AI Powered Defense: Outsmarting Cyber Threats

Jason Proctor
Advisory Systems Engineer, Cyber Resilience & Compliance

DELL Technologies
Data Protection Solutions
Global Technology Office

HUBER & ASSOCIATES
ENCRYPTED: A CYBERSECURITY SYMPOSIUM
TUESDAY, JUNE 18
TEAMHUBER.COM/BESTOFCYBER


CYBER
is the new
DISASTER

What is Cyber Resilience?

"The ability to **anticipate**, **withstand**, **recover from** & **adapt** to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment."

SP800-160 V2 R1

- Developing Cyber-Resilient Systems: A Systems Security Engineering Approach

Cyber Attack

A cyber attack is an attempt by cybercriminals, hackers or other digital adversaries to access a computer network or system, usually for the purpose of altering, stealing, destroying or exposing information

Malware

- Ransomware
- Fileless Malware
- Spyware
- Adware
- Trojan
- Worms
- Rootkits
- Mobile Malware
- Exploits
- Scareware
- Keylogger
- Botnet
- MALSPAM

DNS Tunneling

Code Injection Attacks

- SQL Injection
- Cross-Site Scripting (XSS)
- Malvertising

Phishing

- Spear Phishing
- Whaling
- SMiShing
- Vishing

Insider Threats

Supply Chain Attacks

Spoofing

- Domain Spoofing
- Email Spoofing
- ARP Spoofing

Denial-of-Service (DoS) Attacks

IoT-Based Attacks

Identity-Based Attacks

- Kerberoasting
- Man-in-the-Middle (MITM) Attack
- Pash-the-Hash Attack
- Golden Ticket Attack
- Silver Ticket Attack
- Credential Harvesting
- Credential Stuffing
- Password Spraying
- Brute Force Attacks
- Downgrade Attacks

DELL Technologies

10 Most Common Types of Cyber Attacks Today - CrowdStrike

COMPLEX PROBLEMS

require

COMPLETE SOLUTIONS

DELL Technologies

Steps to Cyber Resilience

Assessment & Planning	Layered Defense	Visibility & Continuous Improvement
• Define the “risk” • Framework • Education & Awareness	• Attack Surface Management • Detection & Response • Recovery	• Testing & Validation • Incident Response & Recovery • Security Dashboard & Reporting

Project Fort Zero

The US DOD developed, engineered, and invested over five years, to architect an **Advanced Zero Trust** system using their best engineers.

This is the foundation of our solution.

Dell will deliver…

- Capabilities integration & orchestration completed by Dell
- Repeatable ZTA blueprint
- Executive order compliance for **federally validated** solution

Dell brings…

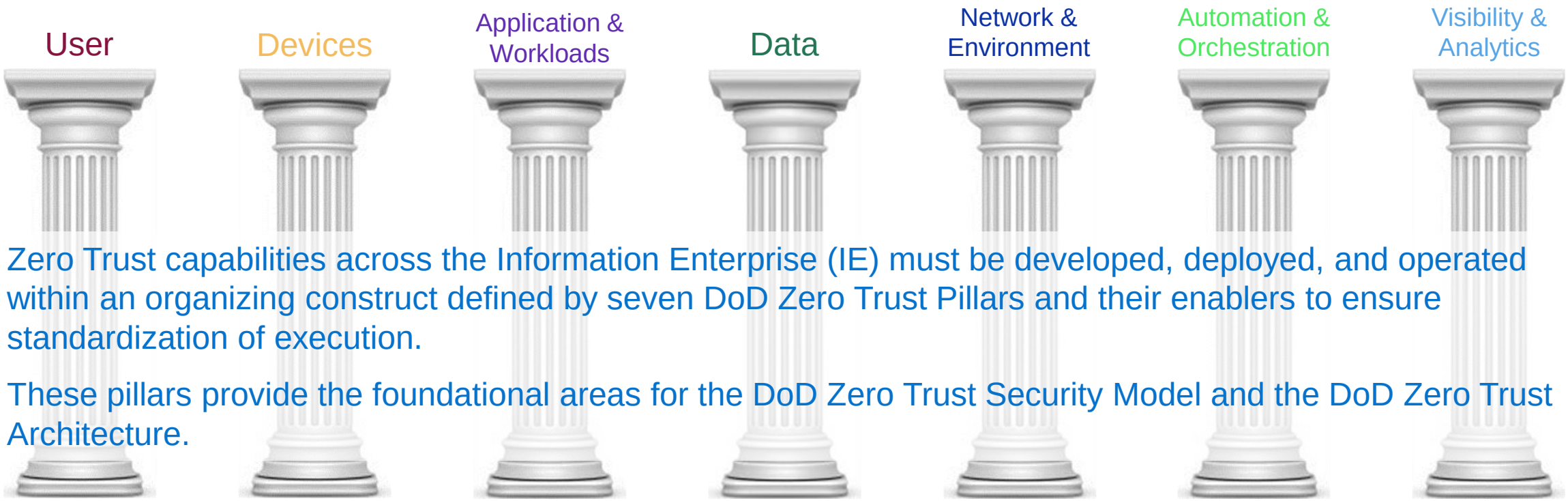
- Dedicated investment
- Leading partner ecosystem
- Advanced maturity ZT
- Hybrid configurations
- Available to all industries
- Center of Excellence
- Ongoing engagement

DELL Technologies

DoD Zero Trust Strategy Goals & Objectives

	Zero Trust Cultural Adoption	DoD Information Systems Secured & Defended	Technology Acceleration	Zero Trust Enablement
GOALS	• A Zero Trust security framework and mindset that guides the design, development, integration, and deployment of information technology across the DoD Zero Trust Ecosystem	• DoD cybersecurity practices incorporate and operationalize Zero Trust to achieve enterprise resilience in DoD information systems	• Zero Trust-based technologies deploy at a pace equal to or exceeding industry advancements to remain ahead of the changing threat environment	• DoD Zero Trust execution integrates with Department-level and Component-level processes resulting in seamless and coordinated ZT execution
IMPACT	• A cybersecurity-minded culture & workforce that embraces ZT • Increased collaboration & productivity • Increased commitment to cybersecurity	• Secured communications at all operational levels • Improved systems & performance • Interoperable & secured data • Automated cyber & AI operations	• Continually updated & advanced ZT enabled IT • Reduced silos • Simplified architecture • Efficient data management	• Enhanced operations & support performance • Consistent, aligned & effectively resourced ZT supporting functions • Speed of ZT acquisition-to-deployed capability
OBJECTIVES	• **Commitment** • **Outreach** • **Awareness** • **Workforce** • **Training**	• **User** • **Device** • **Applications & Workloads** • **Data** • **Network & Environment** • **Automation & Orchestration** • **Visibility & Analytics**	• **Capabilities** • **Architecture** • **Interoperability** • **Ideation / Innovation**	• **Policy** • **Planning** • **Programming** • **Funding** • **Acquisition** • **Performance** • **Zero Trust Portfolio Management Office (PfMO)**

DoD Zero Trust Pillars



Zero Trust capabilities across the Information Enterprise (IE) must be developed, deployed, and operated within an organizing construct defined by seven DoD Zero Trust Pillars and their enablers to ensure standardization of execution.

These pillars provide the foundational areas for the DoD Zero Trust Security Model and the DoD Zero Trust Architecture.

DoD Zero Trust Strategy (p 10)

DoD Zero Trust Capabilities

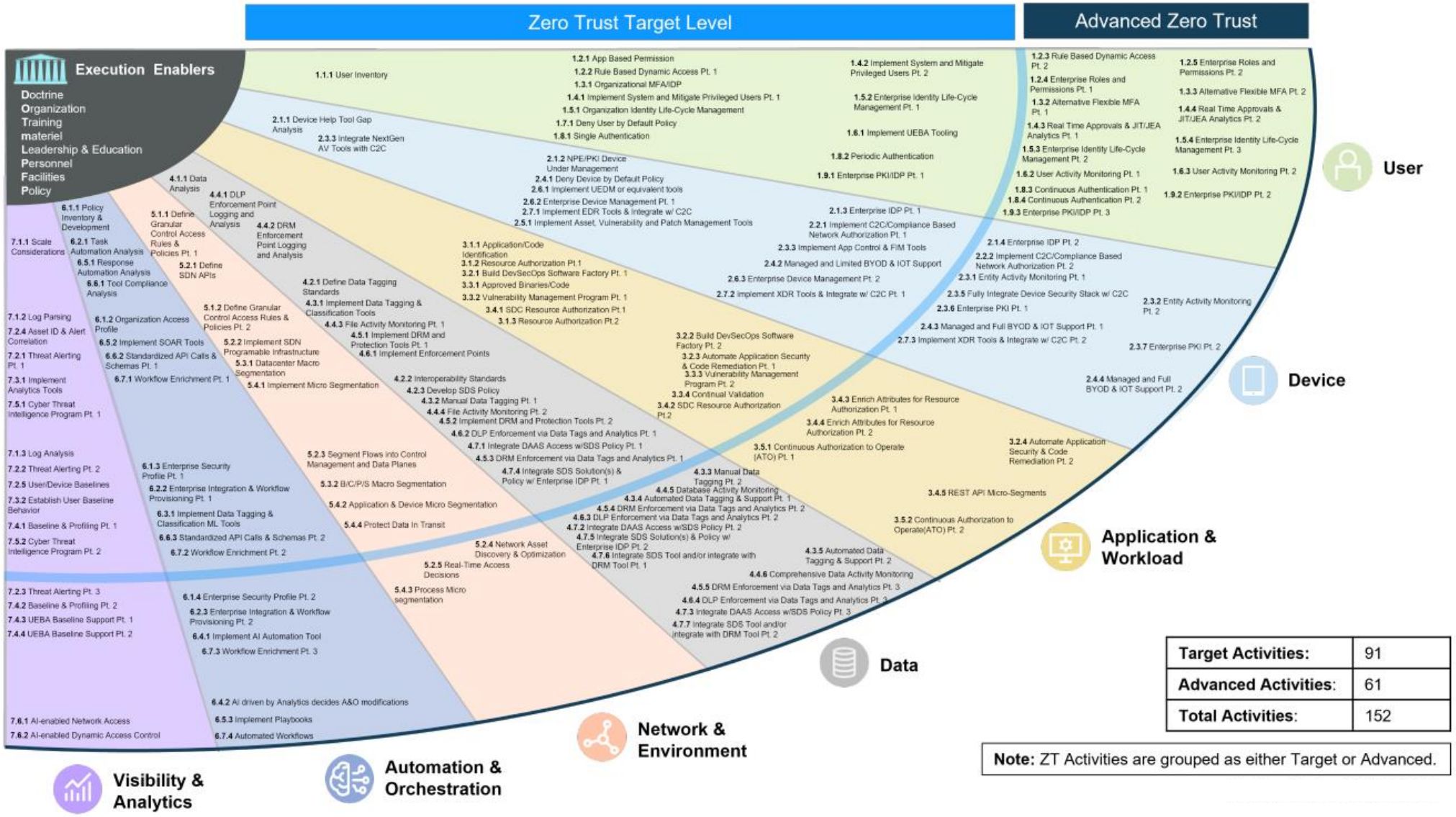
	Target		Target & Advanced		Advanced
User	**1.1** User Inventory	**1.7** Least Privileged Access	**1.2** Conditional User Access **1.3** Multifactor Authentication **1.4** Privileged Access Mgmt. **1.5** Identity Federation and User Credentialing	**1.6** Behavioral, Contextual ID, & Biometrics **1.8** 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** Secure 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	**4.3** Data Labeling & Tagging **4.4** Data Monitoring & Sensing **4.5** Data Encryption & Rights Management	**4.6** Data Loss Prevention (DLP) **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	**6.1** Policy Decision Point (PDP) & Policy Orchestration **6.2** Critical Process Automation	**6.5** Security Orchestration, Automation & Response (SOAR) **6.7** Security Operation Center (SOC) & Incident Response (IR)	**6.4** Artificial Intelligence
Visibility & Analytics	**7.1** Log All Traffic **7.3** Common Security & Risk Analytics **7.5** Threat Intelligence Integration		**7.2** Security Information and Event Mgmt. (SIEM)	**7.4** User & Entity Behavior Analytics (UEBA)	**7.6** Automated Dynamic Policies

EXECUTION ENABLERS	Doctrine	Organization	Training	materiel	Leadership & Education	Personnel	Facilities	Policy

DELL Technologies

DoD Zero Trust Strategy

DoD Zero Trust Activities



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

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

DoD Zero Trust Strategy

What the Experts are Saying

Good enough is not good enough

"Offline backups (or backups that are verified as **inaccessible to attackers with full control of production IT**) must be available for all critical systems, data and infrastructure, including core IT infrastructure such as Active Directory ("AD"), with a well-defined and tested restore procedure that includes verification of ability to recover all systems to a common point-in-time."

- Conti cyber attack on the HSE: Independent Post Incident Review
  03 December 2021
  PricewaterhouseCoopers (PwC)
  Full Report

Immutability ≠ Invulnerable

Good enough is not good enough

im·mu·ta·ble | \ (ˌ)i(m)-ˈmyü-tə-bəl \

Definition of *immutable*
: not capable of or susceptible to change

in·vul·ner·a·ble | \ (ˌ)in-ˈvəl-n(ə-)rə-bəl , -nər-bəl \

Definition of *invulnerable*
1: incapable of being wounded, injured, or harmed
2: immune to or proof against attack

"Immutability is used differently by vendors and varies in implementation and effectiveness. Therefore, it's important to understand what each vendor means by "immutable" and how its functionality is implemented to assess the risk that hackers can override it."

- Gartner

3 I's of Cyber Recovery

Modern threats require modern solutions

Isolation

Physical & logical separation of data

Protected with operational air gap either on-premises, public cloud or multi-cloud environments

Immutability

Preserve original integrity of data

Multiple layers of security and controls protect against destruction, deletion and alteration of vaulted data

Intelligence

ML & analytics identify threats

Proactively identify data integrity issues to enable assured recovery of "good" data + offers insight into attack vectors from within the vault

DELL Technologies

Incident Response & Recovery

Experiencing a Cyber Incident?
Email: INCIDENT.RECOVERY@DELL.COM
OR call 1-800-433-2392

Dell Technologies Approach to Cyber-Incidents: Best Practices & Methodology

Phase I
Steps: 1 - 4

Phase II
Step: 5

Phase III
Steps: 6 - 8

Phase IV
Step: 9

Phase V
Step: 10

DETECTION, NOTIFICATION & PROTECTION

THREAT HUNTING & ANALYSIS

CONTAINMENT & ERADICATION

RECOVERY & STABILIZATION

MONITORING & DOCUMENTATION

5 Phase approach to Incident Response

HUBER & ASSOCIATES

ENCRYPTED: A CYBERSECURITY SYMPOSIUM

TUESDAY, JUNE 18

TEAMHUBER.COM/BESTOFCYBER

Jason Proctor

Advisory Systems Engineer, Cyber Resilience & Compliance

jason.proctor@dell.com
+1 773.217.2479

Geography: Chicago, IL (US Central Time)

Follow me on: X (Twitter) LinkedIn

DELL Technologies

Data Protection Solutions
Global Technology Office