DAU

Zero Trust – Leading the Journey

Zero Trust Industry Day 2024
Carnegie Mellon University, Software Engineering Institute
May 2024

Tim Denman
Cybersecurity Learning Director
Defense Acquisition University (DAU)

What Propelled the DoD to Consider Zero Trust?

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."

Source: DoD Zero Trust "Way Ahead" – Randy Resnick

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

MAY 12, 2021

- **To keep pace with today’s dynamic and increasingly sophisticated cyber threat environment**, the Federal Government must take decisive steps to modernize its approach to cybersecurity.
- The Federal Government must adopt security best practices; **advance toward Zero Trust Architecture**; accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS); centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks; and invest in both technology and personnel to match these modernization goals.

Our culture of cybersecurity must be based on Zero Trust.

Honorable Mr. John Sherman, DoD CIO
DoD Zero Trust Symposium, April 2, 2024

DoD Zero Trust Strategy *(Introduction – October 2022)*

- Our adversaries are in our networks, exfiltrating our data, and exploiting the Department's users.
- <u>Defending DoD networks with high-powered and ever-more sophisticated perimeter defenses is no longer sufficient for achieving cyber resiliency and securing our information enterprise that spans geographic borders.</u>
- **To meet these challenges, the DoD <u>requires</u> an enhanced cybersecurity framework built upon Zero Trust principles that must be adopted across the Department, enterprise-wide, as quickly as possible.**
- **This urgency means that our colleagues, our warfighters, and every member of DoD must adopt a Zero Trust mindset,** regardless of whether they work in technology or cybersecurity or the Human Resource department.

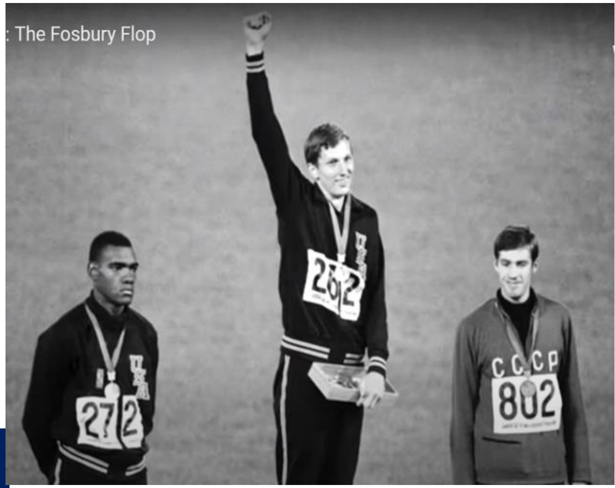
Zero Trust – Cybersecurity's Fosbury Flop

"When the environment around a task changes, a new and better way to do things is usually possible."

James Clear, Olympic Medalist Dick Fosbury and the Power of Being Unconventional, https://jamesclear.com/dick-fosbury

- *In 1968 Dick Fosbury first used the Flop method and won gold.*
- *Since 1976, all gold medalists have used the Fosbury Flop.*

The Fosbury Flop does not replace the High Jump, it enables it.



- *In Oct 2022 the DoD ZT Strategy outlined ZT implementation.*
- *All DoD organizations must adopt target level ZT by the end of 2027.*

Zero Trust does not replace cybersecurity, it enables it.

The Changing Environment

The Computing Environment

- **Mainframe**
  - Centralized computing/ central data repository
  - Remote access was rare
- **Virtual private networks**
  - Provides secure access to a remote computer over an insecure medium (the internet)
  - Confidentiality at the packet level via encryption
- **Cloud computing / distributed environment**
  - Delivery of computing services over the Internet ("the cloud")
  - Multiple software components often run as a single system

> ***"The Federal Government must adopt security best practices; advance toward Zero Trust Architecture; accelerate movement to secure cloud services, …"*** *EO 14028, May 2021*

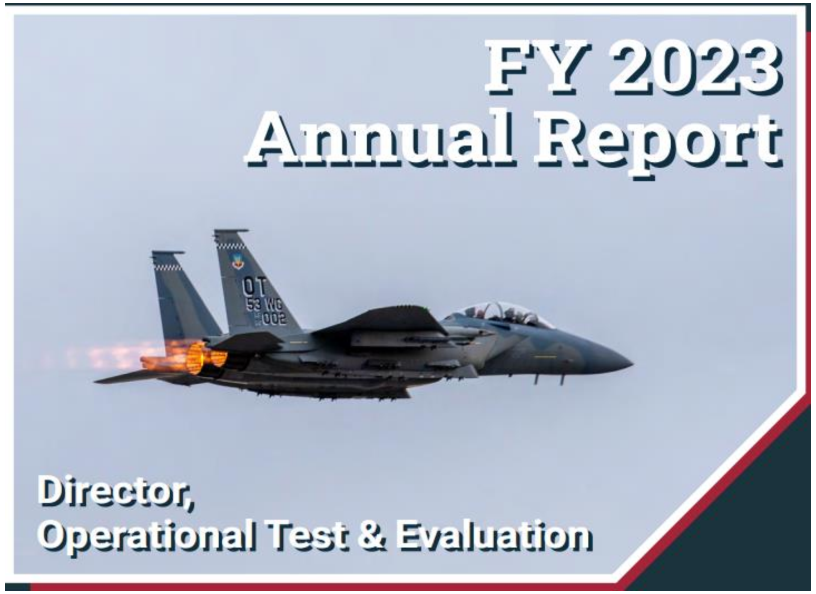
Zero Trust Growth in a Changing Environment

- The global zero trust security market size is projected to grow from $31.45 billion in 2023 to $95.22 billion by 2030, at a CAGR of 17.1%
- With the widespread shift to remote work during the COVID-19 pandemic, organizations faced new challenges in securing distributed networks and endpoints
- Moreover, organizations accelerated their migration to cloud services during the pandemic, which led to a surge in cyber threats and attacks.
- ZT principles helped organizations secure endpoints by implementing robust controls, continuous monitoring, and dynamic access policies based on user behavior.

https://www.fortunebusinessinsights.com/zero-trust-security-market-108832

The 2023 DOT&E Annual Report *(January 2024)*

- As DoD cyber defenses continue to improve, the offensive capabilities of potential adversaries are escalating
- Many DoD cyber defenses and warfighter missions remain vulnerable to offensive cyber capabilities of potential adversaries.
- **DoD is implementing Zero Trust best practices, which are imperative to defend against advanced cyberattacks**
- **The Cyber Assessment Program (CAP) has observed positive outcomes because of the adoption of various combinations of the tenets and pillars of Zero Trust, as defined by the DoD CIO.**


FY 2023
Annual Report

Director,
Operational Test & Evaluation

Making it Happen

Zero trust is not going to be unobtainium in the department. We're going to make this happen by 2027 from all of our networks and again, preventing lateral movement through microsegmentation, fine-grained access endpoint management in a way we've not done, and assuming an adversary is already on our network and then proceeding apace.

We cannot fail on this …

Honorable Mr. John Sherman, DoD CIO, May 4, 2023

Not a Single Product

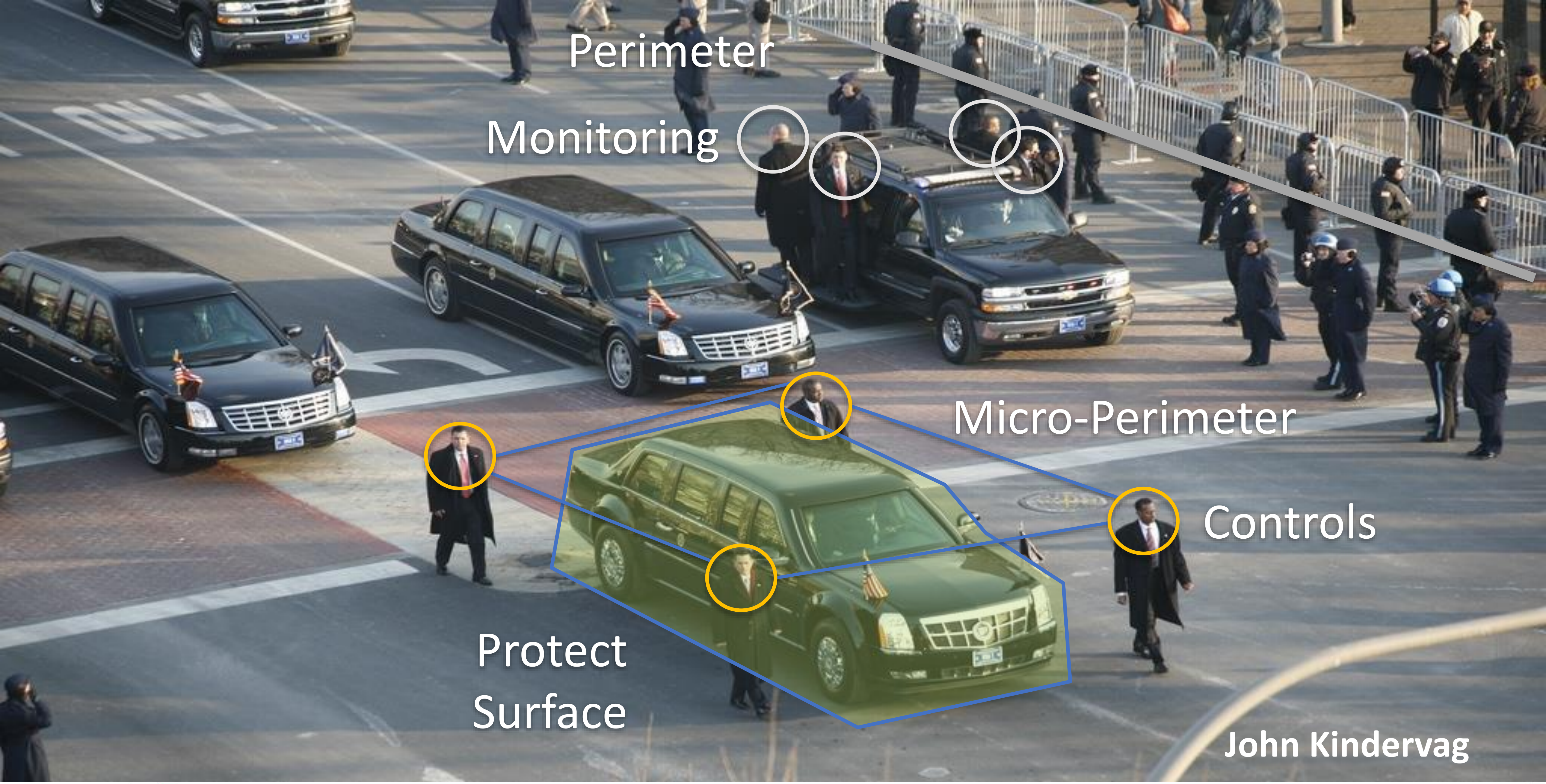
Zero Trust is not a capability or device you buy, rather it is a security framework, an architectural approach, and a methodology to prevent malicious actors from accessing our most critical assets and reducing existing attack surfaces.

Randy Resnick, DoD CIO Zero Trust Portfolio Management Office

The Underlying Strategy Behind Zero Trust

- The foundational principle of the Zero Trust model is that nothing is implicitly trusted, and everything is continuously and fully verified.
- This applies to people or actors, systems, networks, and services both inside and outside the security perimeter.
- There are no trusted insiders, only verified insiders. It assumes a breach and a hostile environment.

The Zero Trust transformation will not happen overnight. It requires an overarching strategy, a focused implementation plan, and buy-in at all levels of the organization. It is a cultural and paradigm shift at its very core.


Perimeter
Monitoring
Micro-Perimeter
Controls
Protect Surface
John Kindervag

Zero Trust Implementation Case Study

US Army Cyber Center of Excellence

- Zero Trust (ZT) can be implemented using fielded hardware and software
- Three-phase approach:
  - Build the architecture
  - Implement ZT design concepts in detection mode
  - Move to prevention mode
- Utilized 4 Red team engagements to prove successful implementation
- Organization had never defeated a red team during training events prior to ZT implementation

Zero Trust in an Army Tactical Environment – CW3 Benjamin Koontz, April 2023

Training Vision

DoD Zero Trust Strategy, Oct. 2022

Goal 1: Zero Trust Cultural Adoption. *A Zero Trust security framework and mindset that guides the design, development, integration, and deployment of information technology across the DoD Zero Trust Ecosystem.*

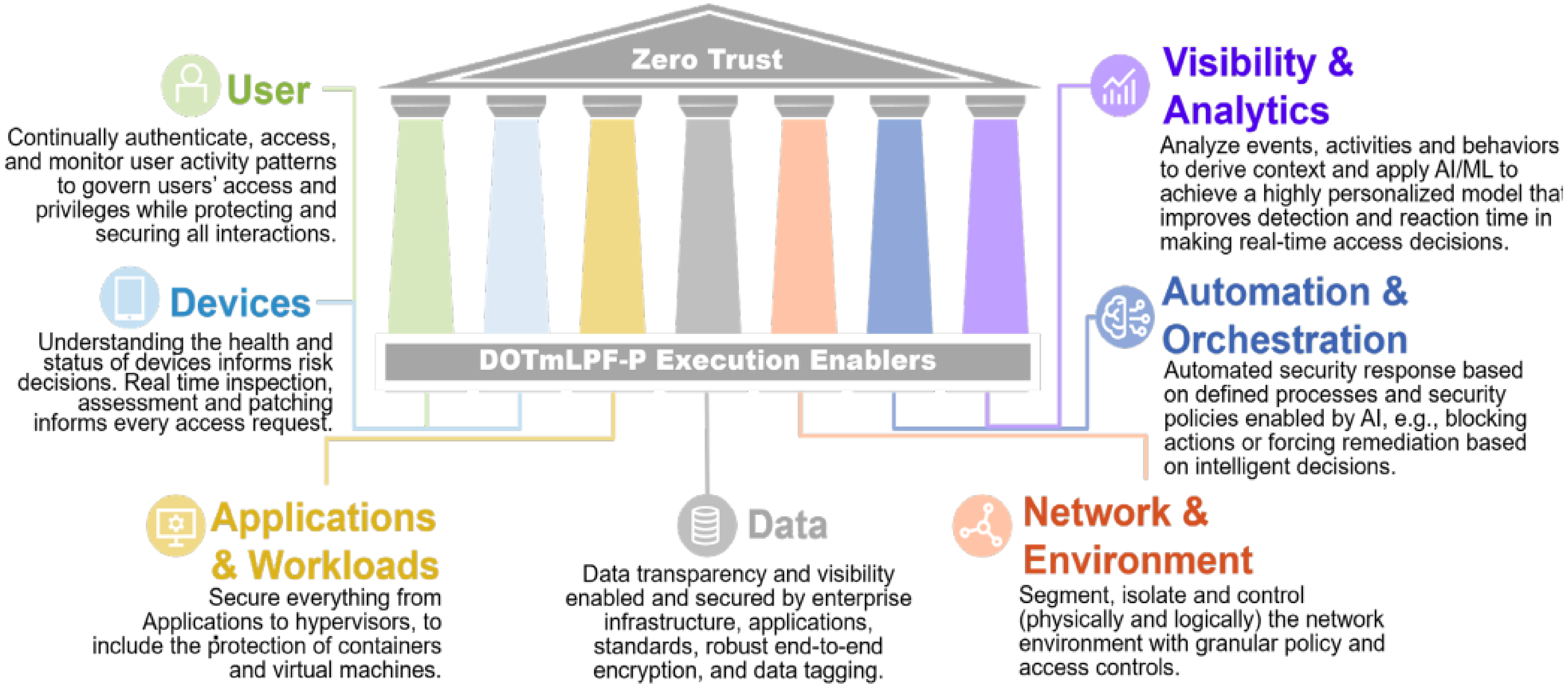
- All DoD personnel are aware, understand, commit to, and trained to embrace a ZT mindset and culture and support integration of ZT technologies in their environments …

Culture Eats Strategy for Breakfast

Work Rules!: Insights From Inside Google That Will Transform How You Live and Lead, **Laszlo Bock**

DoD Zero Trust Pillars

Figure 3. DoD Zero Trust Pillars



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

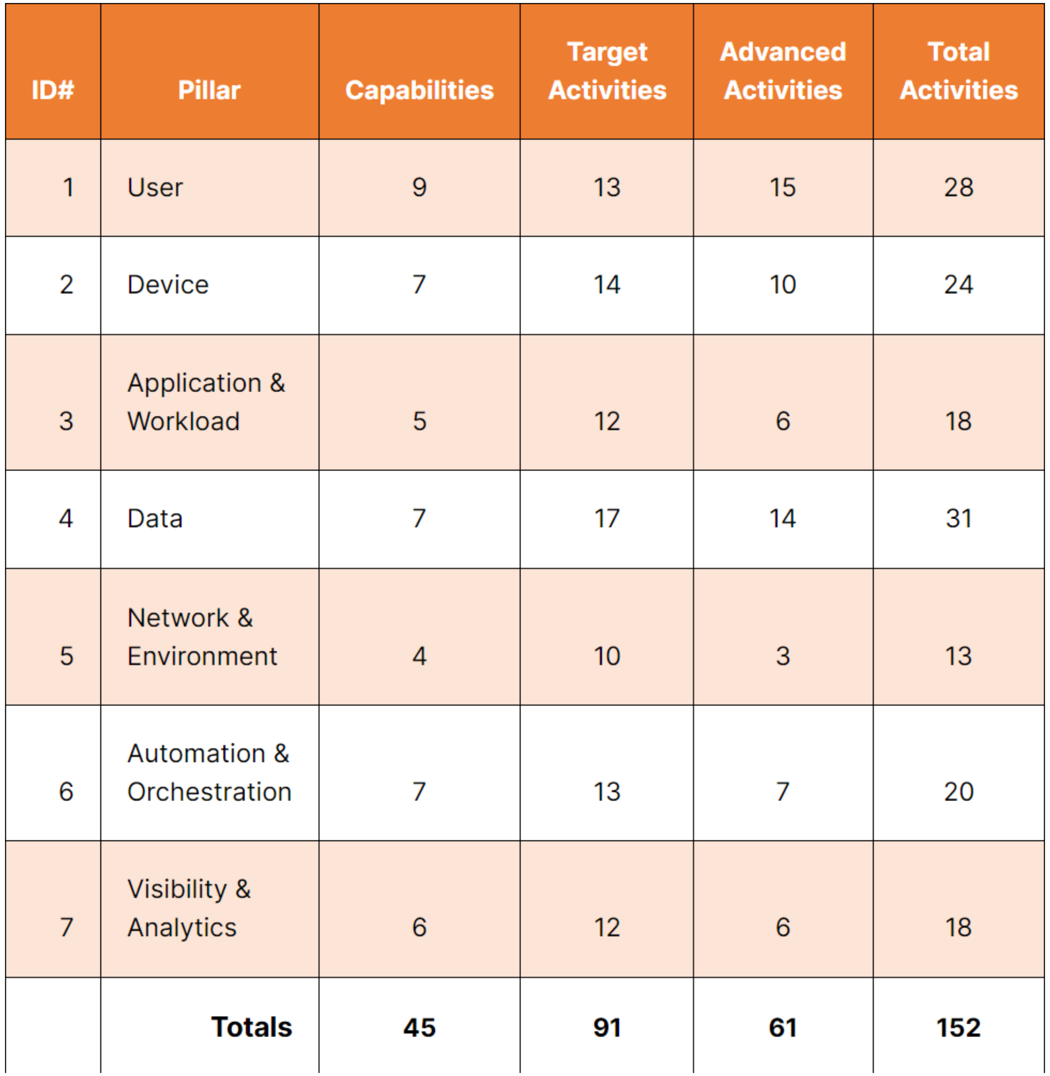
Automated security response based on defined processes and security policies enabled by AI, e.g., blocking actions or forcing remediation based on intelligent decisions.

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.

(DoD Zero Trust Strategy, p. 10)

Summary of Capabilities & Activities



ID#	Pillar	Capabilities	Target Activities	Advanced Activities	Total Activities
1	User	9	13	15	28
2	Device	7	14	10	24
3	Application & Workload	5	12	6	18
4	Data	7	17	14	31
5	Network & Environment	4	10	3	13
6	Automation & Orchestration	7	13	7	20
7	Visibility & Analytics	6	12	6	18
	Totals	**45**	**91**	**61**	**152**

Extending from the 45 Zero Trust capabilities are a total of 152 target and advanced activities. In the DoD, these activities determine whether your system is Zero Trust or not. There are 91 activities required to achieve target level Zero Trust. The goal is for all DoD systems to achieve Target Level on or before the end of FY 2027. There are 61 additional activities that are required to reach the Advanced Level of Zero Trust. The 91 target activities will be your implementation focus. The chart below summarizes the number of target and advanced activities in each pillar.

Implementation may not cover all 152 activities or even the 91 Target activities, but it should span all seven pillars.

Executing Zero Trust – The COAs

COURSE OF ACTION (COA)	OVERVIEW	POTENTIAL SOLUTION	CURRENT STATUS
COA 1: Legacy Infrastucture	Components augment existing infrastructure to meet Target and Advance level ZT.	Additional licensing and/or hardware configuration changes will likely be required.	ZT integrated solutions proposed by Vendors will be assessed and validated in Q2 & Q3 of FY24.
COA 2: Commercial Cloud	Components can leverage Cloud Service offerings from Cloud Service Providers if they meet Target or Advanced level ZT.	Components can leverage Joint Warfighting Cloud Capability (JWCC) or other vehicles if AWS, Google, Microsoft, and/or Oracle meet Target or Advanced level ZT.	All four CSPs will complete their ZT assessments NLT Q3 of FY24.
COA 3: Single Ecosystem	A private Cloud completely owned, controlled and operated by a single organization (i.e.: DoD) or a Component.	Component tier, mid-tier, edge tier or DDIL environments can be addressed.	ZT integrated olutions propose d by Vendors will be assessed and validated in Q2 & Q3 of FY24.

Components may choose to leverage any or all of the COAs, depending on their unique mission requirements.

The DoD Zero Trust Portfolio Management Office (ZT PfMO)

The ZT PfMO is the central point in the DoD to coordinate, synchronize, and advance the DoD Enterprise to a ZT architecture, modernizing the Department's ability to defend against malicious threat actors in cyberspace.

Mission

Provide strategic guidance, direct alignment of efforts, and prioritize resources to accelerate Zero Trust adoption across the DoD

DoD CIO ZERO TRUST
DATA
SERVICES
ASSETS
APPLICATIONS
ZT
numquam confidunt semper verificate
PORTFOLIO MANAGEMENT OFFICE

Vision

Directive authority for Zero Trust across the DoD Information Enterprise

Zero Trust Portfolio Management Office was created in January of 2022.

Links to Current Zero Trust Training

Zero Trust Level 1 - Online courses - Joint Knowledge Online

- ***Zero Trust Awareness***
  - *https://jkosupport.jten.mil/html/COI.xhtml?course_prefix=DOD&course_number=-US003*
- ***Zero Trust for Executives***
  - *https://jkosupport.jten.mil/html/COI.xhtml?course_prefix=DOD&course_number=-US005*
- ***Zero Trust Strategy and Guidance***
  - *https://jkosupport.jten.mil/html/COI.xhtml?course_prefix=DOD&course_number=-US006*

Zero Trust Level 2 – Webinars and Online course

- ***Zero Trust Webinar (3rd Thursday /month – Next webinar May 16)***
  - *https://www.dau.edu/events/zero-trust-transforming-cybersecurity-implementing-best-practices-and-lessons-learned*
- ***Zero Trust Implementation (Online course)***
  - *https://jkosupport.jten.mil/html/COI.xhtml?course_prefix=DOD&course_number=-US007*

Level 3 ZeroTrust Workshops

- ***ZT Engineering Workshop (2 Day in person event at Johns Hopkins, Laurel, MD – July 16-17)***
  - *https://rise.articulate.com/share/LqctSKWz4-P0TWiurDA-vtNnnFHRfuFl*
- ***ZT Practitioner Workshop (2 Days - Virtual, in-person, and by request – Mar 27, Ft Belvoir, Apr 16, Virtual)***
  - *https://rise.articulate.com/share/l2lWLnBx_ue9iOoLi10wz_Wv1XbehRif*

DAU Zero Trust Media Channel
https://media.dau.edu/channel/CyberSecurity/62925431

DoD ZT Symposium Day 1
https://media.dau.edu/playlist/dedicated/62925431/1_rba8a3vf/1_ipd4aaet

DoD ZT Symposium Day 2
https://media.dau.edu/playlist/dedicated/62970351/1_x60u42f2/1_3dvhj8zn

ZT Engineering Workshop, Laurel, MD
Johns Hopkins Applied Physics Lab (APL)
(In-person only)
July 16-17 (By invitation)

Zero Trust Summary

To highlight the **DoD's Zero Trust Journey** given the reality that the enemy is ALREADY IN OUR NETWORKS and continues exfiltration of our precious data.

Zero Trust implementation is imperative, given that the traditional security model of protecting our perimeters is no longer sufficient.

Leadership must lead the way!

Zero Trust cannot be accomplished through a single application, technology, or vendor. Cultural change is critical.

Email: Zerotrust@dau.edu