

2026
DEFENSE HEALTH INFORMATION
TECHNOLOGY SYMPOSIUM

AUGUST 11-13, 2026
HYATT REGENCY NEW ORLEANS
NEW ORLEANS, LA

Military Health Zero Trust Evolution: Achieving Target State & Beyond

Ms. Megan Morales, DHA Zero Trust Program Manager



Agenda

1 Zero Trust and the Defense Health Agency (DHA) Overview

2 Purple Team Assessment Results and Lessons Learned

3 Pressing into Advanced Level Zero Trust (ZT)

4 Paving the Way Ahead for Operational Technology (OT)

5 Q&A

Speaker Introduction



Megan Morales, Zero Trust Program Manager

Engineering, Solutions Architecture
& IT Business Analytics Division (ESA-BAD)
Defense Health Agency

Megan Morales is the Zero Trust Program Manager for the Defense Health Agency, bringing 20 years of experience in project management, leadership, cybersecurity, and acquisition. A U.S. Air Force veteran and former Registered Respiratory Therapist, she has led key healthcare IT initiatives across DHA and the VA. She holds a B.A.S. and M.B.A. in Project Management.

Learning Objectives



Zero Trust Purple Team Assessment Results

Outline the unified framework that combines security operations, architecture, and real-world testing to make Zero Trust measurable.



Purple Team Assessment: Lessons Learned

Describe the lessons learned and security gaps identified from the recent purple team assessment.

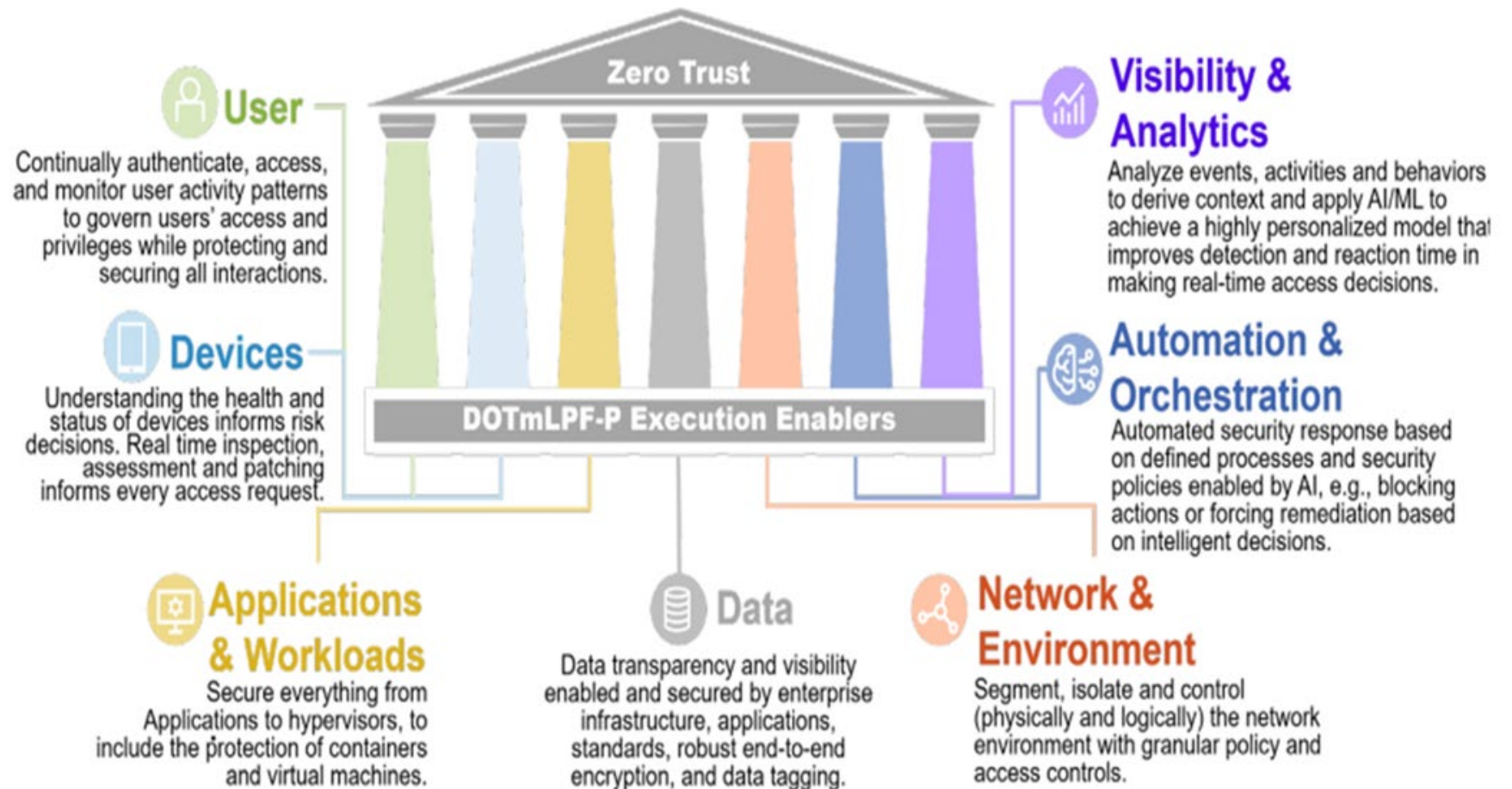


Future State Implementation

Plan strategies for shifting Zero Trust implementation towards advanced-level outcomes for Information Technology (IT), and future state for Operational Technology (OT).

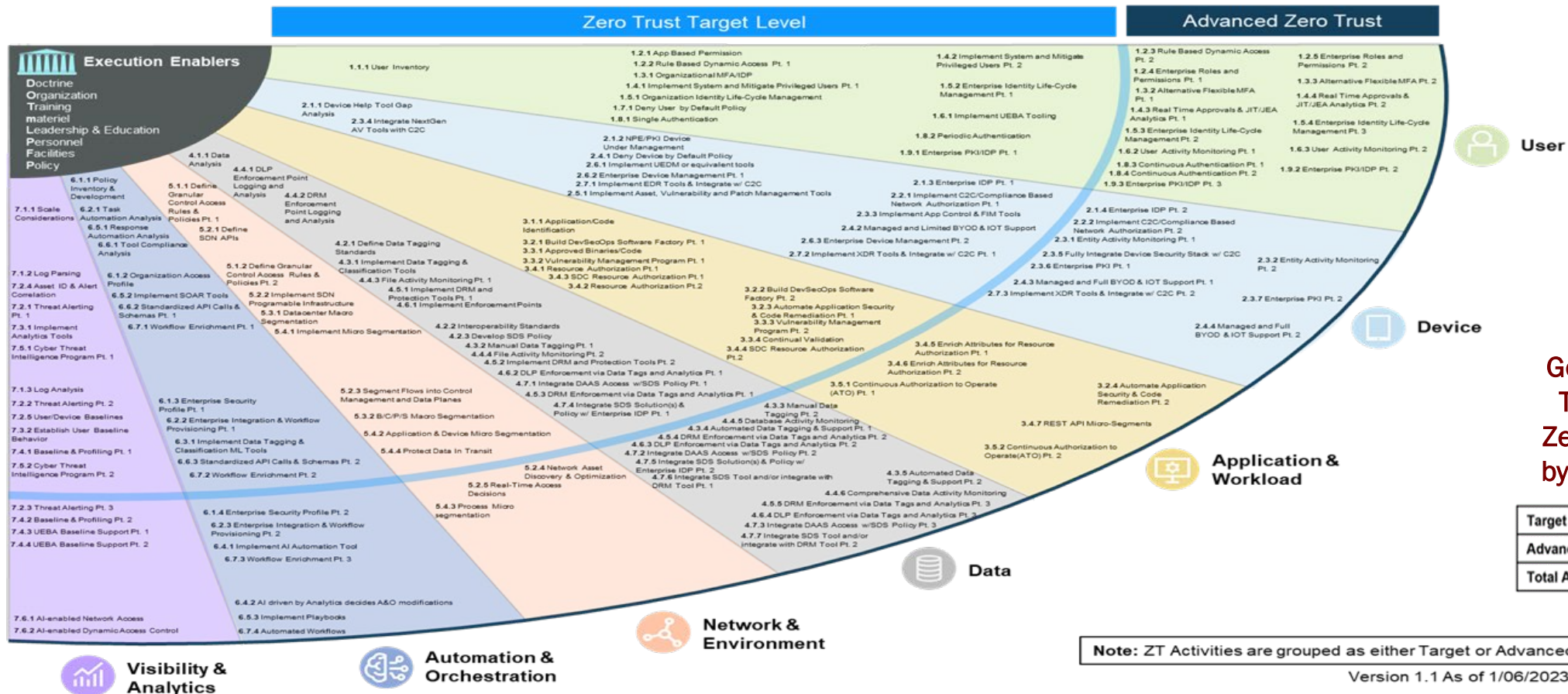
Zero Trust Pillar Integration

The validated Zero Trust approach stresses integration across all seven pillars. The goal is to establish multiple policy checkpoints and automatically approve or deny requests based on the user's behavior patterns.



Department of War (DoW) Zero Trust Strategy Fan Chart

91 ZT Activities within TARGET + **61 ZT Activities** within ADVANCED
= **152 ZT Activities** for Maximum Level ZT (full achievement of ADVANCED Level)



Goal - achieve
Target Level
Zero Trust (91)
by end of FY27

Target Activities:	91
Advanced Activities:	61
Total Activities:	152

Note: ZT Activities are grouped as either Target or Advanced.

Version 1.1 As of 1/06/2023

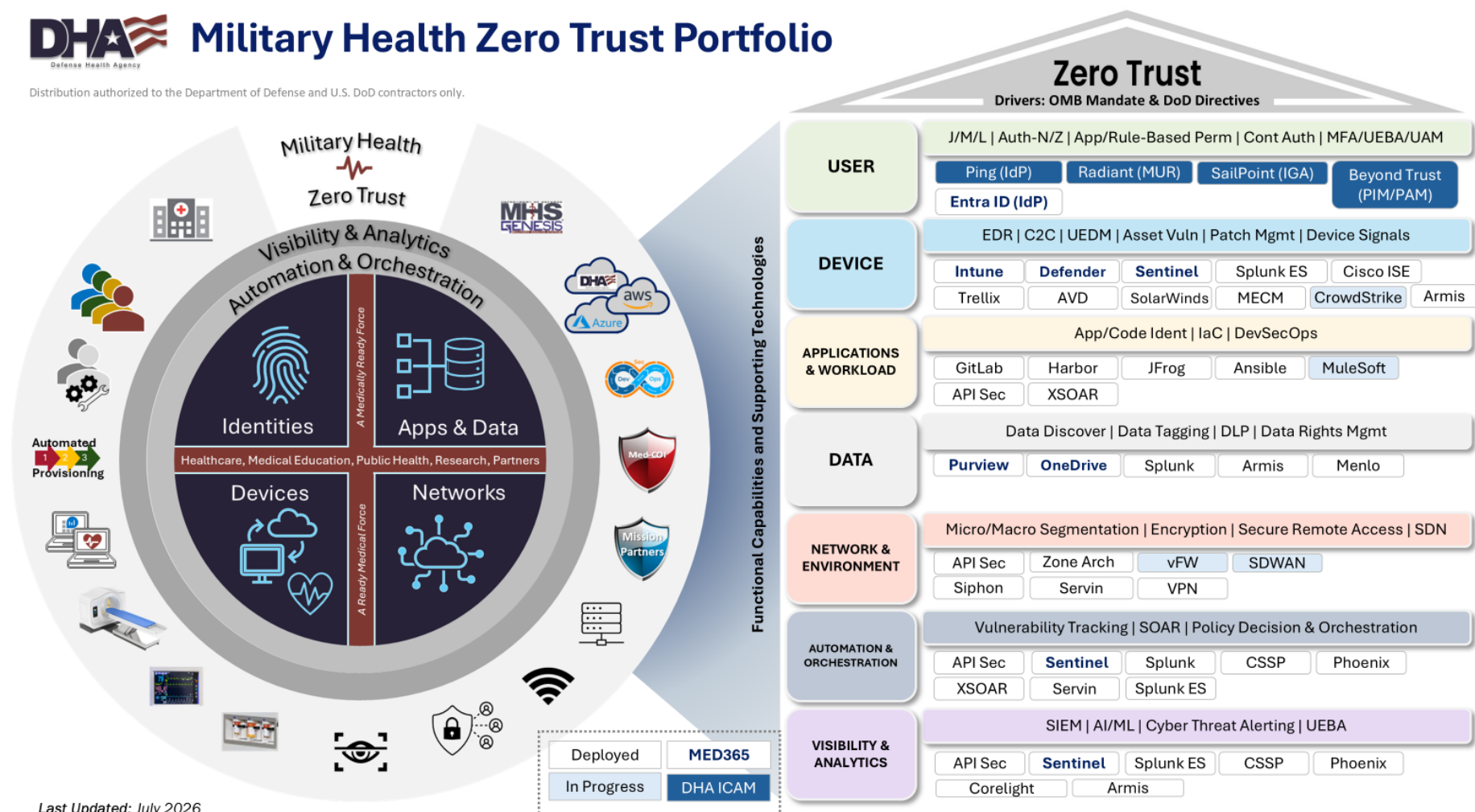
Zero Trust Capability Overview

DHA's Zero Trust strategy is represented through an evolving, integrated set of capabilities that are designed to manage the risks and challenges associated with the Military Health mission.



Military Health Zero Trust Portfolio

Distribution authorized to the Department of Defense and U.S. DoD contractors only.



Last Updated: July 2026

Zero Trust Purple Team Assessment Overview



MISSION

Validate DHA's Zero Trust implementation against the DoW CIO Zero Trust Architecture Framework and Zero Trust Acceptance Criteria (ZTAC) using an ***assumed compromise*** approach.



ASSESSMENT PARTNERS

NIWC Purple Team, NIWC CSSP, DHA, DoW CIO, ZT PfMO, MITRE



ASSESSMENT DATES

11 – 22 May 2026



On-site in Charleston, SC

ASSESSMENT SCOPE



ENVIRONMENT

Global DHA Enterprise (MTFs, AWS, Azure, AVD, VPN)



THREAT PERSPECTIVES

Insider • Nearsider • Outsider



ASSESSMENT METHOD

Purple Team (Red Team + Blue Team)
Threat-based with cooperative intent



FOCUS

Validate Zero Trust capabilities and operational effectiveness



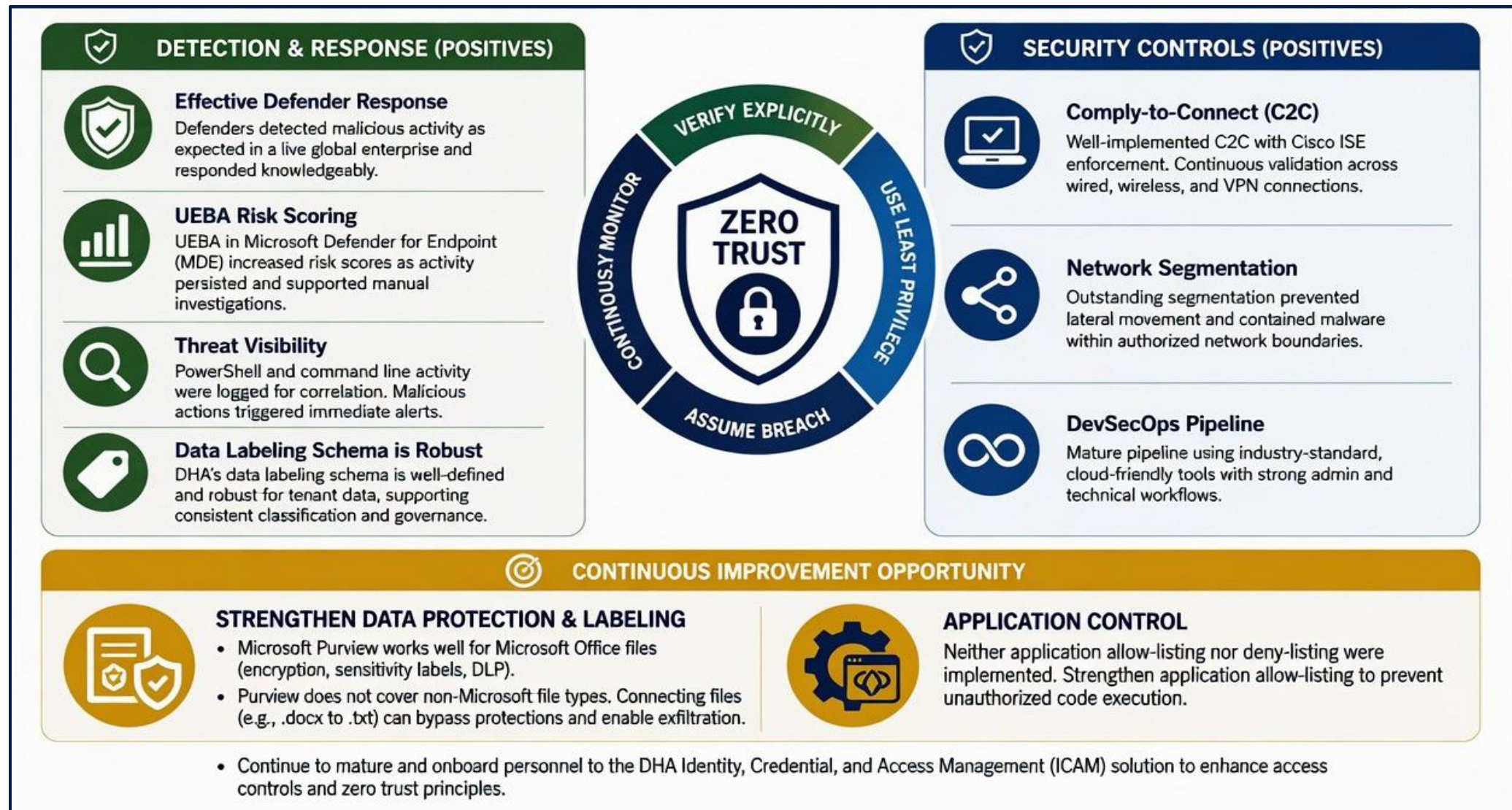
EVALUATED



152

**ZERO TRUST
ACTIVITIES
ASSESSED**

Observations – Insights from the Zero Trust Assessment



Lessons Learned



BLUF: DHA demonstrated advanced ZT capabilities on a live network, but DoW-wide policy gaps and data tagging guidance remain critical dependencies.



OPERATIONAL SUCCESSES



Live Network Execution

Achieved "Target" & "Advanced" ZT activities on a live, global network (exceeding isolated dev environment norms).



Micro-segmentation

Highly praised by assessors for demonstrated network defense capabilities.



Tactical Synergy

Co-locating the CSSP alongside the Red Team proved crucial to the assessment's success.



POLICY & STRATEGY



Strategic Inheritance

DHA published an overarching ZT Policy Memo adopting enterprise capabilities to bridge gaps.



Policy Gap Analysis

DoW ZT PfMO is finalizing an analysis to address the lack of 1-to-1 administrative policy mapping across components.



CRITICAL NEEDS



Data Tagging

DoW requires definitive guidance regarding strategic direction and future integration.



Common DoW Failure

Application allow-listing is lacking. Must enforce signature-based baselines to permit only valid applications.

Pressing into Advanced Level ZT



BLUF: Based on the preliminary Purple Team assessment results of your advanced activities, DHA has successfully built a robust policy and application defense foundation. To achieve a true "Advanced" state, the next phase must transition from isolated, manual tools to fully integrated, real-time automated enforcement.



WHAT WE DID RIGHT (OPERATIONAL SUCCESSES)



PKI & Policy Foundation:

Successfully established global policies for Enterprise PKI (device/server certificate issuance) and expanded manual data-tagging guidelines.



Modern DevSecOps & App Security:

Demonstrated high maturity in automated security remediation, API micro-segmentation, and resource authorization within your development pipelines.



AI Threat Detection:

Successfully implemented AI automation tools (such as Microsoft Sentinel Fusion) to flag complex threat patterns.



WHAT WE NEED TO FOCUS ON (FUTURE PRIORITIES)

Focus Area	Core Action Required
 Dynamic Access Control	Move from rigid, static RBAC to real-time, risk-based access decisions driven by behavioral telemetry.
 Active UEBA Integration	Feed risk scores from UEBA and AI/ML monitoring directly into access-control engines to block threats instantly.
 Automated Identity Lifecycle	Replace manual processes with automated Just-in-Time (JIT) / Just-Enough-Access (JEA) credentials.
 Full Data Monitoring	Expand active monitoring beyond file systems to include comprehensive database activity monitoring.



KEY TAKEAWAYS



STRONG FOUNDATION ESTABLISHED

DHA has built a solid foundation in policy and application defense with demonstrated maturity in several key areas.



TRANSITION REQUIRED

The path to "Advanced" requires moving from manual, siloed tools to integrated, automated enforcement.

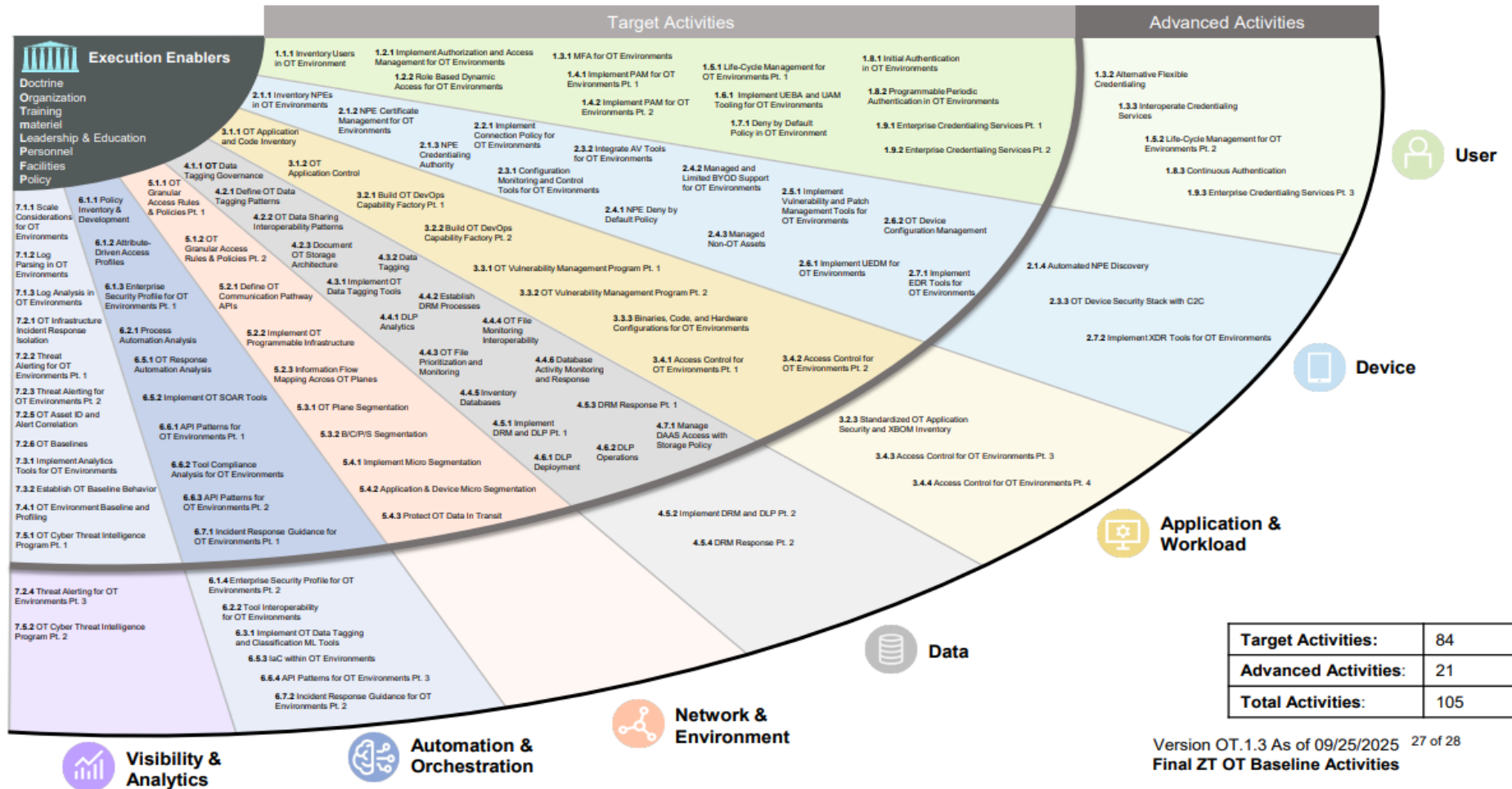


FOCUS ON AUTOMATION

Real-time automation, integration, and continuous monitoring are critical to achieving true Zero Trust maturity.

Paving the Way Ahead for Operational Technology (OT)

APPENDIX B: Zero Trust Fan Chart for Operational Technologies



Securing DHA's Horizon: OT Strategic Next Steps

DHA Zone Architecture (ZA)

- Refine the ZA to isolate and explicitly define unique OT components on our network

MHS - Facility Related Control Systems (FRCS) and Medical Devices

- Conduct gap analysis
- Pull in stakeholders outside of J6
- Understand our FRCS and their reference architectures, such as the Purdue Model

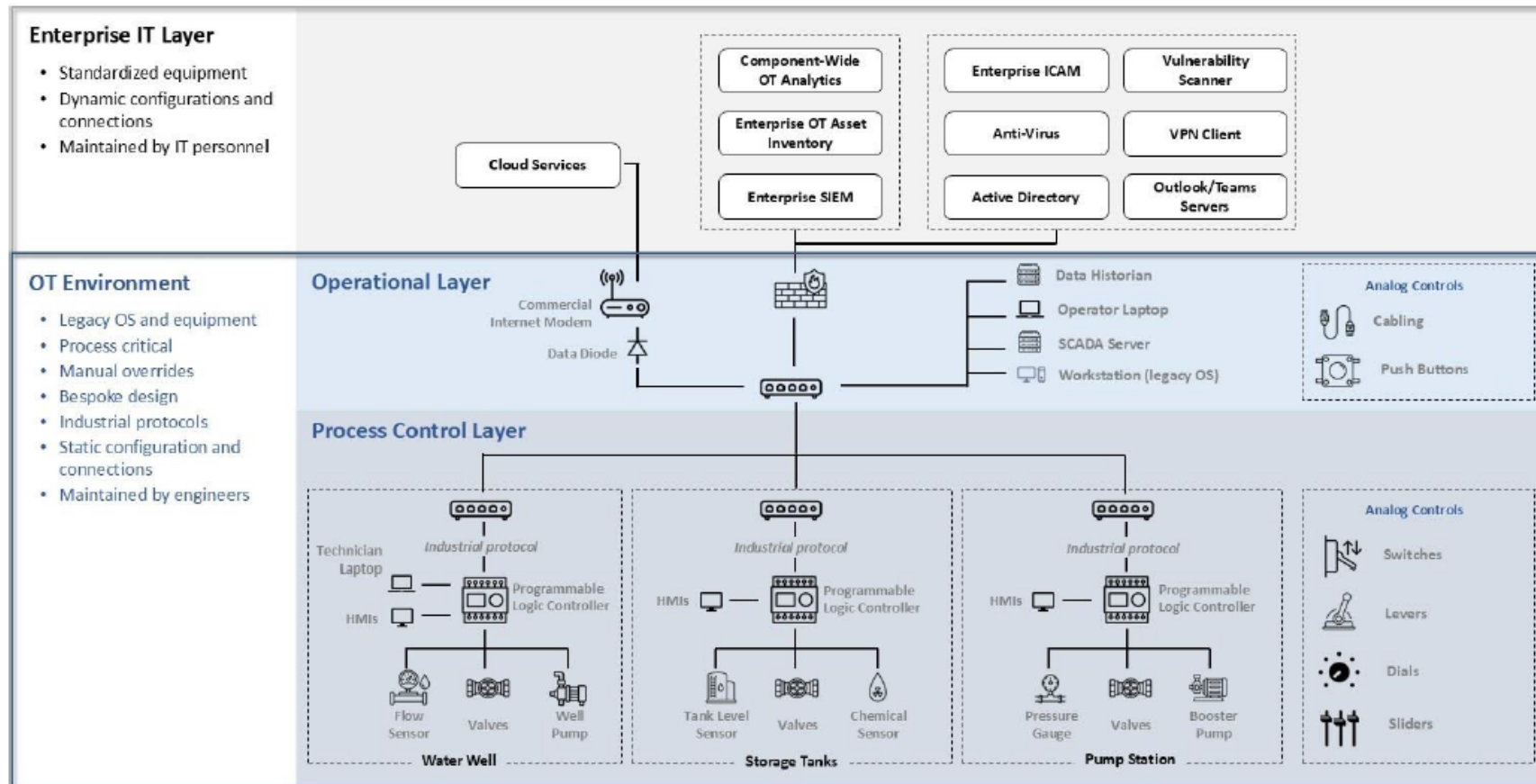
DoW CIO Zero Trust Portfolio Management Office (PfMO) Collaboration

- Tracking tentative 2032 deadline to meet OT
- In regular discussion with DoW CIO Zero Trust PfMO to shape the future of OT within the Med-COI
- DHA is one of the largest components collaborating with the PfMO

Securing DHA's Horizon: OT Strategic Next Steps (cont'd)

APPENDIX C: Distinction Between Enterprise IT and OT Environments

September 2025



[DoW Executive Summary – Zero Trust for Operational Technology, Nov. 18, 2025](#)

WarU Zero Trust Training



DHA Zero Trust Strategy Course

The DHA J-6 Academy and the Warfighting Acquisition University (WarU) have joined forces to bring you a groundbreaking training event: the new, all-in-one DHA Zero Trust Strategy course!

We have fused our Operational and Advanced trainings into a single, power-packed 16-hour curriculum from foundational principles to advanced strategic implementation.

WarU Professor: Mr. George Alves

- Full Course (16 hours): Go all in and earn 16 continuous learning points (CLPs).
- Part 1 Only (Operational Focus): Join us for the fundamentals and earn 4 CLPs.
- Part 2 Only (Advanced Strategy): Dive deep into advanced concepts and earn 12 CLPs

This also encompasses the JKO training that corresponds to the employee's position:

Level 1

- DOD-US003 - DoD Zero Trust Awareness Course (1hr)
- DOD-US005 - Zero Trust for DoD Executives Course (1hr)
- DOD-US006 - Zero Trust Strategy and Guidance (1hr)

Level 2

- DOD-US007 - DoD Zero Trust Implementation (1hr)

Advertised on J6 Academy site & CIO WG, but please reach out to DHA ZT PMO if you are interested in registering!



[Zero Trust 101 Workshop](#)

[DoW CIO PfMO Training Resources](#)

Contacts

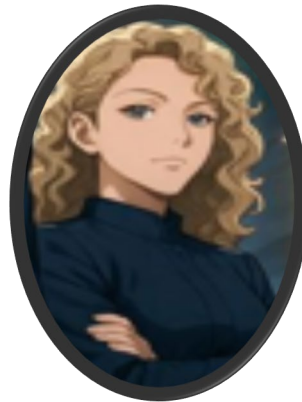
Ms. Megan Morales
Zero Trust Program Manager

✉ Megan.a.morales.civ@health.mil



Ms. Chelsi Vanderpol
Zero Trust Project Management

✉ Chelsi.n.Vanderpol.ctr@health.mil



Ms. Erica Vega
Zero Trust Project Management

✉ Erica.l.vega2.ctr@health.mil





**2026
DEFENSE HEALTH INFORMATION
TECHNOLOGY SYMPOSIUM**

AUGUST 11-13, 2026
HYATT REGENCY NEW ORLEANS
NEW ORLEANS, LA

Thank You!



UNCLASSIFIED