?

Zero trust is an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources.

Source: *DoD Zero Trust Reference Architecture, V2, September 2021, p. 9*

Zero Trust is:

A Cultural Shift in Security Philosophy	A Paradigm Shift in Security Implementation
Trust no one/nothing; always assume a breach	**Holistically examine cybersecurity** – from users to applications to networks
Trust is an exploitable emotion – thus it must be removed from cyber security	**Employ risk-based confidence levels**
	Goal: prevent data breaches, protect your key information assets

Can we “buy” Zero Trust?

No; Zero Trust may include certain products or technologies but cannot be achieved **solely** through introducing new technologies.

“**Zero Trust is not a capability or device you buy**, rather it is a security framework, an architectural approach, and a methodology to prevent malicious actors from accessing our most critical assets and reducing existing attack surfaces.”

– Mr. Randy Resnick
Director, DoD Zero Trust Portfolio Management Office

The Strategy Behind Zero Trust

The underlying strategy behind Zero Trust is to embed security across the architecture to keep malicious actors from the DoD's critical assets. As the name implies, the foundational principle of the Zero Trust model is that basically nothing is trusted, everything is continuously and fully verified. This applies to people or actors, systems, networks and services both inside and outside of the security perimeter. It is a completely new way of thinking and a major cultural and paradigm shift from verify only at the perimeter to continually verifying every user, device, application and transaction.

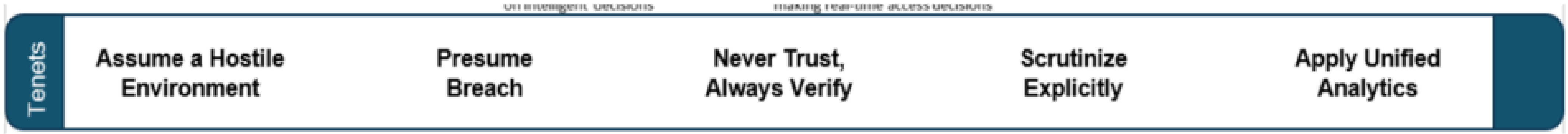
ZT focuses on protecting critical data and resources, not just the traditional network or perimeter security

Directives and Memorandums Driving ZT

- **National Manager Memorandum 2022-01: National Security Memorandum 8, Zero Trust Security and Cloud Migration Security Guidance, Feb 2, 2022**
  - The heads of USG Departments and Agencies that owns/operates NSS are responsible for updating existing plans to reprioritize resources for the adoption of Zero Trust Architectures (ZTA)
- **OMB Memo M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, Jan 26, 2022**
  - Aligns with EO 14028. Requires Agencies to achieve specific Zero Trust security goals by end of FY24
- **Memorandum on *Improving the Cybersecurity of National Security, DoD & IC Systems,* National Security Memorandum // NSM-8, Jan 19, 2022**
  - Sets forth requirements for National Security Systems (NSS) that are equivalent to, or exceed, cybersecurity requirements in EO 14028
- **National Defense Authorization Act (NDAA) Section 1528 for Fiscal Year (FY) 2022, December 27, 2021**
  - Seeks to further the government-wide adoption of Zero Trust Architectures (ZTA)
- **Executive Order (EO) 14028 on *Improving the Nation's Cybersecurity*, May 12, 2021**
  - Head of each Agency shall develop a plan to implement Zero Trust Architectures (ZTA)

Basic Tenets of Zero Trust

According to the **DoD Zero Trust Reference Architecture** there are five basic Zero Trust tenets. These tenets are as follows:



on intelligent decisions

making real-time access decisions

Tenets

- Assume a Hostile Environment
- Presume Breach
- Never Trust, Always Verify
- Scrutinize Explicitly
- Apply Unified Analytics

Zero Trust assumes continued and mandated use of communication encryption to the greatest extent possible.

Zero Trust Tenets Explained

1. **Assume a Hostile Environment.** There are malicious personas both inside and outside the network. All users, devices, and networks/environments are treated as untrusted.
2. **Presume Breach.** There are hundreds of thousands of attempted cybersecurity attacks against DOD networks every day. Consciously operate and defend resources with the assumption that an adversary has presence within your environment. Enhanced scrutiny of access and authorization decisions to improve response outcomes.
3. **Never Trust, Always Verify.** Deny access by default. Every device, user, application/workload, and data flow are authenticated and explicitly authorized using least privilege, multiple attributes, and dynamic cybersecurity policies.

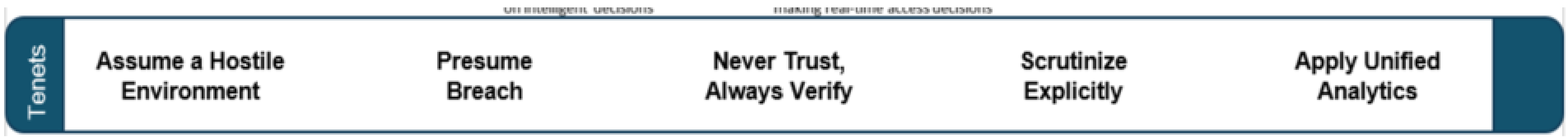
on intelligent decisions

making real-time access decisions

Tenets	Assume a Hostile Environment	Presume Breach	Never Trust, Always Verify	Scrutinize Explicitly	Apply Unified Analytics

Zero Trust Tenets Explained

4. **Scrutinize Explicitly**. All resources are consistently assessed in a secure manner using multiple attributes (dynamic and static) to derive confidence levels for contextual access to resources. Access to resources is conditional and access can dynamically change based on action and confidence levels resulting from those actions.
5. **Apply Unified Analytics**. Apply unified analytics for Data, Applications, Assets, Services (DAAS) to include behavioristics, and log each transaction.



on intelligent decisions making real-time access decisions

Tenets	Assume a Hostile Environment	Presume Breach	Never Trust, Always Verify	Scrutinize Explicitly	Apply Unified Analytics

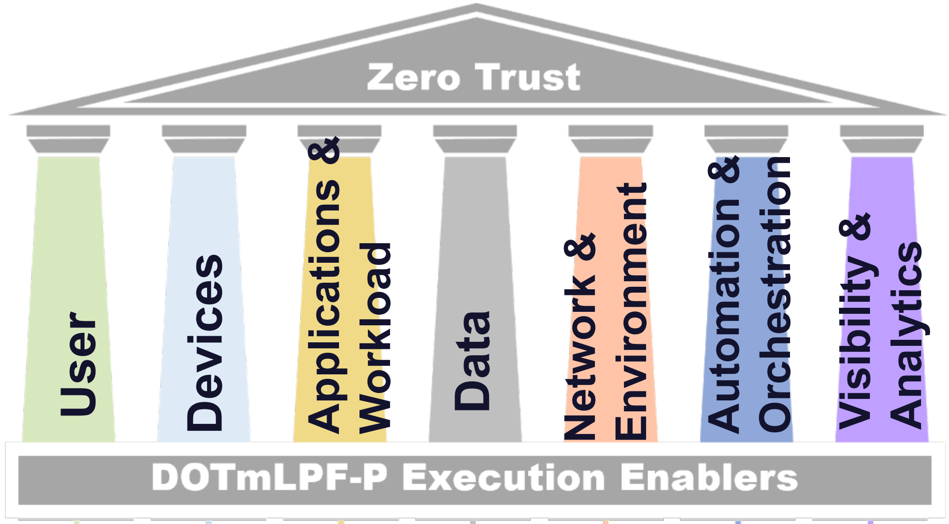
The Pillars and Capabilities of Zero Trust

(DoD Zero Trust Reference Architecture)

There are many important aspects of Zero Trust and ways it can be implemented. DoD expresses the most important of these aspects as being pillars. These pillars align with capabilities and allow for a logical presentation of Zero Trust principles. According to the DoD Zero Trust Reference Architecture, pillars and capabilities can be defined as follows:

- **Pillar** - a key focus area for implementation of Zero Trust controls.
- **Capabilities** - the ability to achieve a Desired Effect under specified (performance) standards and conditions through combinations of ways and means (activities and resources) to perform a set of activities

DoD Zero Trust Pillars: A Cultural and Paradigm Shift



User

Continually authenticate, access, and monitor user activity patterns to govern users' access and privileges while protecting and securing all interactions.

Devices

Understanding the health and status of devices informs risk decisions. Real time inspection, assessment and patching informs every access request.

Applications & Workloads

Secure everything from Applications to hypervisors, to include the protection of containers and virtual machines.

Data

Data transparency and visibility enabled and secured by enterprise infrastructure, applications, standards, robust end-to-end encryption, and data tagging.

Network & Environment

Segment, isolate and control (physically and logically) the network environment with granular policy and access controls.

Automation & Orchestration

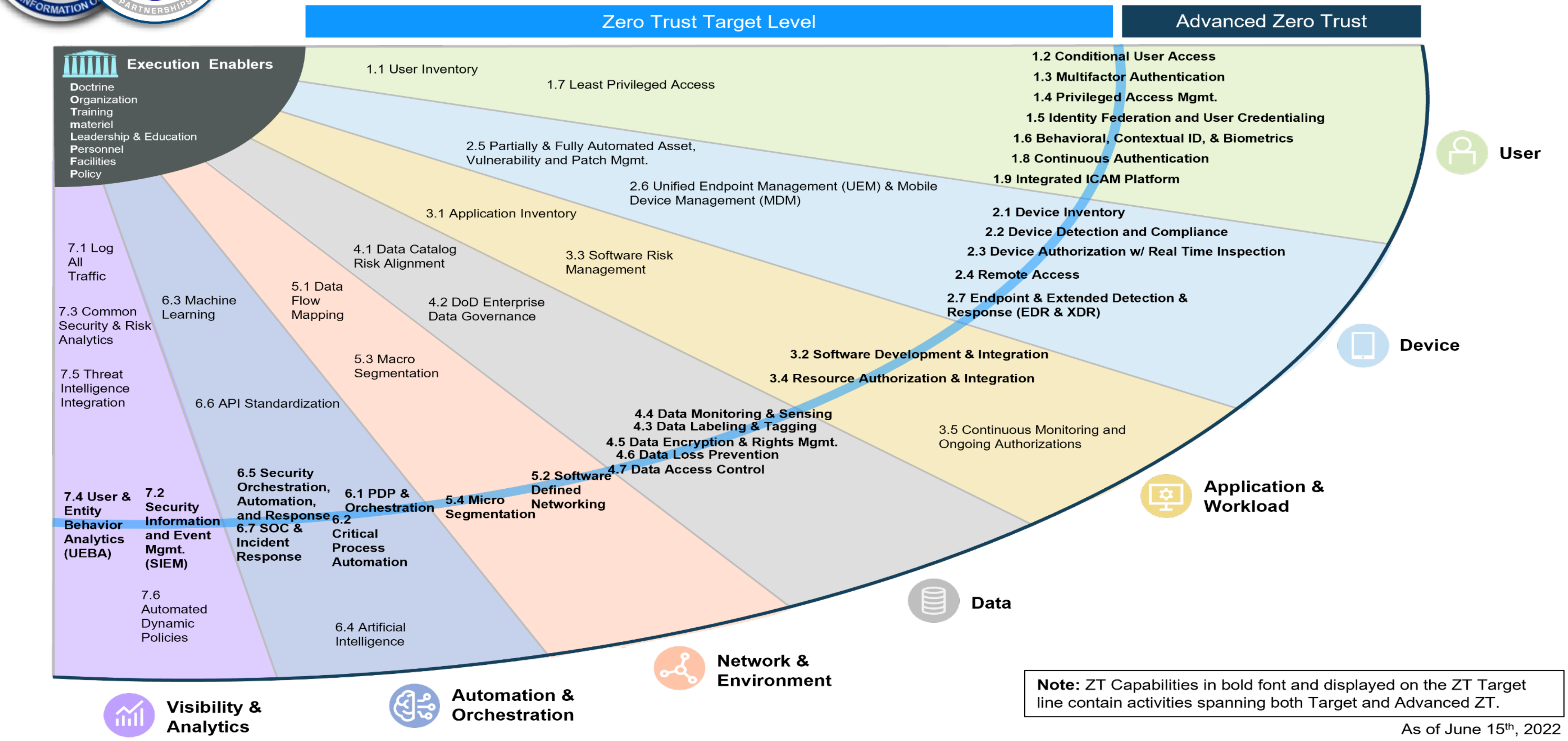
Automated security response based on defined processes and security policies enabled by AI, e.g., blocking actions or forcing remediation based on intelligent decisions.

Visibility & Analytics

Analyze events, activities and behaviors to derive context and apply AI/ML to achieve a highly personalized model that improves detection and reaction time in making real-time access decisions.

UNCLASSIFIED

DoD ZT Capability Maturity Model: a Zero Trust Accelerator



Zero Trust Target Level

Advanced Zero Trust

Execution Enablers

Doctrine
Organization
Training
materiel
Leadership & Education
Personnel
Facilities
Policy

User

1.1 User Inventory
1.7 Least Privileged Access
1.2 Conditional User Access
1.3 Multifactor Authentication
1.4 Privileged Access Mgmt.
1.5 Identity Federation and User Credentialing
1.6 Behavioral, Contextual ID, & Biometrics
1.8 Continuous Authentication
1.9 Integrated ICAM Platform

Device

2.5 Partially & Fully Automated Asset, Vulnerability and Patch Mgmt.
2.6 Unified Endpoint Management (UEM) & Mobile Device Management (MDM)
2.1 Device Inventory
2.2 Device Detection and Compliance
2.3 Device Authorization w/ Real Time Inspection
2.4 Remote Access
2.7 Endpoint & Extended Detection & Response (EDR & XDR)

Application & Workload

3.1 Application Inventory
3.3 Software Risk Management
3.2 Software Development & Integration
3.4 Resource Authorization & Integration
3.5 Continuous Monitoring and Ongoing Authorizations

Data

4.1 Data Catalog Risk Alignment
4.2 DoD Enterprise Data Governance
4.4 Data Monitoring & Sensing
4.3 Data Labeling & Tagging
4.5 Data Encryption & Rights Mgmt.
4.6 Data Loss Prevention
4.7 Data Access Control

Network & Environment

5.1 Data Flow Mapping
5.3 Macro Segmentation
5.2 Software Defined Networking
5.4 Micro Segmentation

Automation & Orchestration

6.3 Machine Learning
6.6 API Standardization
6.5 Security Orchestration, Automation, and Response
6.1 PDP & Orchestration
6.7 SOC & Incident Response
6.2 Critical Process Automation
6.4 Artificial Intelligence

Visibility & Analytics

7.1 Log All Traffic
7.3 Common Security & Risk Analytics
7.5 Threat Intelligence Integration
7.4 User & Entity Behavior Analytics (UEBA)
7.2 Security Information and Event Mgmt. (SIEM)
7.6 Automated Dynamic Policies

Note: ZT Capabilities in bold font and displayed on the ZT Target line contain activities spanning both Target and Advanced ZT.

As of June 15th, 2022

UNCLASSIFIED

Summary

- Cybersecurity improvements are not keeping up with adversaries.
- The traditional approach (perimeter security) establishes boundaries and tries to keep intruders from getting into those boundaries.
- Perimeter security is still needed, but this approach alone has not been effective.
- Given the trends of multiple devices, virtual private networks, cloud applications, and remote access, perimeter security is harder than ever.
- This is where Zero Trust comes in.
- Zero Trust
  - Assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned).
  - Moves defenses from static, network-based perimeters to focus on users, assets, and resources.

Zero Trust Learning Assets Being Developed

Three Zero Trust Learning Assets (Foundational, Executive, & Practitioner) to be developed in collaboration with DAU, ZT PfMO, and relevant DoD stakeholders

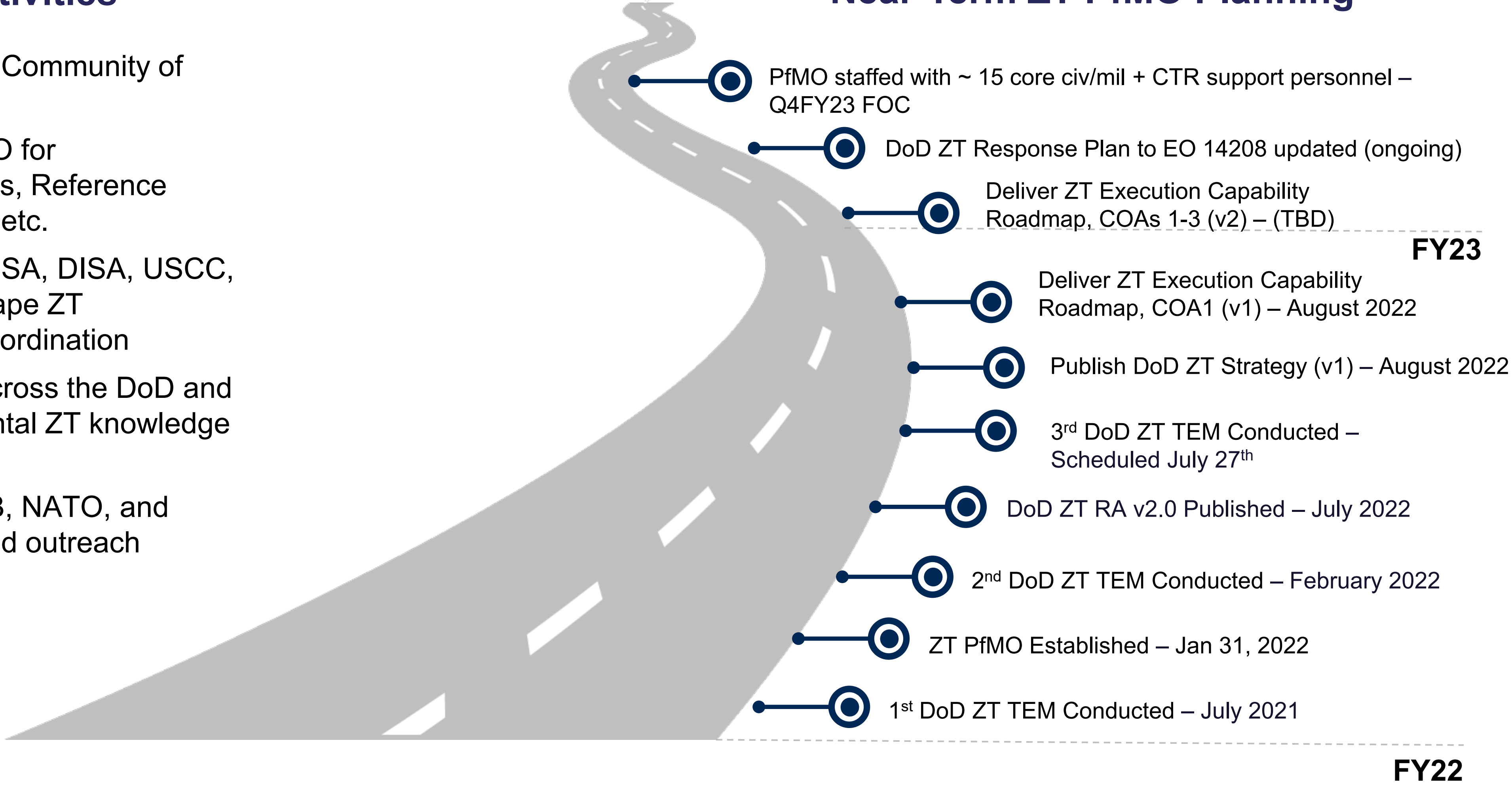
	Foundational	Executive	Practitioner
Target Audience	All DoD workforce needing to learn basic principles of Zero Trust	All DoD leadership with possible oversight over Zero Trust Implementation	DoD cybersecurity professionals planning to implement Zero Trust
Training method	Online learning	Online learning	Online learning and/or instructor led training
Approximate duration	4 to 6 hours	2 hours	6 to 12 hours
Initial completion (Notional)	FY22 Q4/ FY23 Q1	FY 23 Q1	FY23 Q3/Q4
Learning Outcome	Able to explain the foundational elements of DoD ZT implementation	Able to explain essential ZT oversight elements	Able to apply crucial ZT principles for implementation and sustainment

The PfMO is continuing to grow our partnerships and drive strategic initiatives

Ongoing ZT PfMO Activities

- Chair the monthly DoD ZT Community of Interest (COI)
- Collaborate within DoD CIO for Program/Project awareness, Reference Architecture development, etc.
- Facilitate syncs between NSA, DISA, USCC, DMDC and Services to shape ZT implementation & ICAM coordination
- Build stakeholder equity across the DoD and encourage intra-departmental ZT knowledge sharing
- Conduct NIST, CISA, OMB, NATO, and Industry ZT discussions and outreach

Near-Term ZT PfMO Planning



PfMO staffed with ~ 15 core civ/mil + CTR support personnel – Q4FY23 FOC

DoD ZT Response Plan to EO 14208 updated (ongoing)

Deliver ZT Execution Capability Roadmap, COAs 1-3 (v2) – (TBD)

FY23

Deliver ZT Execution Capability Roadmap, COA1 (v1) – August 2022

Publish DoD ZT Strategy (v1) – August 2022

3rd DoD ZT TEM Conducted – Scheduled July 27th

DoD ZT RA v2.0 Published – July 2022

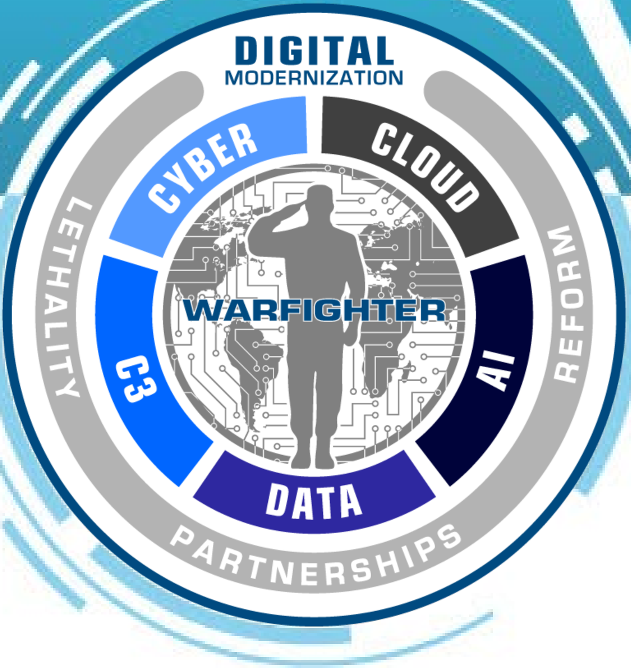
2nd DoD ZT TEM Conducted – February 2022

ZT PfMO Established – Jan 31, 2022

1st DoD ZT TEM Conducted – July 2021

FY22

As of 18 July 2022


DIGITAL
MODERNIZATION
CYBER
CLOUD
C3
WARFIGHTER
AI
DATA
LETHALITY
REFORM
PARTNERSHIPS

Questions?

BACKUPS

Zero Trust Capabilities and Definitions

Capability	Definition
Authentication	The ability to verify the identity of a user, often as a prerequisite to allowing access to a system's resources.
Authorization	The ability to grant or deny device access to data, assets, applications, or services after a prerequisite check.
Privileged Access Management (PAM)	The ability to secure, control, and manage privileged access on critical assets and applications.
Software-Defined Networking (SDN)	The ability for software to provision and manage network configurations on programmable infrastructure such as routers, switches, and firewalls.
Macro Segmentation	The ability to segment traffic on the network using broad categories. These categories can be defined by items such as location, network type, branch, organization and segmentation are typically achieved through the application of additional hardware, SDN or VLANs.
DevSecOps	The ability to develop software in concert with the operations and security teams to maximize the protection, quality integrity of applications while shortening the development life cycle.

Zero Trust Capabilities and Definitions

Capability	Definition
Micro Segmentation	The ability to divide or isolate logical segments on a network at the individual workload or process level. Security settings can be applied to different types of traffic, creating policies that limit network and application flows between workloads to those that are explicitly permitted.
Data Rights Management (DRM)	The ability to align access controls to encryption on a file that prevents unauthorized users or devices from modifying, accessing or distributing, data.
Machine Learning	The ability to study data on security events regarding all aspects of the network, environment, device and application to improve the security, performance, and execution of future policy and risk scoring decisions.
Security, Orchestration, Automation & Response (SOAR)	The ability to automate detection, response and remediation of security incidents. The SOAR capability will integrate with the SIEM for analysis of security events and execute automated workflows in response to threats.

For a full listing of Zero Trust Capabilities and their definitions from the DoD ZT Reference Architecture, please follow the link below and review pages 159 to 162.

https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf