Technology Needs for Accelerating Zero Trust

DoD SAP IT & Cybersecurity Summit

Mr. Randy Resnick
DoD-CIO Director, ZT Portfolio Management Office (ZT PfMO)
25 October 2023

What propelled the DoD to consider ZT

INCIDENTS

SolarWinds | Sep 2019 - Dec 2020

MS Exchange Server | Sep 2019 - Dec 2020

Colonial Pipeline | May 2021

Log4J | Dec 2021

VMWare | May 2022

Persistent attacks | Continuous…

JAN 2019

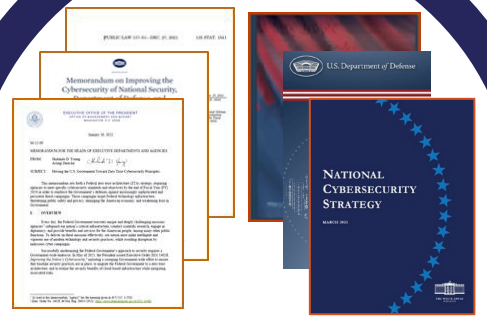
NSA, DISA, USCYBERCOM, and others got together and studied **Zero Trust** in response to continuous attacks on DoD & FedCiv systems evidencing escalation in sophistication.

Prompted SecDef to create "Tiger Team."

The traditional security model of protecting our perimeters is no longer sufficient

DoD ZT Strategy Journey

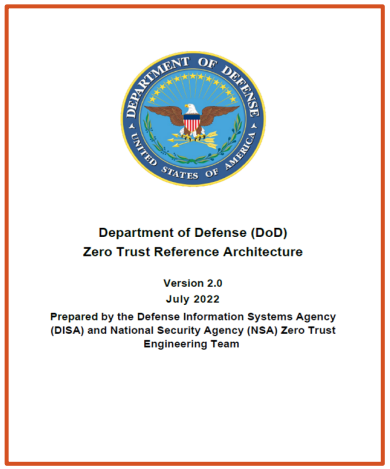
Strategic Guidance



- **EO 14028,** "Improving the Nation's Cybersecurity" (21 May 2021)
- **National Defense Authorization Act for FY 2022** (27 Dec 2021)
- **OMB M-22-09,** "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles" (26 Jan 2022)
- **National Defense Strategy** (22 Mar 2022)
- **National Cybersecurity Strategy** (1 Mar 2023)
- **2023 Cyber Strategy of The Department of Defense** (May 2023)
- **National Cybersecurity Strategy Implementation Plan** (13 Jul 2023)

DoD ZT Reference Architecture

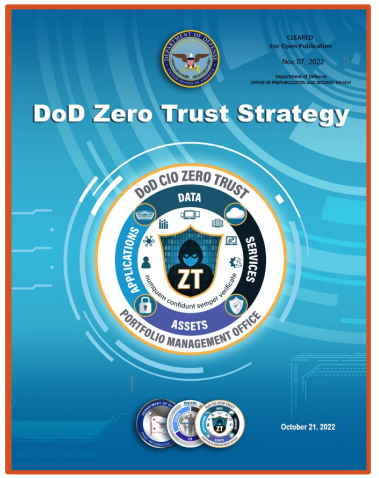
July 2022 v2.0:
The Zero Trust Reference Architecture (v2.0) is the Department's authoritative source that guides and constrains the instantiations of ZT architectures and solutions.


Department of Defense (DoD)
Zero Trust Reference Architecture

Version 2.0
July 2022
Prepared by the Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team

Link HERE

DoD ZT Strategy



21 October 2022 v1.0
Establishes desired outcomes that achieve "ZT Target Level" capabilities and activities across the DoD Information Enterprise for data, assets, applications & services.

Link HERE

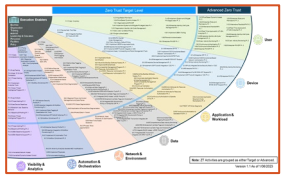
ZT Capabilities & Activities

DoD ZT Capabilities

Link HERE

Capabilities define the outcomes that Components must reach to achieve Target & Advance Levels of Zero Trust.

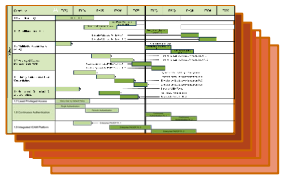
DoD ZT Activities



Link HERE

Activities defined outcome-based metrics to achieve Zero Trust & Advanced Levels of ZT.

ZT Capability and Activity Timelines

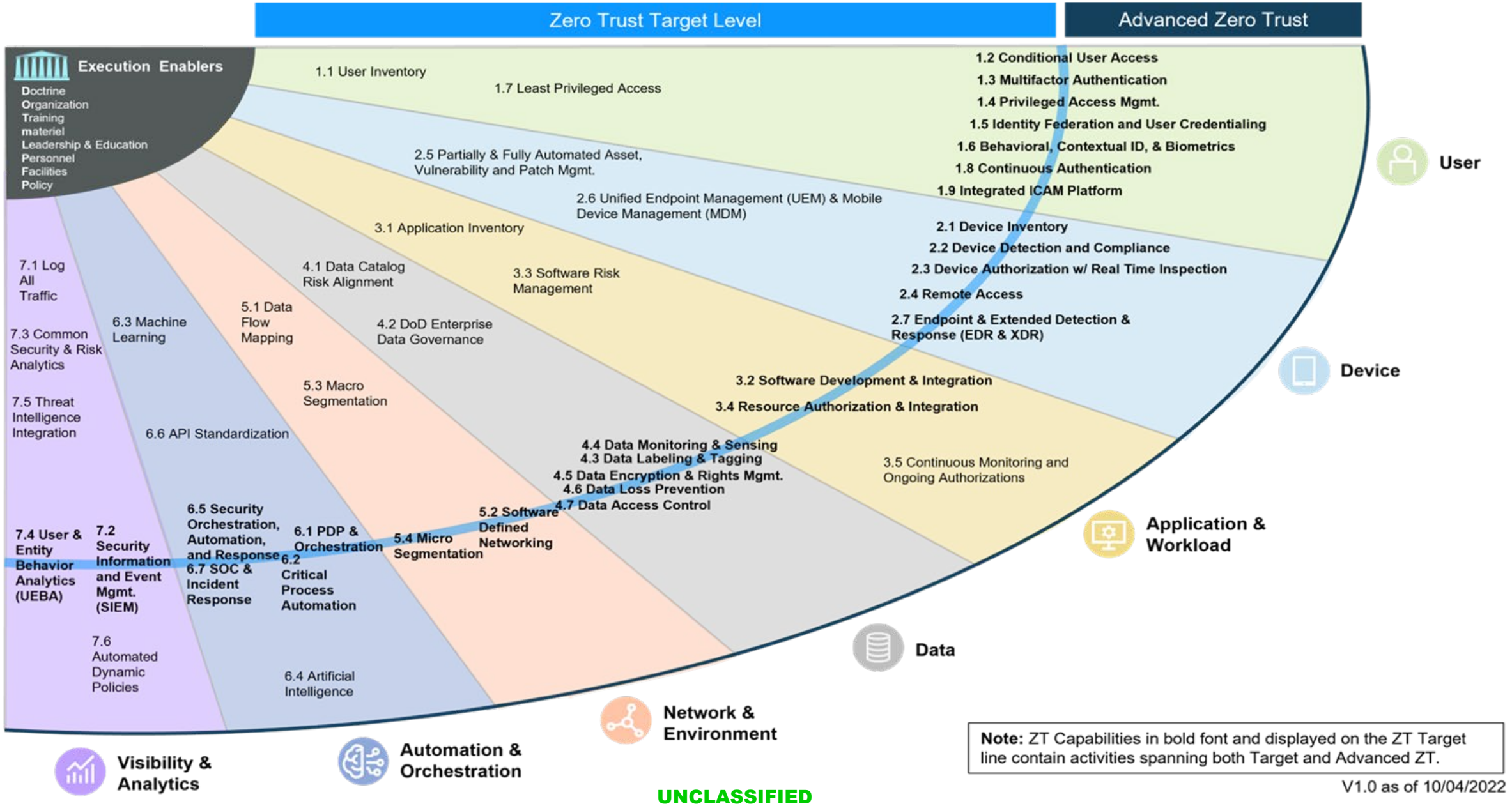


Link HERE

Roadmap depictions show how Zero Trust capabilities will advance across the 7 pillars.

As of 27 Sept 2023

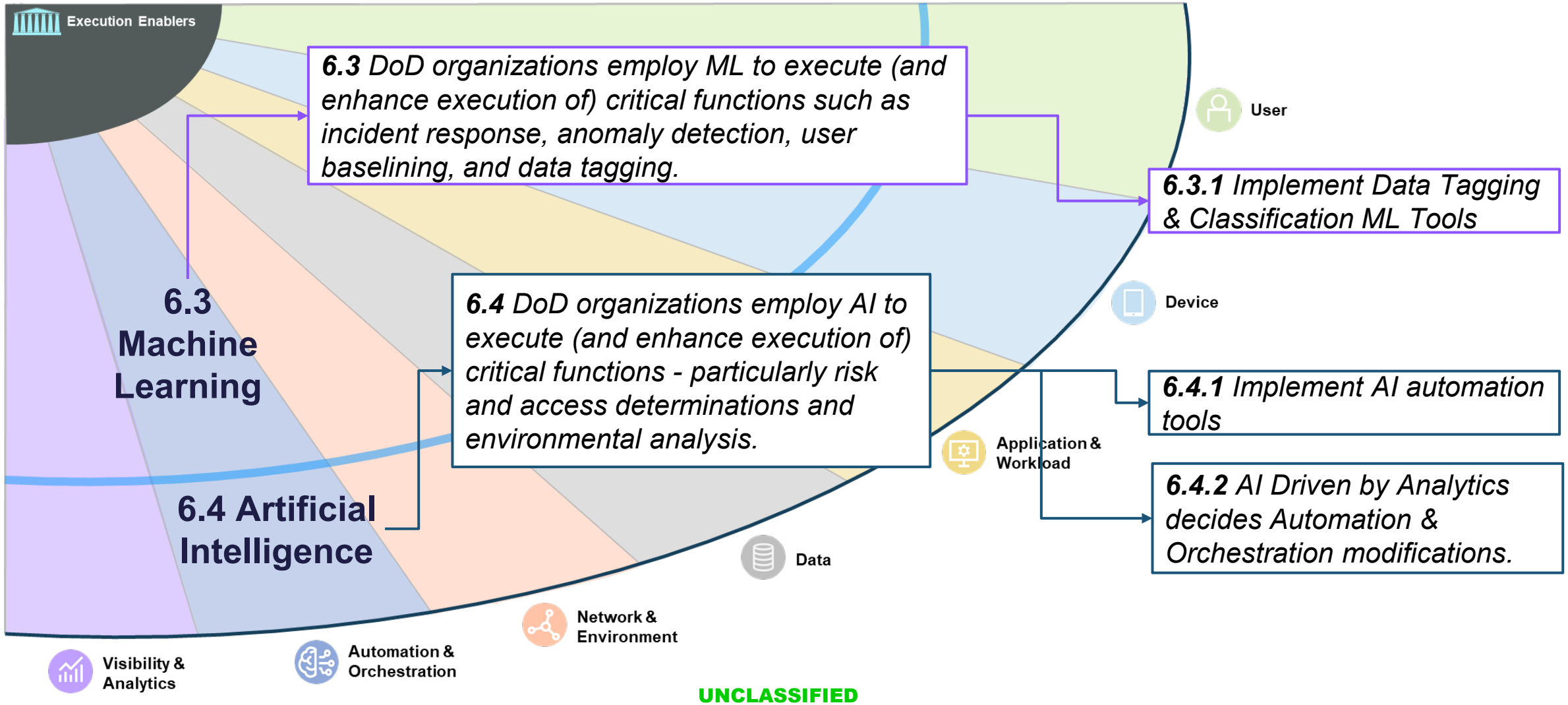
42 ZT *Capabilities* within TARGET + 3 ZT *Capabilities* within ADVANCED = 45 ZT *Capabilities* for Maximum Level ZT (full achievement of ADVANCED Level ZT within DoD)



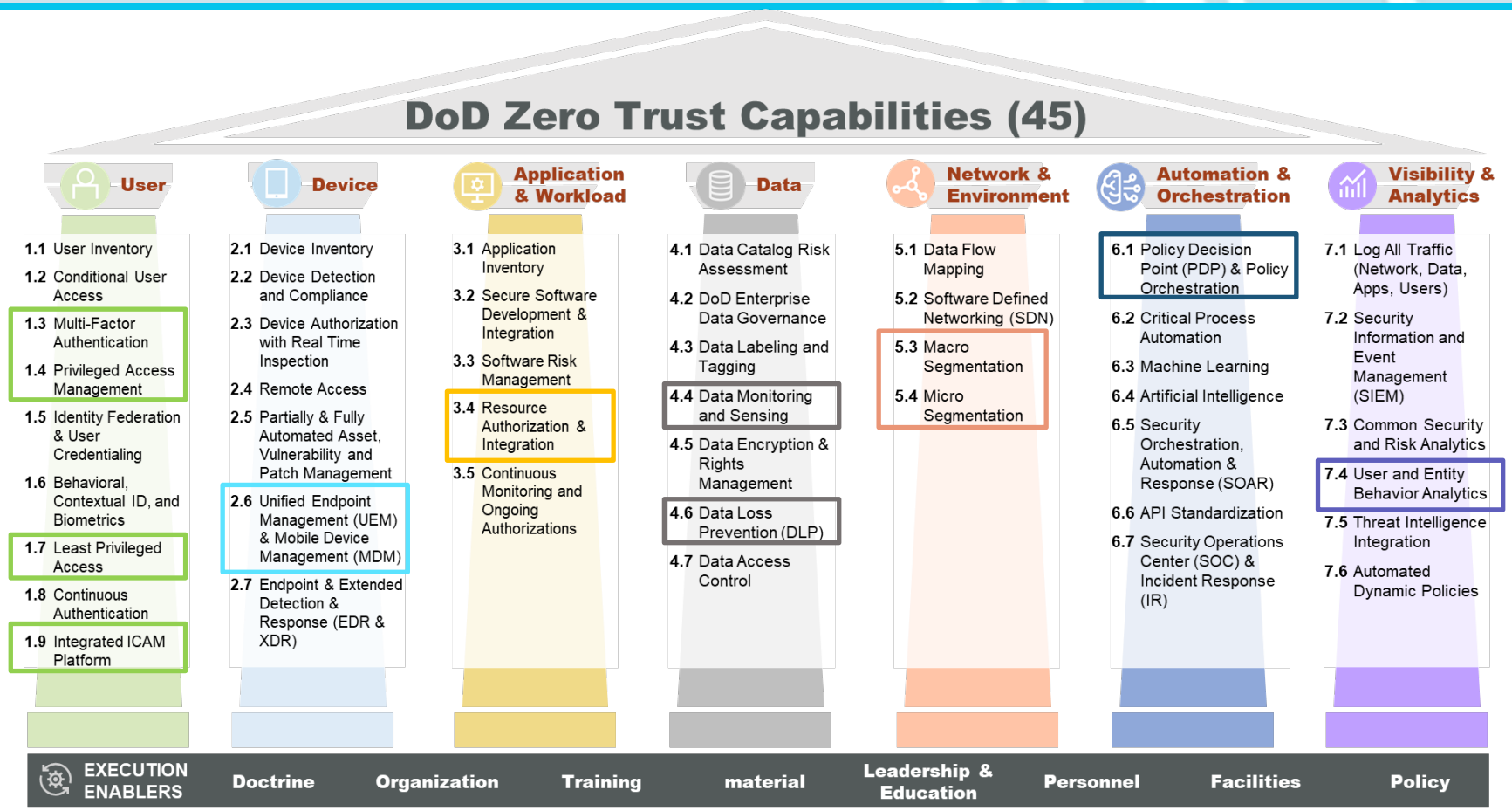
Note: ZT Capabilities in bold font and displayed on the ZT Target line contain activities spanning both Target and Advanced ZT.

V1.0 as of 10/04/2022

DoD Zero Trust Capabilities & Activities: Artificial Intelligence & Machine Learning



Executing key ZT capabilities may reduce occurrence and impact of breaches



Improved user access management, entitlement authorization, data management, and segmentation not only represent critical steps towards a Zero Trust environment but also present near-term opportunity in reducing leaks and cyber attacks

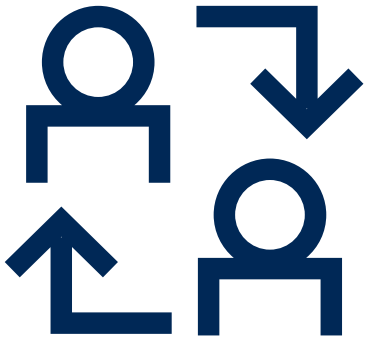
Partnership Information Sharing: Zero Trust Considerations

1. **Coalition Partners: Mission Partner Environment (MPE)**

   Incorporating Zero Trust into information sharing environments will allow for increasing the protection of mission-related data to support the warfighter. Examples:

   - SABRE (Secret & Above Releasable Environment) – USEUCOM, USSOUTHCOM & others.
   - CPN (Collaborative Partner Networks) – USCENTCOM.
   - Indo-PACNET (underlying infrastructure for MPE) – USINDOPACOM.

2. **Services & Combatant Commands (CCMD) Zero Trust Use Cases:**
   - Understanding ZT in the tactical environment.
   - Collected and analyzed mission-focused use cases in advance of Joint Staff sponsored Security Interoperability in Tactical Environment (SITE) 3 Conference in Dec 2023.



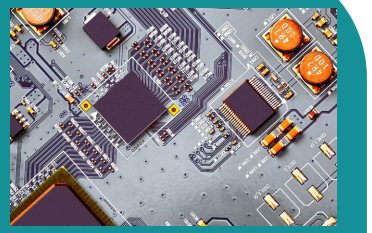
3. **IC, FedCiv, DIB, R&D Labs & Academia Partners Sharing Cross Domain Solutions (CDS) & ZT within an Information Domain.**
   - CDS implementation can be difficult. Transferring sensitive data between security domains requires rigorous security controls to prevent unauthorized access, data leakage, and other security breaches.
   - Zero Trust requires a secure, high-assurance identity fabric.

Success depends on better collaboration among academia, industry, and government

Academia educates and trains younger citizens on cyber security and Zero Trust approaches to **support future research** and studies.

- **AI acceleration and education**

Academia



Industry

Industry is innovating and bringing to the market new approaches, technologies and tools to improve our security posture.

- Advancing ZT solutions and **multi-vendor integrations**

It takes a **"Whole of Community"** approach to **stop** unauthorized lateral movement across our networks and protect our **Vital Data**

Collaborating and **partnering across government agencies is helping** us with **improved interoperability**, sharing better data and lessons learned.

Government

Research Labs

Research Labs are helping us **test the emerging technologies** and tools to ensure that there is minimal impact on existing environments.

Accelerating ZT: Near-Term Milestones

Strategy & Planning

- ***DoD ZT Implementation Plans* submitted** by Military Departments/Components (Oct 23)
- ***DoD ZT Implementation Plans* evaluated** (Nov – Dec 23)
- ***ZT Implementation Plans* briefed to Congress** (Jan 24)

ZT Adoption Enablers

ZT Assessments

- **Baseline** (Infrastructure Modernization) validation
  - DISA Thunderdome / DoD Solutions
- **Commercial Cloud** – Pilots/Purple Team assessments
- **Private Cloud**
  - Commercial Solution
  - Gov't Owned/Operated Solution

ZT Tools & Enhancements

- **ZT Data Tagging (Canonical Controlled Vocabulary – CCV)** Proof of Concept
- **NIST 800-53 ZT Security Controls**, Public release of draft ZT Overlay (Oct/Nov 23)
- **DoD 5G Reference Architecture** (Nov 23)

Partnerships

- **Industry:**
  - Defense Industrial Base Cybersecurity (DIB CS) Engagement
- **Cross-Gov Collaboration (IC, FedCiv, DoD, DHS CISA, others):**
  - Weekly coordination & collaboration, bi-weekly ZT Syncs, Monthly Working Groups, Quarterly Technical Exchanges, and more
- **Training & Education:**
  - ZT Introductory Courses (JKO): ZT Awareness, ZT for Executives, Strategy & Guidance Course
  - Intermediate Course: ZT Implementation
  - ZT Advanced Training: Practitioner and Engineering Workshops

Training Details: https://www.dau.edu/zerotrust


Q
A

Thank You!

DoD ZT PfMO Mailbox: osd.pentagon.dod-cio.mbx.dcio-cs-zt@mail.mil