DAY ONE

WEDNESDAY, APRIL 2ND

Randy Resnick

ZT3 Symposium --- Zero Trust Progress Report

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

April 2nd, 2024

Zero Trust PfMO Overview, Mission and Vision



OVERVIEW

Zero Trust is a modern cybersecurity approach requiring all users & devices, whether inside or outside an organization's network, to be authenticated & authorized before being granted (and to maintain) access to data, assets, applications and services.

MISSION

Lead and synchronize the Department's effort to accelerate Zero Trust adoption across the DoD & achieve Target Level ZT before the end of FY27

VISION

Convert the DoD Information Enterprise into a fully implemented, Zero Trust framework which prevents adversary freedom of movement & exploitation of DoD data

External Accelerants Prompted a ZT Response

SolarWinds
Sep 2019 - Dec 2020

MS Exchange Server
March 2021

Colonial Pipeline
May 2021

Log4J
Dec 2021

VMWare
May 2022

Persistent Attacks
Continuous



In Jan 2019, in response to continuous attacks on DoD & Federal Civilian systems with increased escalation and sophistication, NSA, DISA, and USCYBERCOM came together to study Zero Trust.

This prompted the Secretary of Defense to create a ZT Tiger Team.

ZT Assessment Process Overview

STEP 1

ZT Readiness Assessment Tool (ZTRAT)



STEP 2

Automated Threat Based Cyber Assessment (TBCA)



STEP 3

Independent Purple Team Exercises



ZT Assessment Acceptance Criteria (Draft)

i.e.: Purple Team testing criteria – aiming for repeatability

1 YOU ARE WHO YOU SAY YOU ARE



Continuous authentication and credentialing.

2 YOU ARE AFFIRMED TO ASSUME A ROLE



Authorization, verification, and validation.

3 ROLE ASSUMED IS SPECIFIED



Attribution and behavioral rules.

4 RESOURCES ARE ASCRIBED W/ OPERATING CHARACTERIZATIONS



Attribution.

5 ASSETS ARE ASCRIBED W/ ACCESS & USE CHARACTERIZATIONS



When, where, and how information is allowed for use.

6 POLICY IS SPECIFIED TO DICTATE ACTIONS



Rules.

7 IBAC/RBAC/ABAC IS CONSISTENT & VALIDATED



Rules are consistent, coherent, complete, and validated.

8 ENFORCEMENT SERVICES CAN APPLY ZT DETERMINATIONS ACCURATELY



Continuous authentication and credentialing.

9 BEHAVIORAL ANALYTICS TRACK AND EVALUATE PATTERNS



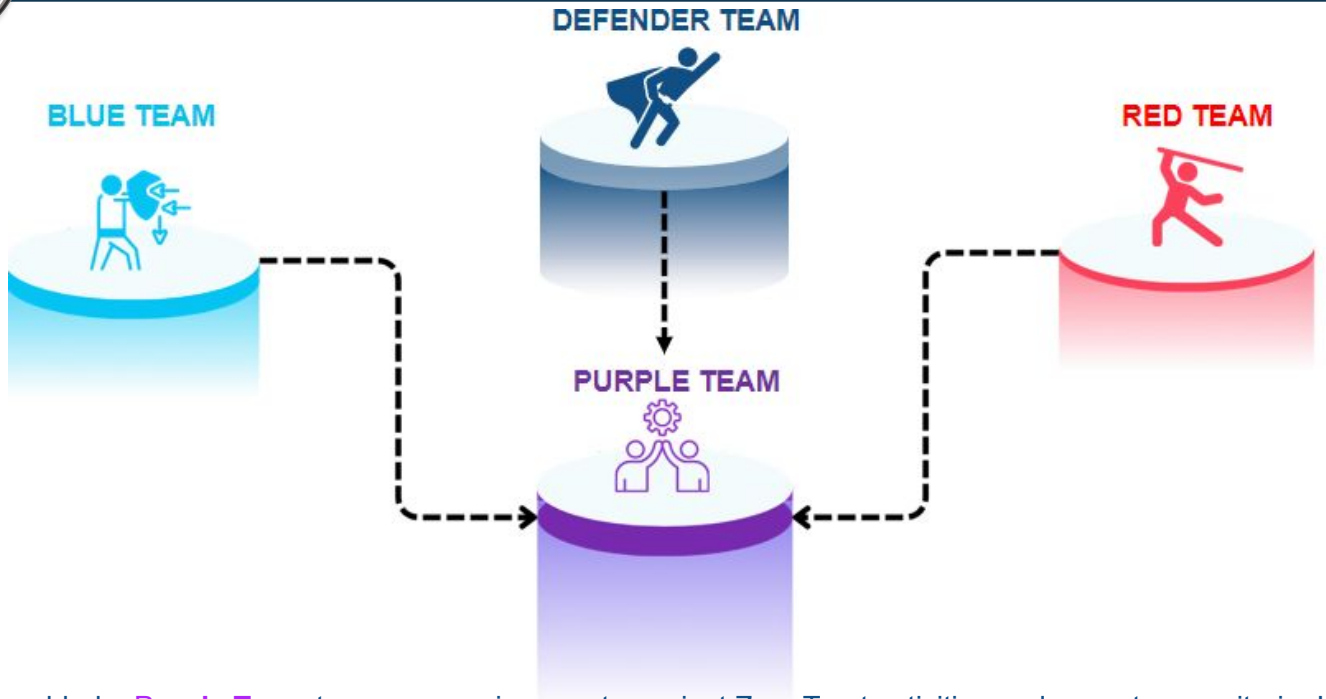
ML/AI.

10 UNANTICIPATED CONDITIONS ESCALATED



Immediately for accommodation.

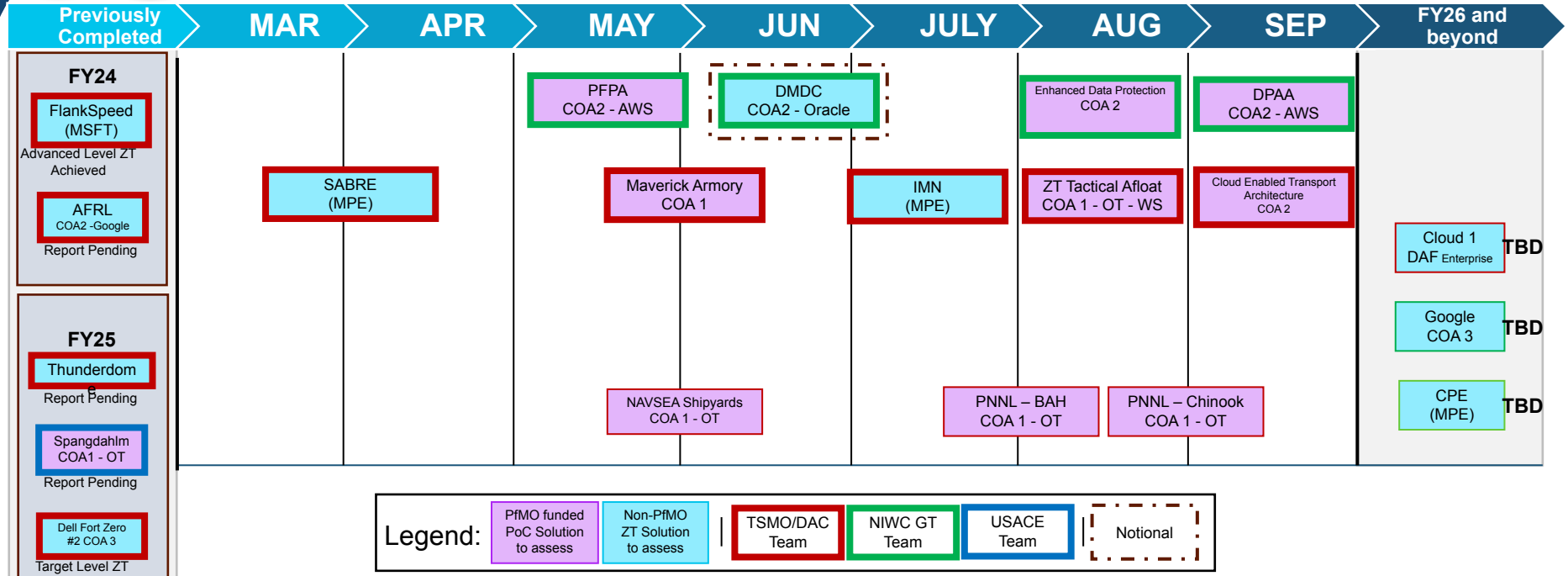
DoD ZT PfMO utilizing Red/Blue Teams in a powerful new way



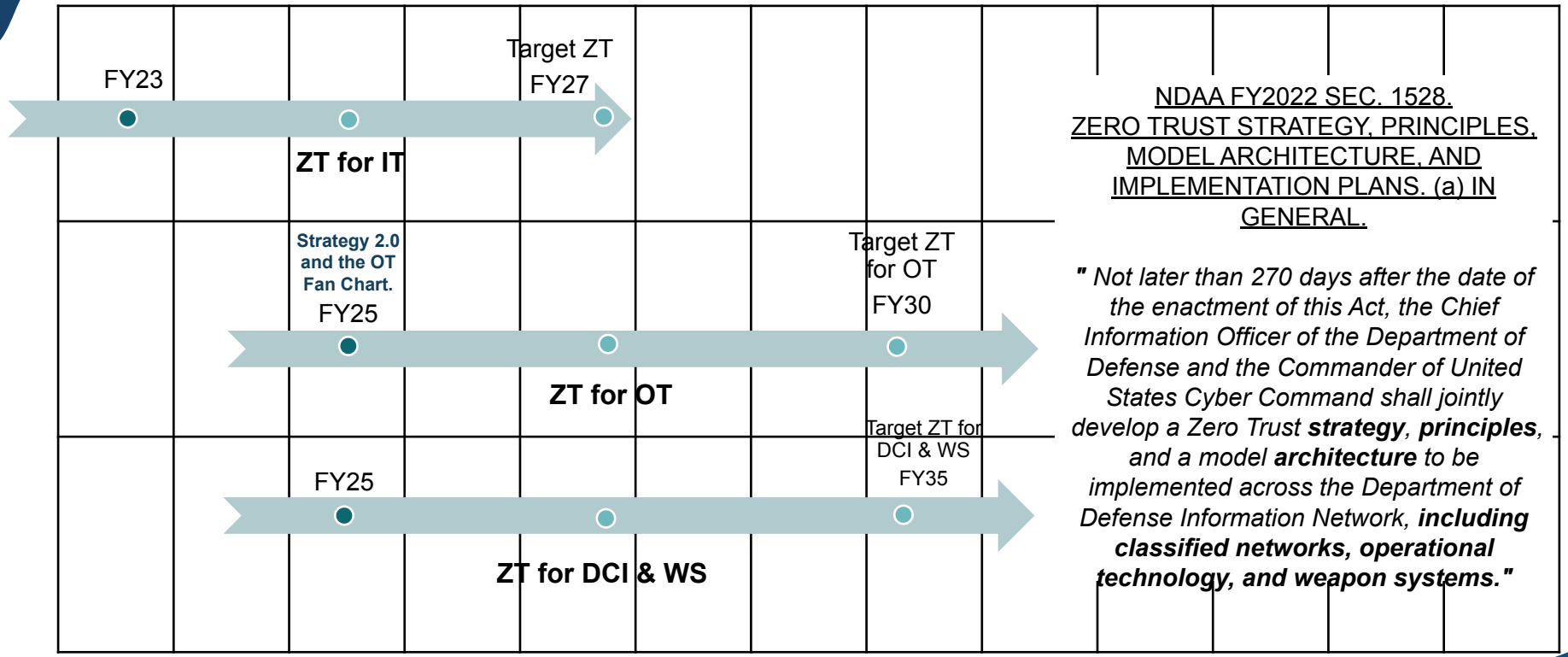
ZT PfMO assembled a **Purple Team** to assess environments against Zero Trust activities and acceptance criteria. Integrating the **red team** (attackers), **blue team** (cyber readiness & resilience) and **defender team** (detection, prevention, and response) into a unified **Purple Team Assessment mindset** significantly enhances the Department's security posture by ensuring continuous, iterative attack testing, vulnerability discovery and remediation which hardens the ZT System Under Test through dynamic adaptation.

FY25 IT-ZT Assessment Schedule

As of March 28, 2025



Mission: ZT PfMO "Notional" Deadlines for DoD



NDAA FY2022 SEC. 1528. ZERO TRUST STRATEGY, PRINCIPLES, MODEL ARCHITECTURE, AND IMPLEMENTATION PLANS. (a) IN GENERAL.

*" Not later than 270 days after the date of the enactment of this Act, the Chief Information Officer of the Department of Defense and the Commander of United States Cyber Command shall jointly develop a Zero Trust **strategy**, **principles**, and a model **architecture** to be implemented across the Department of Defense Information Network, **including classified networks, operational technology, and weapon systems."***

Accelerating to FY27 Process



Questions?

Questions, Comments, Concerns

Ismael Valenzuela

SANS | GIAC CERTIFICATIONS

I Have Zero Trust Issues: Identity Management in Defensible Security Architectures for 2025

Based on Security 530: Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise

ISMAEL VALENZUELA

Ismael Valenzuela

→ SEC530 and SEC568 Co-author

→ +14 yrs teaching for SANS internationally DFIR, CyberDefense & BlueTeam curriculum

→ GSE # 132, plus 11 other GIAC certifications

→ VP Threat Research & Intelligence at BlackBerry

→ Former Foundstone, Intel/McAfee

→ +24 yrs 'Defending All The Things!'

→ **X**: **@aboutsecurity**



What Is A Defensible Security Architecture in 2025

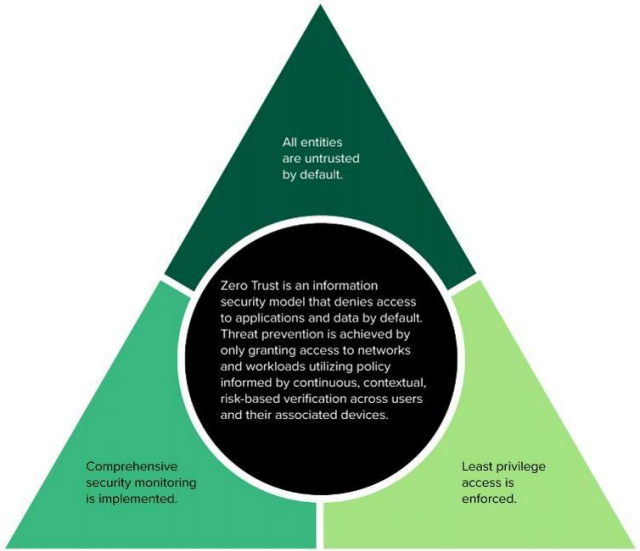
A **Defensible Security Architecture (DSA)** refers to an **approach** to cybersecurity infrastructure that is designed to be **resilient**, **adaptive**, and aligned with modern threat landscapes.

These are key elements that define a defensible security architecture in 2025:

- **Built on Zero Trust core principles to limit attacker's freedom to maneuver**
  - → **Continuous** authentication and authorization.
  - → Network and identity **segmentation** with strict access controls.
  - → Minimal trust even after verification (**least privilege** access).
  - → User, device, and data **monitoring** of behavior for anomalies.
- **Adaptive cyberdefense, based on the knowledge of the adversary**
  - → Threat modeling, including threat intelligence **integration**.
  - → Dynamic defenses based on leveraging artificial intelligence (AI) and machine learning (ML) to **predict** and **adapt** to emerging threats.

Zero Trust Through the 'Stained Glass-Windows of Vendors Marketing'

- As Forrester acknowledged, Zero Trust has become a marketing ploy instead of what it really is: a strategy to reduce implicit trust throughout the enterprise.
- As a model for information security, Zero Trust translates to a data-centric network and security architecture, *one that can be worked toward but without an ultimate end state*.
- Many already have technologies in place that can be leveraged toward achieving "less implicit trust" over time.



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Scenario #1: Exploitation of Public-Facing Applications and Remote Services

- **In 2025, a primary vector for initial access continues to be the exploitation of public-facing applications and remote services.**
  - → Critical vulnerabilities in widely-used software, such as Citrix, Cisco, and Apache…
- **According to the 2024 Verizon Data Breach Investigations Report (DBIR), the primary vector for initial access is still phishing, accounting for 36% of breaches. Following closely are vulnerability exploitation (21%) and use of stolen credentials (20%).**
  - → This reflects an increase in the exploitation of vulnerabilities as an entry point, which **grew by 180% from the previous year.**
- **Why? More remote users, more remote applications, more attack surface…**
- **Antipattern: VPNs are part of the issue**
  - → Maintenance and patching headaches
  - → Too much implicit trust. They were never designed as a security solution.
- **But let's not just to the technology solution just yet..**

The Zero Trust Journey - DARIOM Life Cycle



https://www.sans.org/blog/zero-trust-blog-4-operating-for-zero-trust/

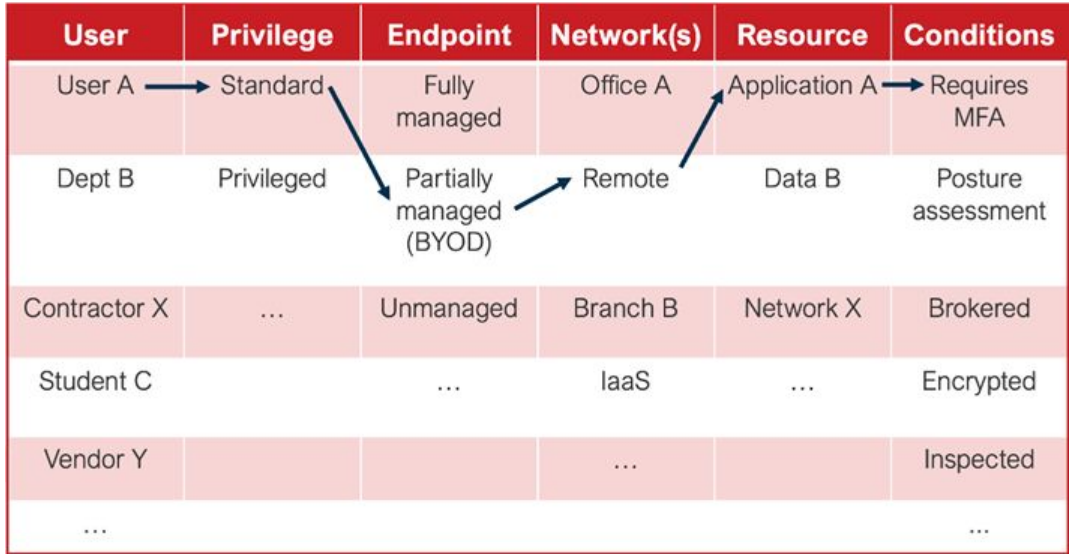
Scenario #1: Defensible Pattern

- **Identify** and **prioritize** critical assets
- Use UEM or tools like BloodHound and/or PingCastle to identify privileged accounts, **excessive implicit trust**, and other AD anomalies
- Use flow data from EDR or NSM/Zeek to **identify where sensitive data flows** from key systems (north/south, east/west)
- Use EDR, DNS, NSM/Zeek, CASB, VPN or NGFW logs to identify traffic to vendor sites based on DNS resolution or application identification



Scenario #1: Defensible Pattern

- **DARIOM model -**
  Discover and Assess
  - → **Evaluate** posture against ZT principles (least privilege approach).
  - → **Identify**, **classify**, and **label** business-critical data
  - → Use your inventory to **map** who has access to what, how and when.
  - → This is a great use case for **analytics** across user access logs (on prem AD, Entra ID, etc.)



Establishing visibility with Zeek

- **Zeek is inherently event-driven IDS (and scripting language). These events can be anything. There's no notion of trusted or untrusted, internal or external.**

```
function KnownOut::known_services_done(c: connection)
    {
    local id = c$id;

    if ( addr_matches_host(id$resp_h, Known::service_tracking) )
        return;
```



service{}	count	percent	is_local_orig
DNS	157404	73.384555	T
SSL	35870	16.723234	T
NTP	1776	0.828003	T
HTTP	1534	0.715178	T
SSH	250	0.116554	T
SMTP	160	0.074595	T
AYIYA	90	0.04196	T
OWAMP	78	0.036365	T
FTP	7	0.003264	T
IRC	1	0.002331	T

In this example, the **ESNet** team uses the Zeek script shown above with a Zero Trust mindset to detect both local hosts or services open to the Internet and Internet hosts/services open to the Internet.

Scenario #1: Defensible Pattern

- **DARIOM model - (Re)Design and Implement based on ZT principles**
  → Zero Trust is not a technology, it's a strategy, a philosophy, a mindset, that can be accomplished via multiple technologies



Modified Version of CISA's Zero Trust Pillars and Maturity Model
https://www.sans.org/blog/zero-trust-blog-1-adopting-zero-trust-mindset/

Scenario #1: Defensible Pattern

- **Start with the policy, not with the technology**
  - → **Subject or Principal**
    - Users who are members of **Tyrell Corporation** and **Project-NEXUS-7** groups (least priv.)
  - → **Action**
    - Access the resource on **TCP port 443 (Web)**
  - → **Resource**
    - Application at **xxx.internal.tyrellcorp.us** (Layer 7 access only)
    - Available **through ZTNA/overlay network only**
  - → **Context**
    - Users must be on a fully **company-managed device**
    - Device must have a **risk rating of 50 or lower**
    - Users may be **remote or on-premises**
    - Remote users **must satisfy phishing-resistant MFA**
    - Remote users can’t connect from a banned country list

Scenario #1: Defensible Pattern - ZTNA Enclave Based Architecture

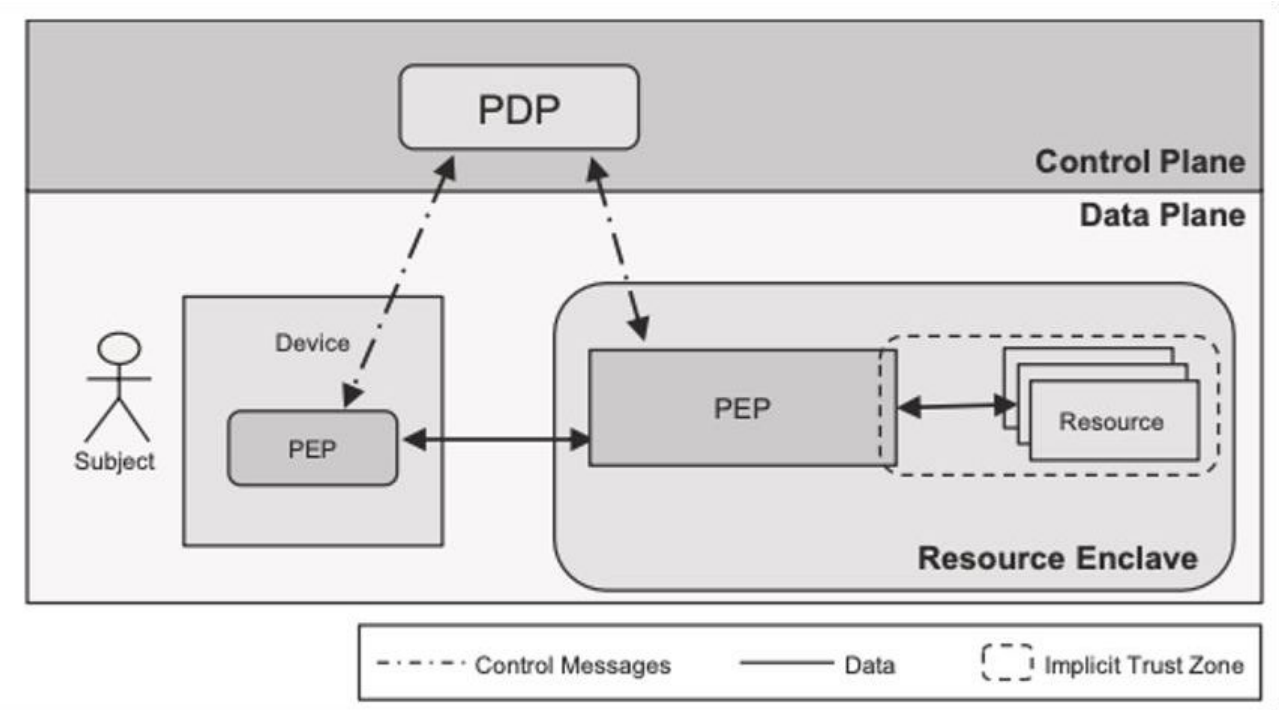


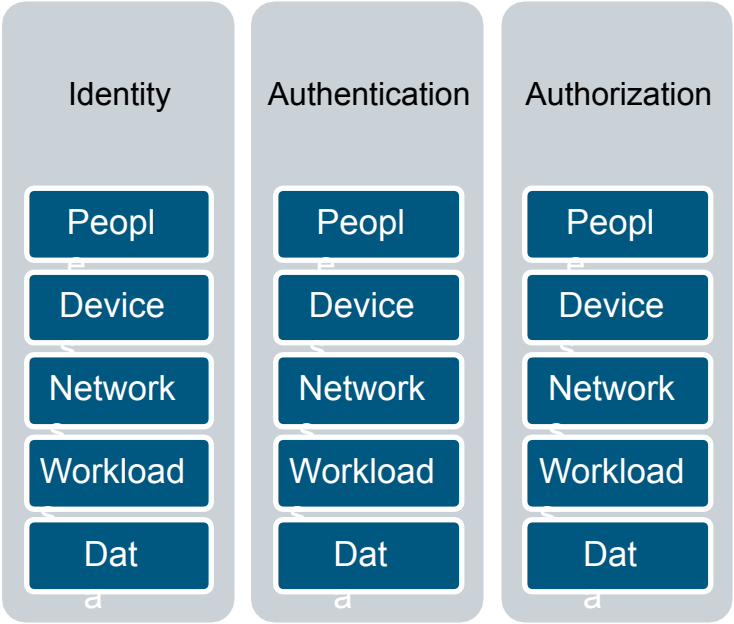
Diagram Source: Zero Trust Security: An Enterprise Guide

Scenario #1: Defensible Pattern

- **Best Practices and Considerations for ZTNA**
  - → Look for breadth of coverage and granularity of access control
  - → Granular, dynamic, and conditional (risk-and context-based) access
  - → **100% API-first**, extensible and programmable, to **integrate with other solutions** (i.e. EDR/NDR/XDR...)
  - → Look for network and application discovery capabilities
- **Realize you will have to coexist with VPN access for a while**
  - → Your goal should be moving toward ZTNA/SDP for most of your users, and partners' access, while maintaining well tuned and secure VPN access to only bring clients into the network when necessary.
  - → To get started:
    - **Define user/group categorization and context**
    - Define endpoint system requirements and policies
    - **Group and categorize services and assets for access control and authorization requirements**

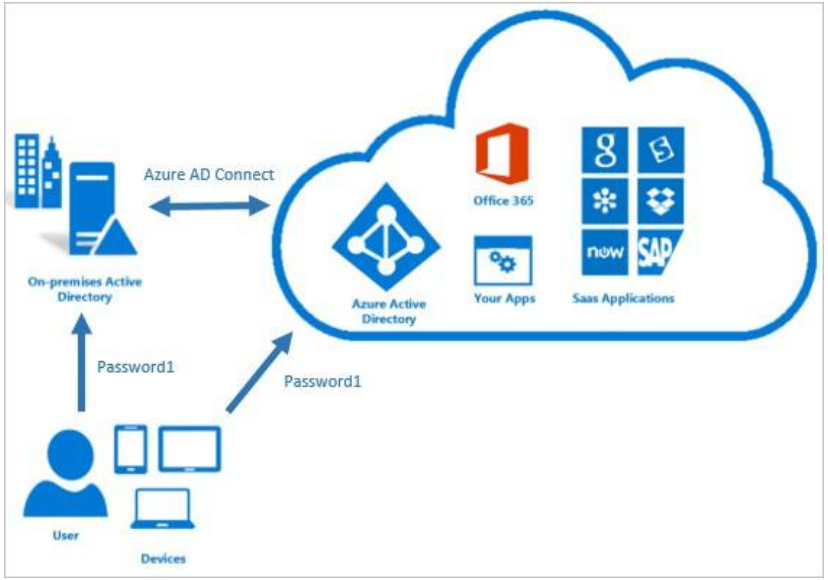
Scenario #2: Identity as a Perimeter

- Probably one of the most important transformations for any organization that wants to implement ZT.
- It requires a short and long-term approach to managing:
  - Identity
  - Authentication
  - Authorization
- Across people, devices, networks, workloads and data.



Scenario #2: Identity Management

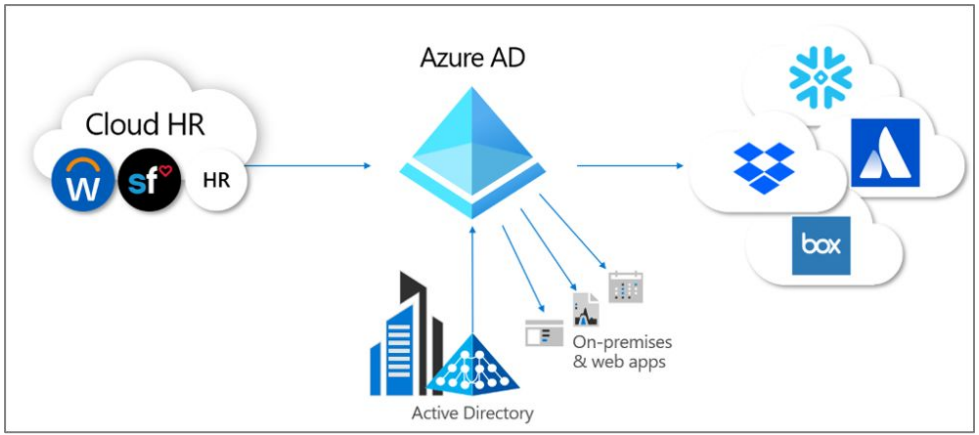
- Ensuring that data is accessed by the right users, at the right time and for the right purposes often requires consolidating using centrally managed identity systems.
- For most of us, the starting point is an on-prem Windows Server AD replicating with Entra ID.
- At this stage, you want to move from creating accounts in on-prem AD to creating them on Entra ID, configuring user objects to replicate down to on-prem Domain Controllers to continue providing access for on-prem apps through Kerberos, LDAP, etc.



AAD connect cloud syncs a hash of the hash, of a user's password from on-premises AD to Azure AD

Scenario #2: Identity Federation

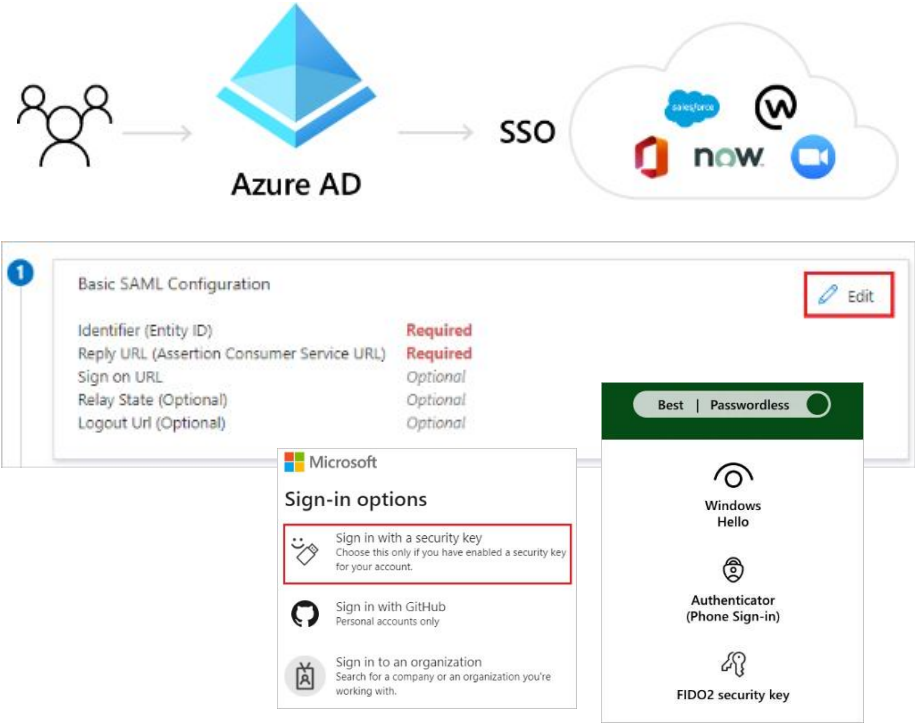
- Next logical step could be to use app provisioning in Entra ID.
- Allows users to access resources across multiple domains or organizations with a single set of credentials (e.g., Dropbox, Salesforce, ServiceNow…)
- SCIM has become the de facto standard for provisioning.
- When used with federation standards like SAML or OIDC, provides administrators an end-to-end standards-based solution for access management.



Entra ID supports provisioning users into applications hosted on-premises or in a virtual machine, via protocols like SCIM, LDAP, SQL, REST, SOAP or just simply PowerShell.

Scenario #2: Authentication, SaaS Applications, and Federated SSO

- On-prem AD servers will continue to use windows authentication protocols.
- For cloud apps, Entra ID will use modern authentication protocols like SAML, OAUTH, OIDC.
- Add **risk-based authentication** and **conditional access**, with **passwordless** capabilities



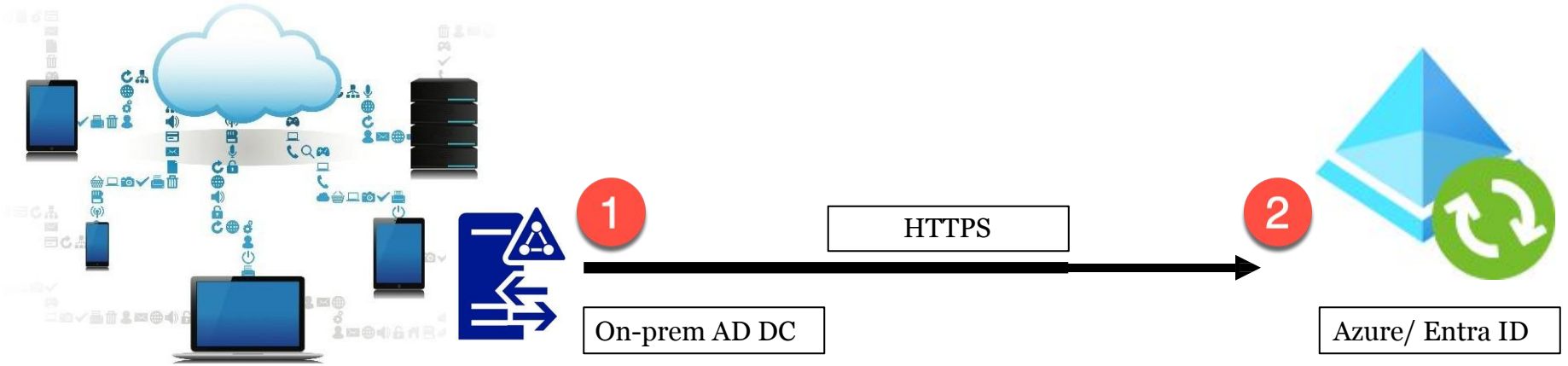
Scenario #2: Are We Secure Yet?

- Hold on...
- Let's apply the new Zero Trust mindset of trust nothing, verify everything.
- And the **Think Red, Act Blue** philosophy.
- What if an attacker could launch a MiTM attack between the Azure AD connect service (on-prem) and the Entra ID?



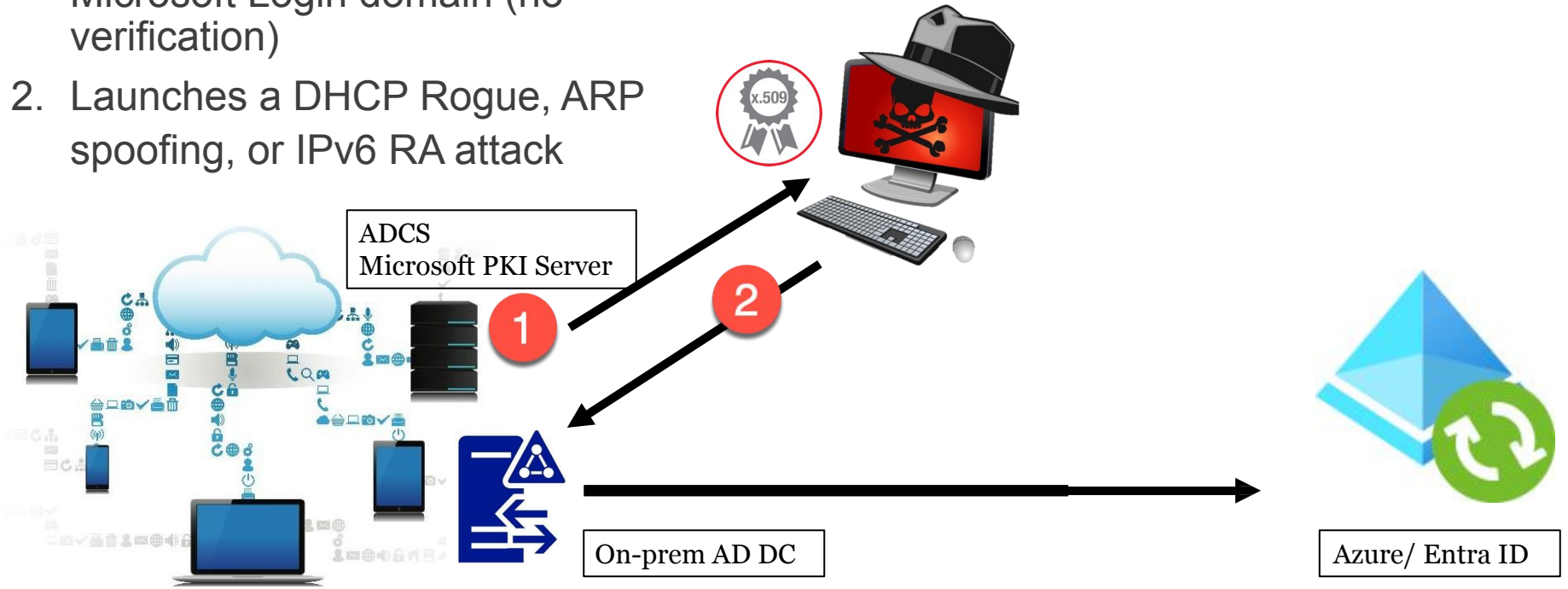
Scenario #2: Attack Vector in Azure/Entra ID (1)

1. Authentication request from on-prem to https://login.microsoftonline.com
2. The on-prem AD Connect service pushes objects to Azure/Entra ID.



Scenario #2: Attack Vector in Azure/Entra ID (2)

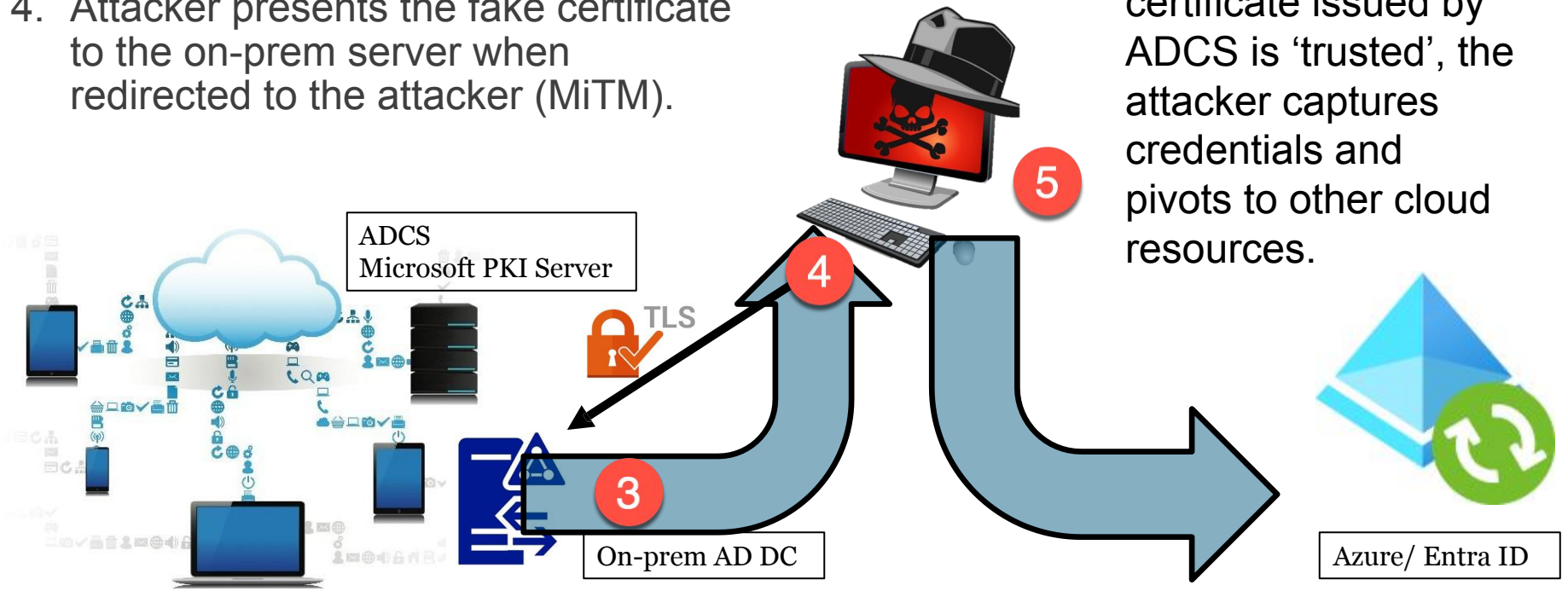
1. Enrollment of a TLS certificate for Microsoft Login domain (no verification)
2. Launches a DHCP Rogue, ARP spoofing, or IPv6 RA attack



Scenario #2: Attack Vector in Azure/Entra ID (3)

3. On-prem AD starts sync.
4. Attacker presents the fake certificate to the on-prem server when redirected to the attacker (MiTM).

5. Since the certificate issued by ADCS is ‘trusted’, the attacker captures credentials and pivots to other cloud resources.



Scenario #2: Attack Vector in Azure/Entra ID: Captured Credentials



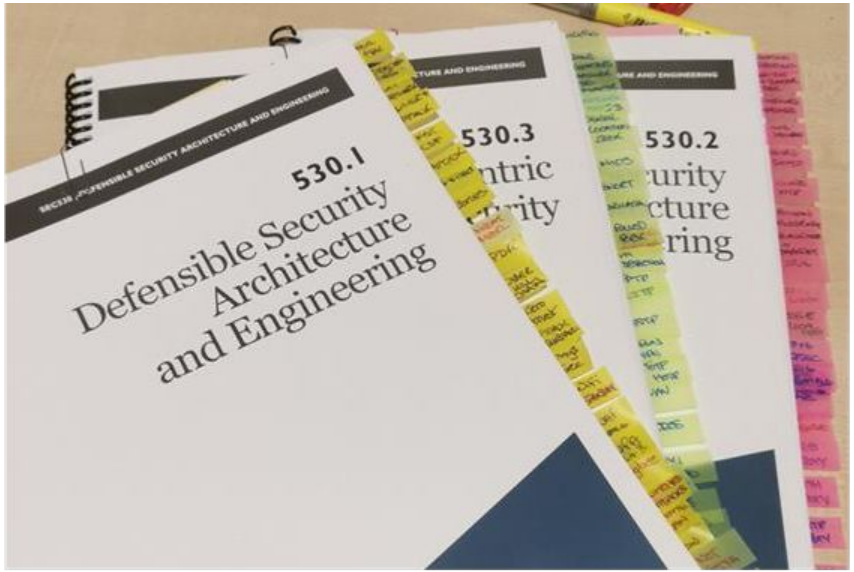
Scenario #2: Lessons learned and mitigations

- **On-prem is still in most cases the weakest link.**
- **Layered defense is vital, including:**
  - **Endpoint security** and secure workstations
  - Network **segregation** and monitoring
  - **Hardening** against L2 attacks (i.e. ARP spoofing, DHCP, IPv6 RA) increases the attacker's cost.
    - Privileged Access Management
      - Implement **PAM** solutions to enforce secure administrative access to the AD Connect server.
      - **Monitor** for abnormal activity.
    - **Restrict access to certificate templates** that allow server authentication and monitor enrollment.

Conclusions

- A defensible security architecture based on ZT principles must be **adaptable**, based on the **knowledge of the adversary.**
- It's not about identity or network based ZT, **you need both**!
- Don't be quick to jump into a technology solution, **start with discover & assess**, and look for opportunities to **re-use what you already have**.
- Add **risk-based** authentication and **conditional access**, with **passwordless** capabilities such as hardware tokens, certificates, or windows hello where possible.
- But remember, **attackers are lazy**! They often follow the path of least resistance, and that's commonly on-prem infrastructure.
- Identify opportunities for limiting the attacker's ability to maneuver, while extending your ability to **take the "adversary by surprise".**

SEC530: Defensible Security Architecture and Engineering



*#SEC530 is absolutely recommended for anyone who is working as Cyber Security Engineer / Analyst / Architect and wants to become an #AllRoundDefender. Great content and learning towards the journey to **Zero Trust Architecture** – Arindham Laha, Lead Architect, The TJX Companies*

*"**I would highly recommend this for any business and organizations** [..] to fully understand why this attitude of Zero Trust needs to be taken into consideration. This covers areas that CISSP or Sec+ would not." – SEC530 student, **DHS-CISA***

*"The labs are absolutely rock solid. I've been around the industry a while and **never experienced labs this good**. Highly commendable." – Michael Curran, Austrade*

https://www.sans.org/cyber-security-courses/defensible-security-architecture-and-engineering/

Karen Uttecht

Measuring Zero Trust

Karen Uttecht

3rd Annual Virtual DoD ZT Symposium

02 April 2025

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

This material is based upon work supported under Air Force Contract No. FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the U.S. Air Force.

© 2025 Massachusetts Institute of Technology.

Delivered to the U.S. Government with Unlimited Rights, as defined in DFARS Part 252.227-7013 or 7014 (Feb 2014). Notwithstanding any copyright notice, U.S. Government rights in this work are defined by DFARS 252.227-7013 or DFARS 252.227-7014 as detailed above. Use of this work other than as specifically authorized by the U.S. Government may violate any copyrights that exist in this work.

Agenda

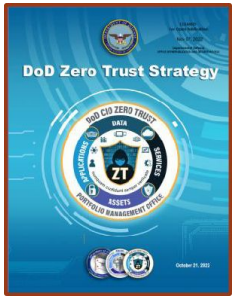
- **Motivation & Problem Space**
- **Assessment & Metric Considerations**
- **Selected Proposed Metrics**
- **Summary**

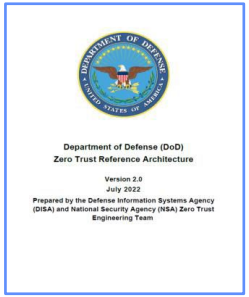
DoD Zero Trust Journey

What is Zero Trust?

How do we implement a Zero Trust Architecture?

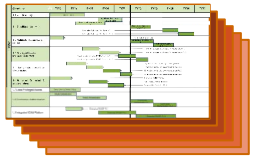
How do we verify our ZTA implementation is really protecting us?





DoD ZT Strategy, DoD ZT Reference Architecture, DoD ZT Capabilities







ZT Capability and Activity Timelines, Implementation Milestones, COAs

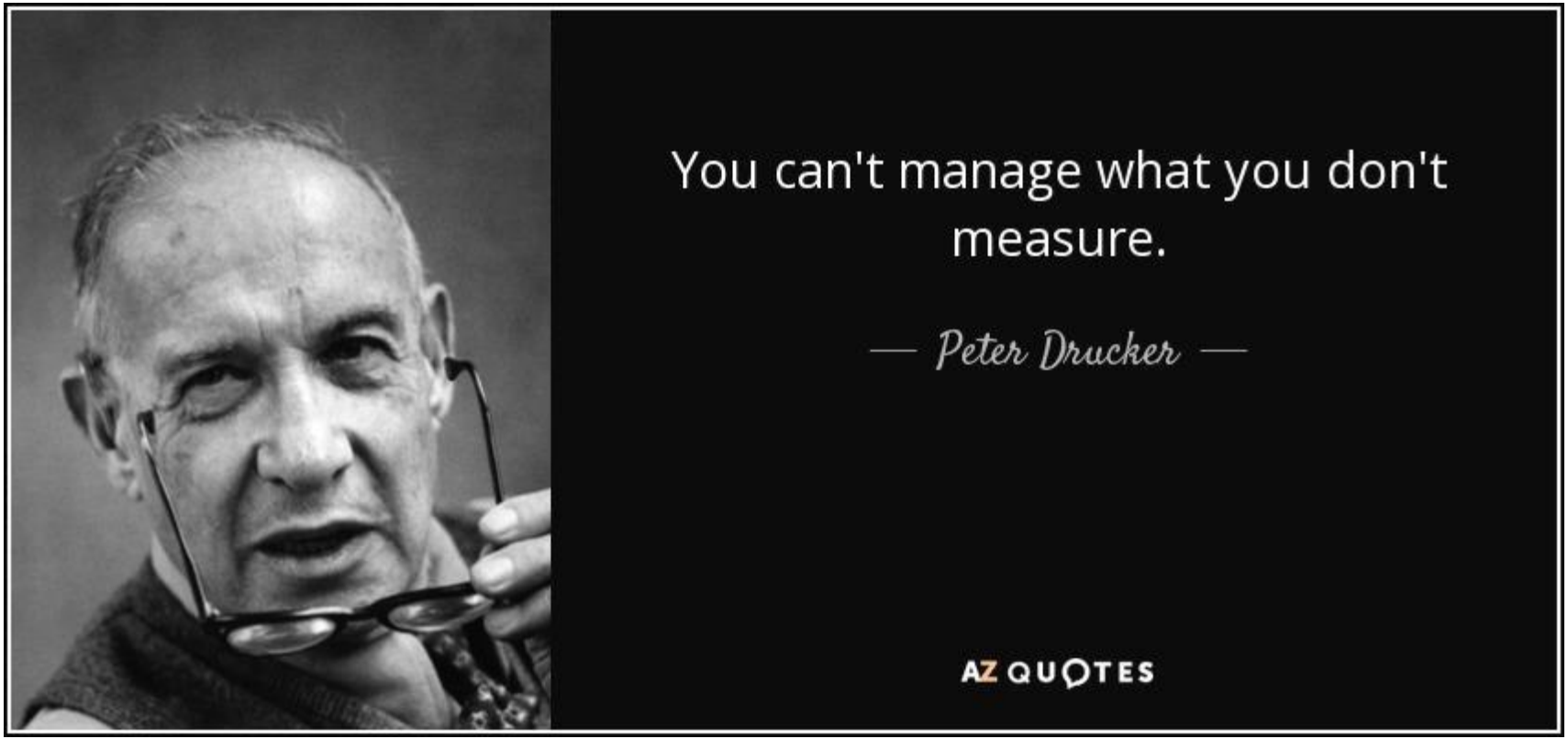
?

What impact does ZT have to our mission?

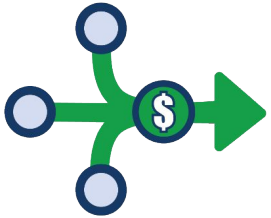
DoD – Department of Defense ZT – Zero Trust
COA – Course of Action

ZTA – Zero trust Architecture

Why Do We Need to Measure?



Measure to Support Decision Making





Acquisition & Development Stakeholders

- How does the ZTA impact my cyber threat surface and impact cyber risk?
- Is additional functionality of worth the cost?
- How do we know this ZTA provides the features we need?
- How can I weigh options between

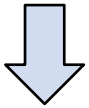
Operational Stakeholders

- How do day to day technical policy choices affect cyber risk?
- Are my policies providing the appropriate level of protection?
- Where would additional improvements provide the most benefit?

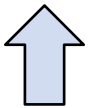
ZT assessments will give stakeholders the information necessary to make effective decisions

Calculating Cyber Risk

Zero Trust Reduces Likelihood of Successful Attack



$$Risk = Likelihood \times Impact$$



Zero Trust Reduces Impact of Successful Attack

Measuring the effectiveness of ZT is critical to calculating cyber risk

Don’t We Already Do This?

We count vulnerabilities!

BUT…

Zero Trust assumes compromise

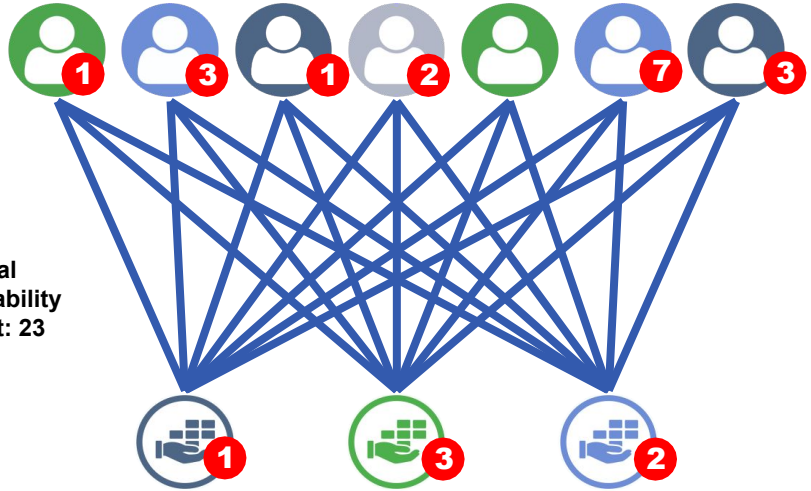
Zero Trust is about what comes before – preventing access to the vulnerability

Zero Trust is about what comes after – limiting the impact of exploiting a vulnerability

Tracking (and patching) vulnerabilities is important, but doesn’t help us understand the effectiveness of ZT

Vulnerability Counts Aren't The Whole Picture

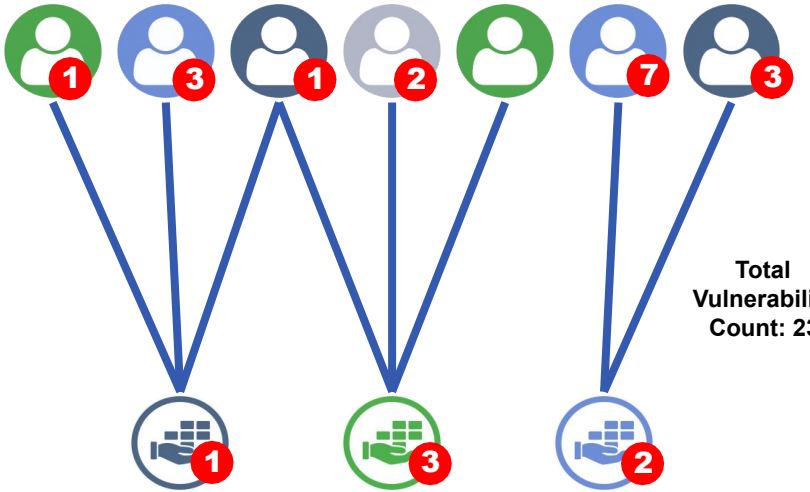
Highly Connected Network



Total Vulnerability Count: 23

More Risk

Sparsely Connected Network



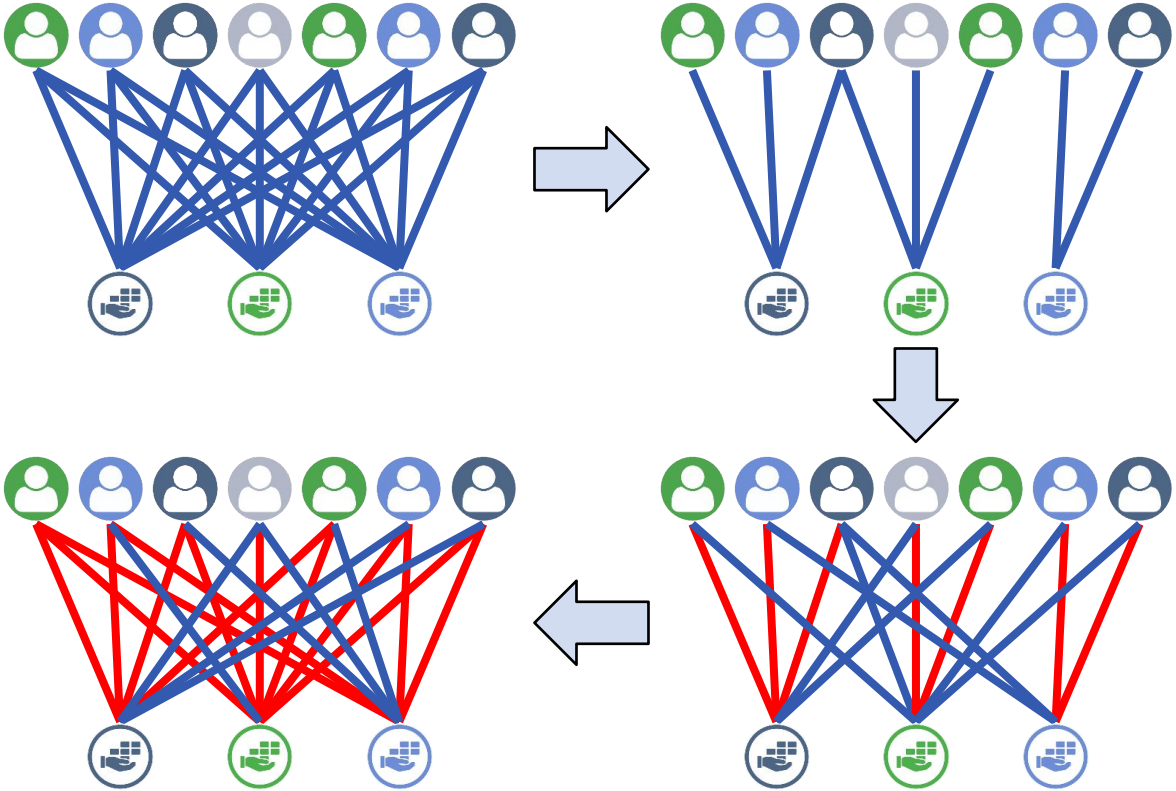
Total Vulnerability Count: 23

Less Risk

Traditional cybersecurity metrics don't capture the ZT cyber risk improvements

Ongoing Policy Validation Is Critical

Before Zero Trust
All users able to communicate with any service



With Zero Trust
Users can only communicate with services they need to access

Changes Occur

User change roles but unneeded access remains

Over Time

Policy reverts towards pre-ZT connectedness

Agenda

- Motivation & Problem Space
- **Assessment & Metric Considerations**
- Selected Proposed Metrics
- Summary

Types of Cyber Assessment

	Compliance Audit	Cybersecurity Testing	Quantitative Metrics
			
	a.k.a. “Checklist” or “Scorecard”	a.k.a. “Red/Purple Team”, “Cyber Table Top”	a.k.a. “KPIs”
Example	***Does this ZTA have multi-factor authentication?***	***Can the red team exfiltrate PII data from the personnel server?***	***How many accounts have access to the confluence service?***
Cost *	**Medium**	**High**	**Low**
Strengths	**Standardizable, may be automated, ensures completeness of solution**	**Applies critical thinking, validates assumptions, identifies major weaknesses**	**Automated, objective, can measure operational policy**
Weaknesses	**Quality varies with detail level, often manual, doesn’t incentivize further improvement**	**Quality varies based on team abilities & time spent, manually intensive, infrequent**	**Quality varies on implementation, (sometimes) encourages gaming the system**

**Per assessment performed*

KPI – Key Performance Indicator ZTA – Zero Trust Architecture

Types of Cyber Assessment

	Compliance Audit	Cybersecurity Testing	Quantitative Metrics
			
	a.k.a. “Checklist” or “Scorecard”	a.k.a. “Red/Purple Team”, “Cyber Table Top”	a.k.a. “KPIs”
Example	***Does this ZTA have multi-factor authentication?***	***Can the red team exfiltrate PII data from the personnel server?***	***How many accounts have access to the confluence service?***
Cost *	**Medium**	**High**	**Low**
Strengths	**Standardizable, may be automated, ensures completeness of solution**	**Applies critical thinking, validates assumptions, identifies major weaknesses**	**Automated, objective, can measure operational policy**
Weaknesses	**Quality varies with detail level, often manual, doesn’t incentivize further improvement**	**Quality varies based on team abilities & time spent, manually intensive, infrequent**	**Quality varies on implementation, (sometimes) encourages gaming the system**

**Per assessment performed*

KPI – Key Performance Indicator ZTA – Zero Trust Architecture

Zero Trust Metric Contexts



Architecture & Design



Capability & Range Testing



Implementation



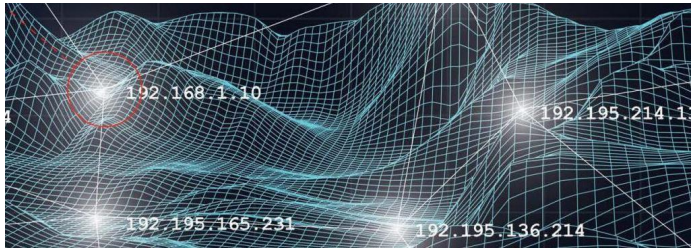
Operations



Organization Management

ZT metrics must be designed to cover all the various contexts in which they will be applied

Objectives for a Suite of ZT Metrics



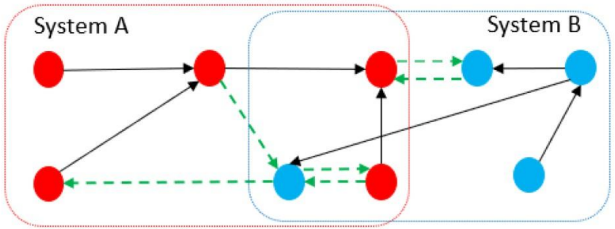
Comprehensive Cyber terrain Coverage



Comprehensive Threat Coverage



Appropriately Detailed



Considers System Dependencies

ATT&CK – Adversarial Tactics, Techniques, and Common Knowledge

Properties of a Good Cyber Metric

Accurate
Stakeholders can trust the results

Relevant
Directly applicable to decision making

Timely
Updated within the decision loop time cycle

Actionable
Stakeholders know how to improve

Understandable
Stakeholders understand the relationship between metric and decisions

Scalable
Can be applied to the entire decision space

Comparable
Results from one system can be compared to another

Automatable
Can be collected with a minimum of human resources

Measurable & Quantifiable
Able to be calculated from direct measurement

Threat applicable
Accounts for the threat the security measure was designed to counter

Incentivize Correct Actions
Should not motivate poor choices

Properties of a Good Cyber Metric

Accurate
Stakeholders can trust the results

Relevant
Directly applicable to decision making

Timely
Updated within the decision loop time cycle

Actionable
Stakeholders know how to improve

Understandable
Stakeholders understand the relationship between metric and decisions

Scalable
Can be applied to the entire decision space

Comparable
Results from one system can be compared to another

Automatable
Can be collected with a minimum of human resources

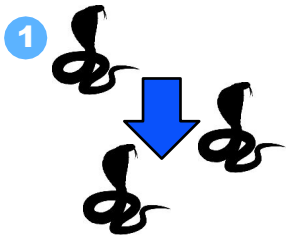
Measurable & Quantifiable
Able to be calculated from direct measurement

Threat applicable
Accounts for the threat the security measure was designed to counter

Incentivize Correct Actions
Should not motivate poor choices

Avoiding Metrics with Perverse Incentives

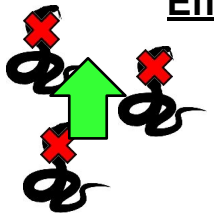
The Cobra Effect

1. 

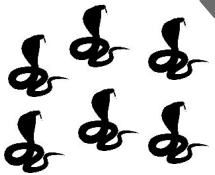
Goal: Reduce cobra population

2. 

Solution: bounty on dead cobras

3. 

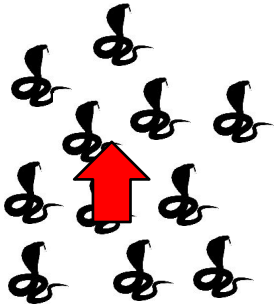
Metric: Number of bounties redeemed

4. 

Perverse Incentive: Breed cobras for fun and profit!

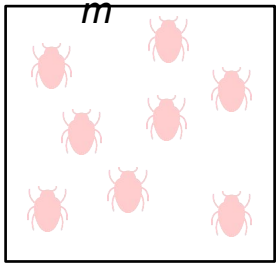
5. 

Solution: Bounty program canceled

6. 

Consequence: breeders release cobras, population higher than before

Perverse Incentives in Cybersecurity: Known Vulnerabilities



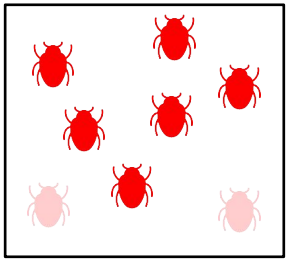
Syste
m

**Vulnerabilitie
s Exist**

Syste
m
Owner



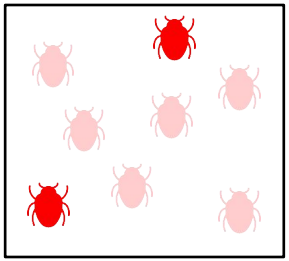
?



**Frequent,
intensive
assessment
s**

**More Known
Vulnerabilitie
s**

Results in more problems for management, less budget for other things



**Infrequent,
cursory
assessments**

**Less Known
Vulnerabilitie
s**

Looks more secure, less headaches for system stakeholders

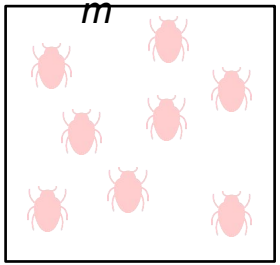


**Incentive To
Avoid
Assessments**

Avoiding or limiting co-operation to reduce the possibility of vulnerabilities being found is incentivized

Perverse Incentives in Cybersecurity: AI/ML

Syste
m



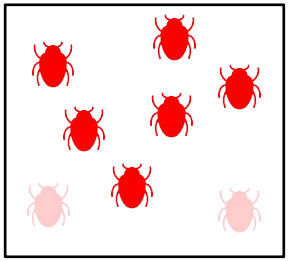
Vulnerabilities Exist

Cyber

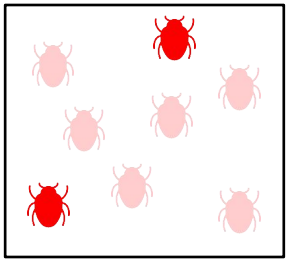


Goal: Improve Cybersecurity by Minimizing Cyber Risk

?



Frequent Scans



Infrequent Scans

More Known Vulnerabilities

More known vulnerabilities means a higher cyber risk score

Less Known Vulnerabilities

Less known vulnerabilities results in a lower cyber risk score



AI Making Poor Choices

Scanning less often or designing scans that detect less vulnerabilities

AI – Artificial Intelligence ML – Machine Learning

Properties of a Good Cyber Metric

Accurate
Stakeholders can trust the results

Relevant
Directly applicable to decision making

Timely
Updated within the decision loop time cycle

Actionable
Stakeholders know how to improve

Understandable
Stakeholders understand the relationship between metric and decisions

Scalable
Can be applied to the entire decision space

Comparable
Results from one system can be compared to another

Automatable
Can be collected with a minimum of human resources

Measurable & Quantifiable
Able to be calculated from direct measurement

Threat applicable
Accounts for the threat the security measure was designed to counter

Incentivize Correct Actions
Should not motivate poor choices

Secure Against What?

Threat: Enemy bomber

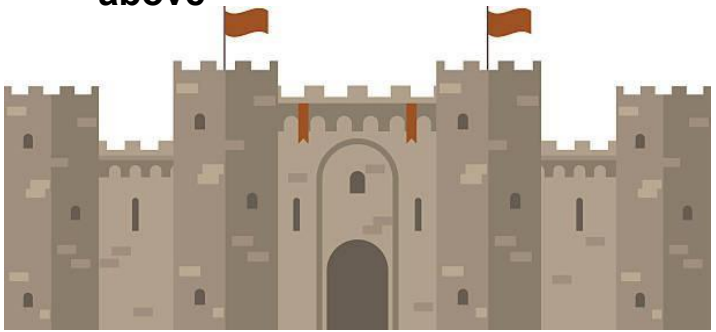


Can drop ordinance from above

Threat: Enemy Cannon



Can penetrate stone walls to 3 feet



10 foot thick, 40 foot high castle wall

Threat: Enemy soldiers with 40 foot ladder



Can scale 43 foot castle walls

Security metrics must be in the context of the threat to be effective

What Threats is Zero Trust Countering?

- **Insider threat**
- **Lateral movement**
- **Persistence**
- ***Not exploiting specific software/firmware vulnerabilities, ZT assumes compromise***

Zero Trust metrics should measure how well a ZTA does at countering these threats

Adversary Assets

- The adversary requires certain assets or resources to complete their mission
- Resisting adversary attack can be accomplished by increasing the required assets necessary for success
- What does the adversary need that ZT denies/makes more difficult?
  - Credentials
  - Access to information for recon
  - Access to services/apps/protocols/network devices
  - Privileges
  - Ability to persist undetected
  - C2 and exfil lines of communication & ability to hide those lines

Metrics identifying average or expected numbers of assets necessary can be used as a heuristic for estimating adversary cost

Overall Key Gaps in Existing Cybersecurity Metrics

- **Threat-based metrics**
- **Measures of lateral movement impedance**
- **Measures of quality of roles, attributes, and tag schemes**
- **Measures of policy value in reducing cyber risk**
- **Ongoing accuracy of AI/ML in operations**

AI/ML – Artificial Intelligence / Machine Learning

Agenda

- Motivation & Problem Space
- Assessment & Metric Considerations
- Selected Proposed Metrics
- Summary

Two Basic Operational Policy Metrics

Exposure

$$Exposure_R = \frac{Users\ w/Access_R}{All\ Users}$$

For each resource R, out of all users in the system, what percentage have access to the resource?

Utilization

$$Utilization_R = \frac{Recent\ Users_R}{Users\ w/Access_R}$$

For each resource R, out of all users with access to the resource, what percentage have accessed it recently?

- **Taking measures to decrease Exposure and increase Utilization reduces the amount of unnecessary access to a resource, reducing the attack surface**
- **Simple to calculate from available data, easy for decision makers to understand and take action**

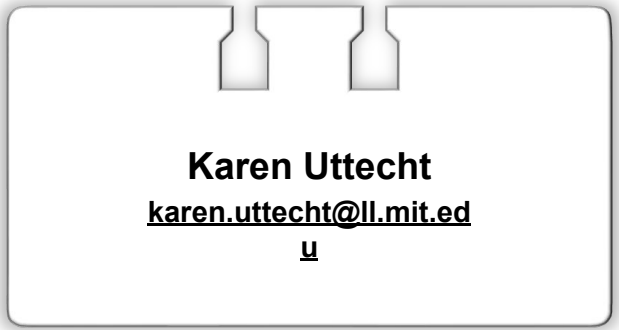
Exposure and Utilization measure how well ZT principles are being applied

Summary

- ZT assessment is a major next frontier to tackle
- Existing cybersecurity metrics don't cover ZT completely
- It is critical that ZT metrics are well-designed and provide adequate coverage,
  especially that they take into account
  - Potential perverse incentives
  - Account for the threat
- Gap analysis of cybersecurity metrics showed a need for metrics measuring
  - Quality & value of attribute, role, tag choices
  - Policies in operations, especially segmentation
  - AI/ML accuracy in operations
- Two basic metrics
  - Exposure – Ratio of users can access a resource
  - Utilization – Ratio of users who don't use existing access

ZT – Zero Trust
AI/ML – Artificial Intelligence / Machine Learning

Contact Info



Jeremy Jones

AGILE & ZERO TRUST

BY: JEREMY JONES
IT SPECIALIST

The views expressed in the presentation are that of mine and do not necessarily reflect the views of MDA or DoD.

IMPLEMENTING ZERO TRUST WITH AGILE

PURPOSE: THIS PRESENTATION ISN'T ABOUT TEACHING YOU AGILE - WE TRUST YOU ALREADY GET IT! INSTEAD, LET'S EXPLORE HOW THE AGILE CORE PRINCIPLES CAN SUPERCHARGE YOUR ZERO TRUST IMPLEMENTATION.

BLUF: ZERO TRUST IS NOT SOMETHING THAT CAN BE ENABLED ALL AT ONCE. IMPLEMENTING ZERO TRUST IS SOMETHING THAT IS ENABLED INCREMENTALLY AND ITERATIVELY TO REACH EACH DESIRED TARGET LEVEL WITHIN ZERO TRUST.

AGILE MANIFESTO



Original

My version



KEY BENEFITS OF AGILE

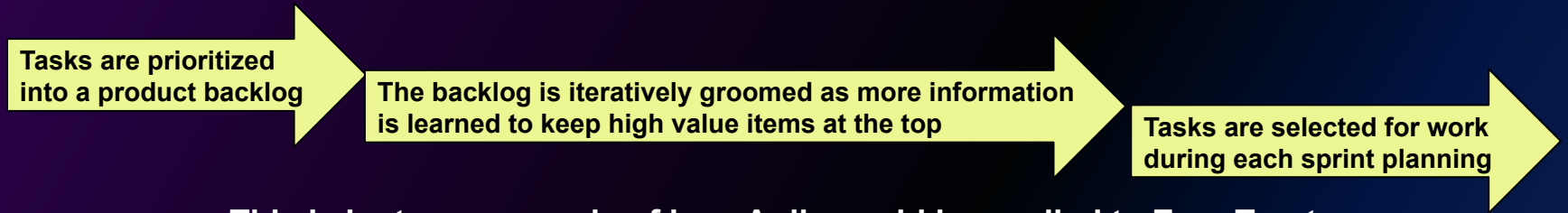
- The general concept of Agile is to break down large bodies of work into smaller tasks that are prioritized into a product backlog.
  - Over time, the work can be refined iteratively while making incremental deliveries to achieve the larger body of work.
- Adaptability – Welcoming of changing requirements
- Risk Management – Smaller increments of delivery allow better mitigation
- Team efficiency – Communication and throughput can be better with smaller teams
- Feedback Loops – Focus on constantly satisfying the customer
- Transparency – Breeds trust with the customer and all stakeholders

Zero Trust scenarios thus far to think about:

- Activities for Facilities Related Control Systems were updated to remove several of the original activities. (Adaptability, Risk Management)
- There are multiple Zero Trust Memo's and Strategies released that need to be deconflicted. (Adaptability, Risk Management)
- User impact. (Risk Management, Feedback Loops, Transparency)

APPLYING AGILE TO ZERO TRUST

- **Agile work is broken up into some variation of the following**
  - Epics = Activities
  - Stories = Outcomes
  - Tasks = Tasks
- **Zero Trust aligns well with the above structure**
  - The activities required for the various levels of Zero Trust Capabilities could be considered as Epics.
  - Each activity (Epic) would be broken down into Stories.
  - The Stories would then be broken down further into Tasks to achieve the Stories.
  - Tasks and Sub-tasks are then prioritized in a product backlog for work during follow on sprints.



This is just one example of how Agile could be applied to Zero Trust

1.1.1 INVENTORY USER (EPIC)

A Sample of the Outcomes (stories) for 1.1.1

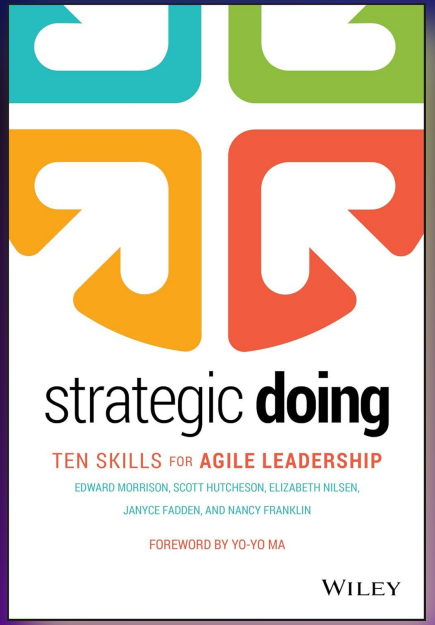
- **Outcome 1(Story): Identified Managed Non-Privileged Users**
  - **Task: Catalog non-privileged Users from all authentication sources.**
    - **Broken down further into sub-task**
- **Outcome 2 (Story): Identified Managed Privileged Users**
  - **Task: Catalog all privileged Users and ensure their identities are managed within authoritative sources**
    - **Broken down further into sub-task**
- **Outcome 3 (Story): Identified applications using independent user account management for non-administrative and administrative accounts**
  - **Task: Inventory applications (Catalog users in each application with independent account management) (Catalog privileged users with independent account management)**
    - **Broken down further into sub-task**

AGILE FAILURES AND MYTHS

- **Common Reasons for Agile Failures**
  - Company or Organization culture does not support trying something new
  - No experience with Agile
  - Not enough support from management and or leadership
  - Pressure to do it "the way that it has always been done"
  - Insufficient training
  - Unwillingness to implement continuous improvement after starting Agile
- **Common Agile myths**
  - Agile is easy
  - Agile means there is no need for documentation
  - Agile is only for software development
  - Agile is cheap

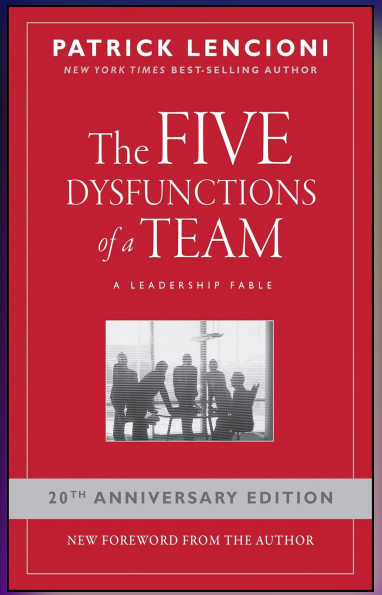
RECOMMENDED READING

- **Strategic Doing: Ten Skills of Agile Leadership**
  - **By Edward Morrison, Scott Hutcheson, Elizabeth Nilsen, Janyce Fadden and Nancy Franklin**



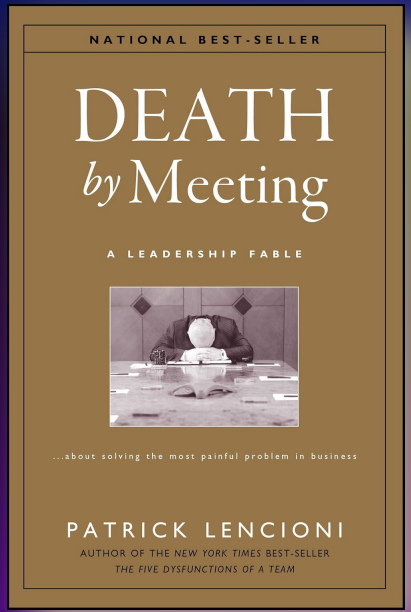
RECOMMENDED READING

- **The Five Dysfunctions of a Team**
  - **By Patrick Lencioni**



RECOMMENDED READING

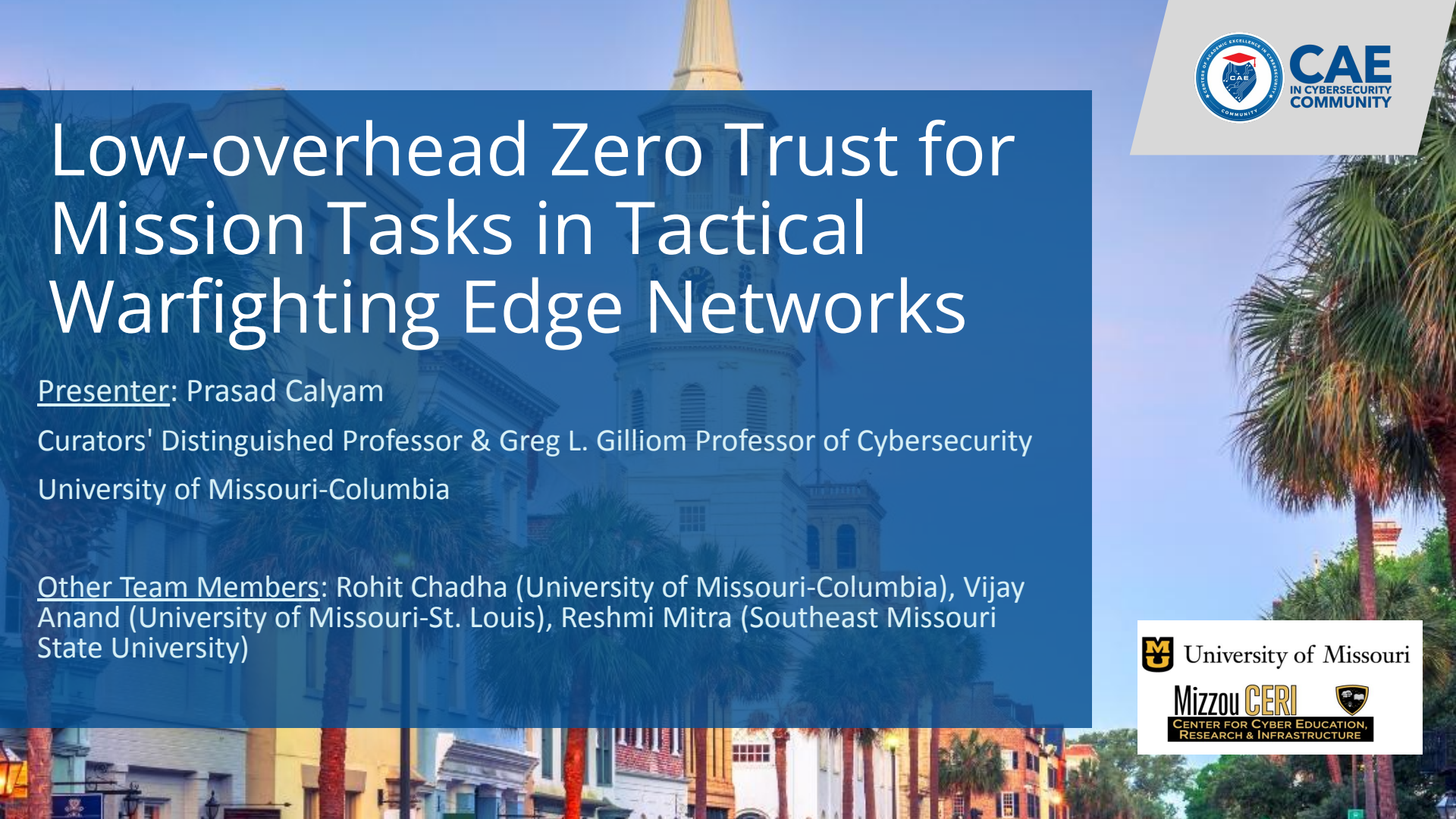
- **Death by Meeting**
  - **By Patrick Lencioni**



THANK YOU

Questions?

Prasad Calyam



Low-overhead Zero Trust for Mission Tasks in Tactical Warfighting Edge Networks

Presenter: Prasad Calyam

Curators' Distinguished Professor & Greg L. Gilliom Professor of Cybersecurity

University of Missouri-Columbia

Other Team Members: Rohit Chadha (University of Missouri-Columbia), Vijay Anand (University of Missouri-St. Louis), Reshmi Mitra (Southeast Missouri State University)

CAE IN CYBERSECURITY COMMUNITY

University of Missouri

Mizzou CERI

Center for Cyber Education, Research & Infrastructure

Agenda

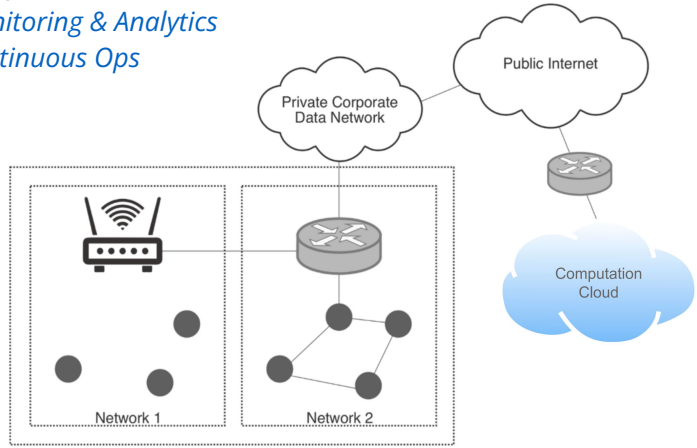
- Research Motivation
  - Tactical Warfighting Edge
  - Zero Trust
  - Problem Statement
- Arculus: Low-overhead Zero Trust Security Architecture
- AI-driven Predictive Model Technologies
  - RL-based Intelligent Drone Trajectory Management
  - Bayesian Network for Risk Quantification
- Arculus Evaluation
  - TBAC vs RBAC results
  - Predictive models results
  - Hardware experimentation results for TWE threat scenarios
- Conclusion and Future Directions

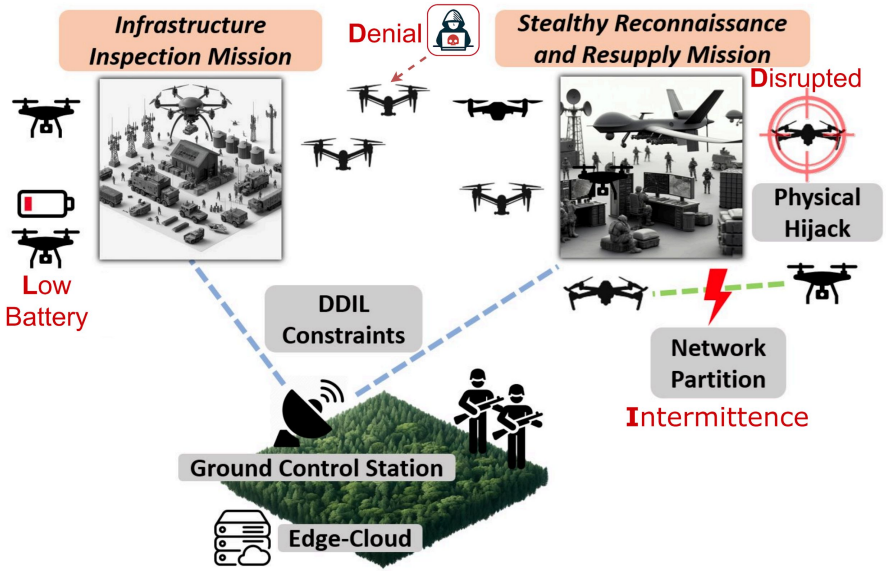
Enterprise Network vs TWE Network

Capabilities:
Identity Verification
Access Control
Resource Protection
Policy & Orchestration
Monitoring & Analytics
Continuous Ops

Enterprise Network Vs. Tactical Warfighting Edge

High Availability | *Intermittent / Low Availability*





ZT Enterprise capabilities **are not effective at the tactical warfighting edge** due to operational impacts from denied, disrupted, intermittent, and limited **(DDIL) environments**, including limited bandwidth, and other constrained resources.

Exemplar TWE Mission Types and Tasks

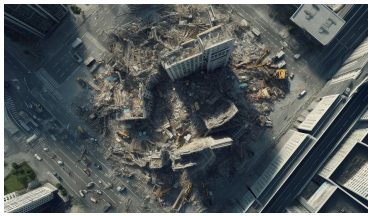
Stealthy Reconnaissance and Resupply



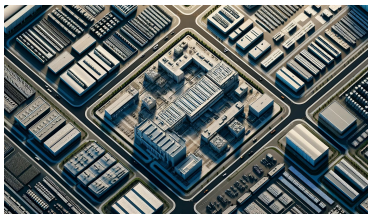
Mine-Aware Search and Rescue



Disaster Assessment and Recovery



Infrastructure Inspection

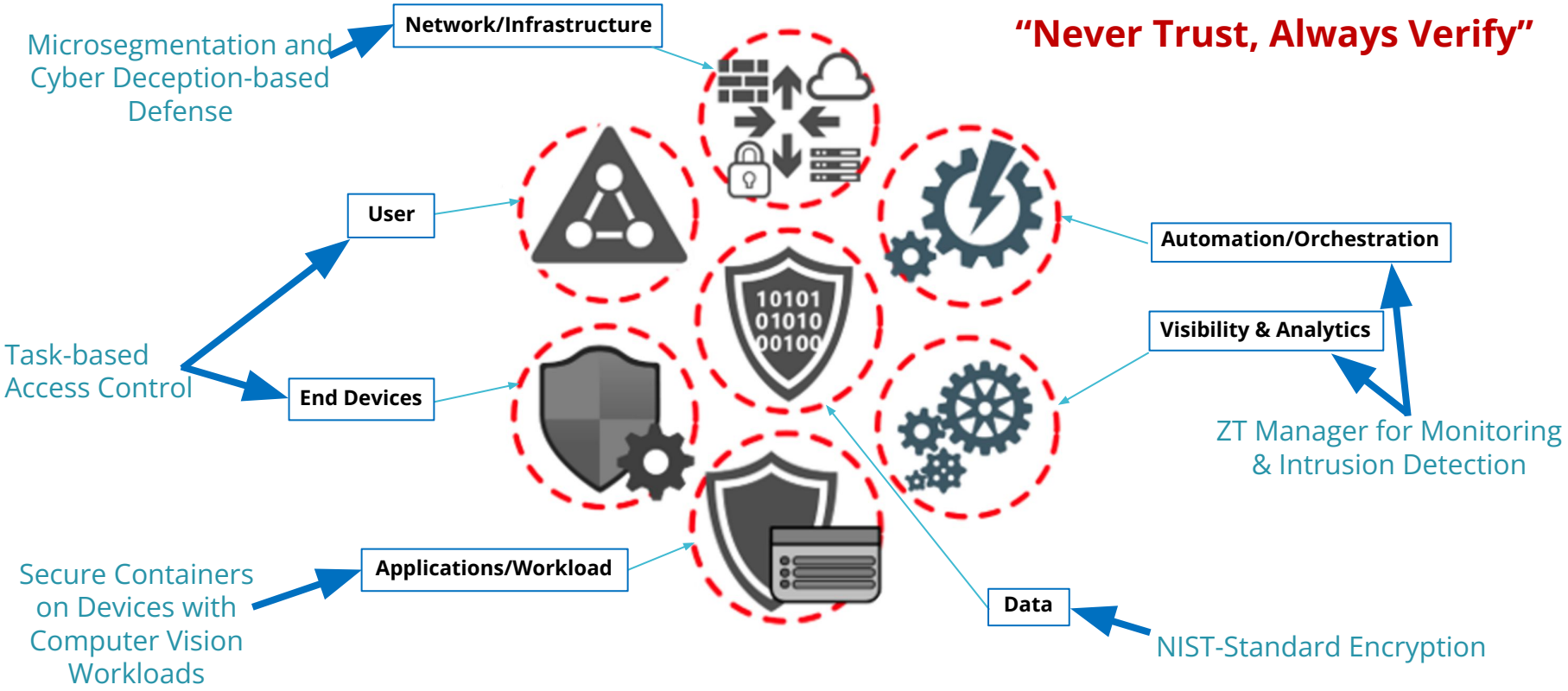


Mission Tasks Carried out by TWE devices in the Internet of Battlefield Things (IoBT) - Stakeholder Scenarios

- **Video data collection, transmission and processing** for real-time situational awareness, decision-making, and strategic intelligence *(highly sensitive task)*
- **Sensor data processing** for surveillance on environmental conditions, target movements, and potential threats, guiding actions, and ensuring operational success
- **Chemical, Biological, Radiological, & Nuclear (CBRN) threat detection** to safeguard civilians, prevent catastrophic incidents, and execute effective response measures in hazardous situations
- **Tracking casualties, injuries, and medical help requirement** ensuring optimal resource allocation, and swiftly delivering life-saving care during missions *(lower sensitive task)*

Liu, Dongxin, et al. "Iobt-os: Optimizing the sensing-to-decision loop for the internet of battlefield things." *2022 International Conference on Computer Communications and Networks (ICCCN)*. IEEE, 2022.
Stocchero, Jorgito Matiuzzi, et al. "Secure command and control for internet of battle things using novel network paradigms." *IEEE Communications Magazine* 61.5 (2022): 166-172.

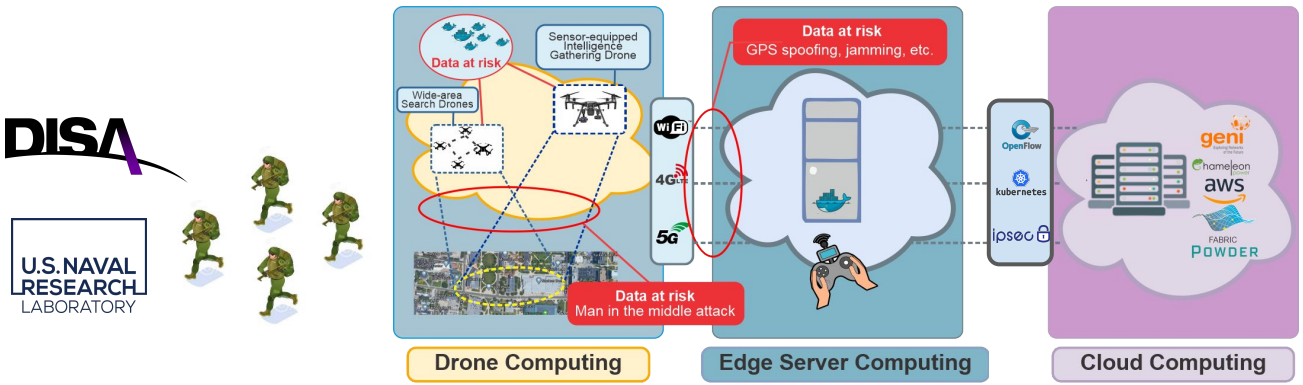
DoD Seven Pillars of Zero Trust: Requirements



Problem Statement - Use Case

Network-edge Connectivity and Computation Security in Drone Video Analytics

- **Drone operations in FANETS are inherently insecure** but need to aid warfighters in scenes of interest
- **Limited resources on UAVs brings additional constraints** on any security scheme that can be applied to the common protocols in the UAV systems
- **Malicious communications, jams or spoofs in Ground Control Station (GCS) signals, or Denial of Service (DoS) attacks or malware that corrupts containerized data collection/processing** - all these disrupt the drones operations (e.g., cause data integrity or loss of privacy issues)



Cyber attacks can target UAV flight networks, GCS communication, or containerized data processing tasks

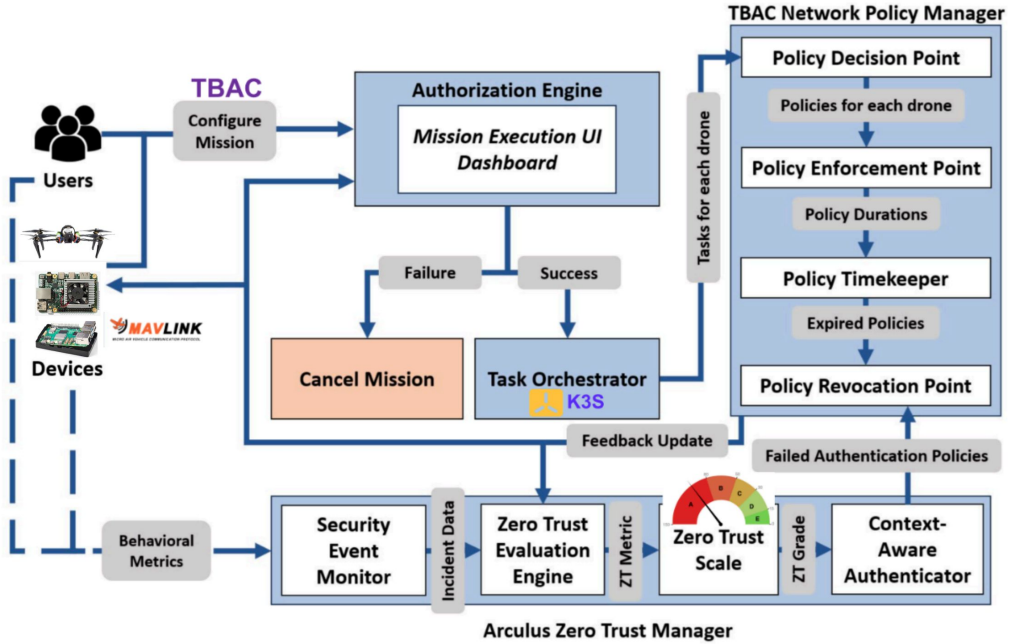
C. Qu, F. Sorbelli, R. Singh, P. Calyam, S. Das, "Environmentally-Aware and Energy-Efficient Multi-Drone Coordination and Networking for Disaster Response", IEEE Transactions on Network and Service Management (TNSM), 2023.

Low-Overhead ZT Architecture of Arculus

with Task-based Access Control at the TWE

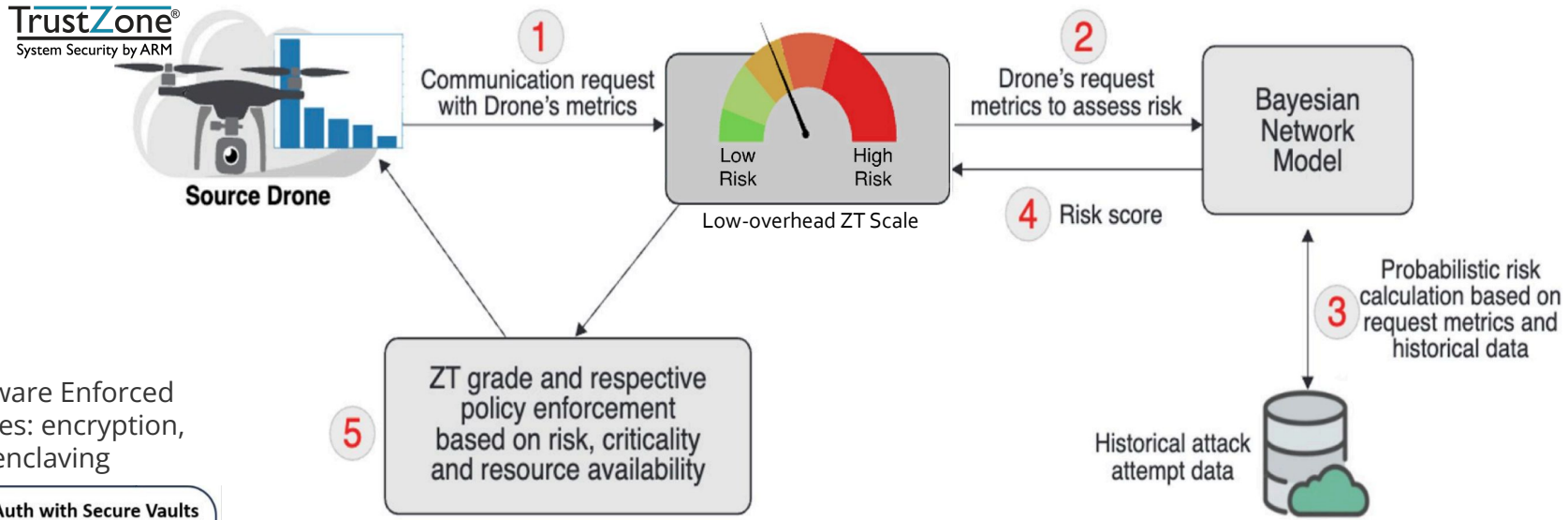
- Reference Architecture
  - Adheres to NIST ZT model guidelines SP 800-207 and SP 800-201
- Low Overhead features
  - Sliding-scale ZT
  - Task-based Access Control
  - K3s Lightweight Kubernetes
  - MAVLink protocol
- Threat agent handling using predictive modeling
  - RL-based drone guidance for safe mission recovery
  - Bayesian network-based risk quantification
  - FedML-based threat detection

Towards implementation for automation of control policies
Listen → Record → Detect → Defend



ARCULUS

Risk Quantification-based Zero Trust Scale
for Tactical Edge Network Environments [*]



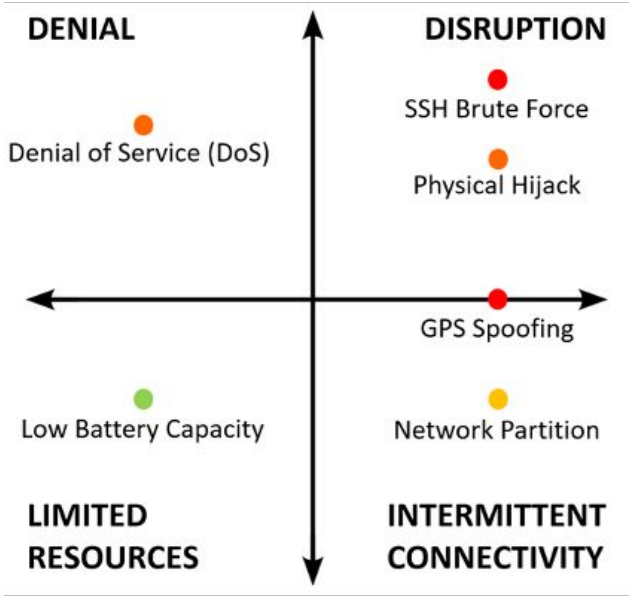
Hardware Enforced Features: encryption, enclaving

- Mutual Auth with Secure Vaults
- Basic Mutual Authentication
- Higher Authentication Rate
- Token-based Authentication
- Basic Lightweight Authentication

[*] S. Poduvu, S. Saghaian N. E., E. Ufuktepe, A. Esquivel Morel, P. Calyam, "Risk-based Zero Trust Scale for Tactical Edge Network Environments", *ACM Trustworthy Edge Computing Workshop, 2023.*

Classification of threats based on DDIL constraints

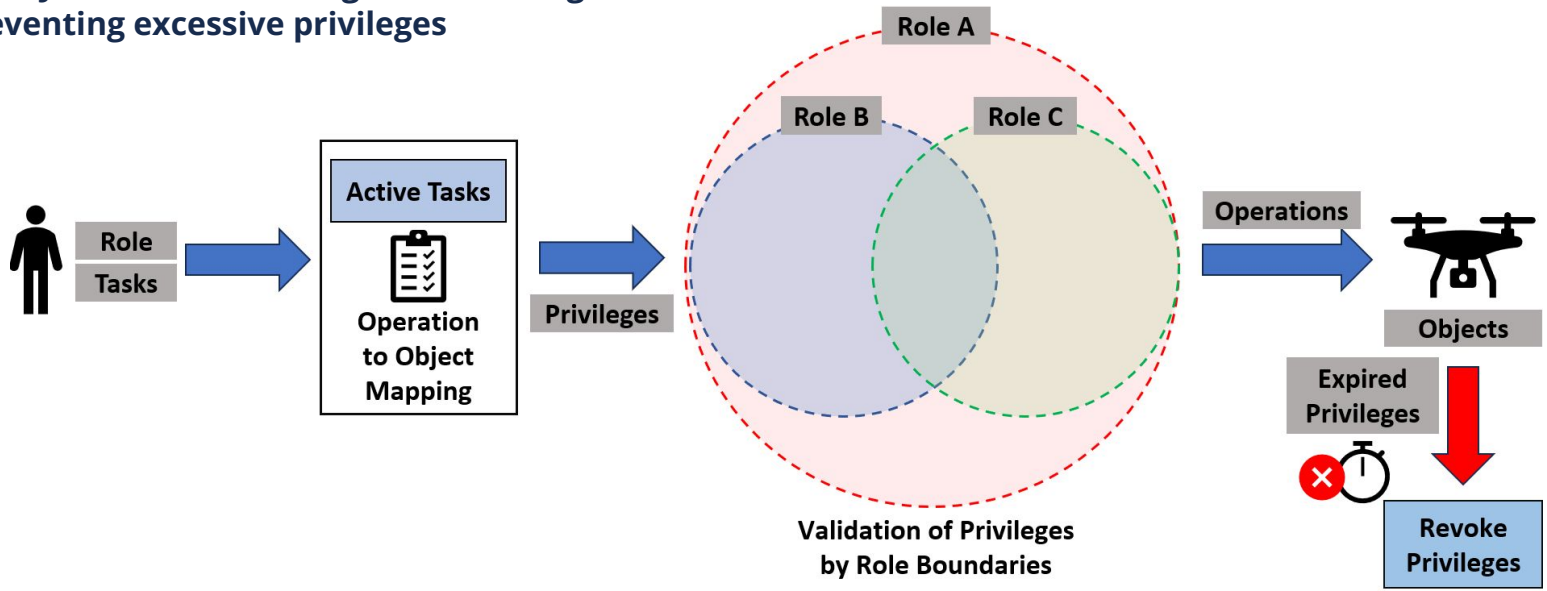
Classifying the modeled threats based on the attack impact they cause on the Tactical Warfighting Edge and mapping them onto the **DDIL Quadrants** can help better understand their quantifiable impact.



An attack like GPS Spoofing can have impact in multiple ways like disrupting the mission execution as well as causing the drone to lose connectivity to the ground control station.

Task-based Access Control for DDIL Cases

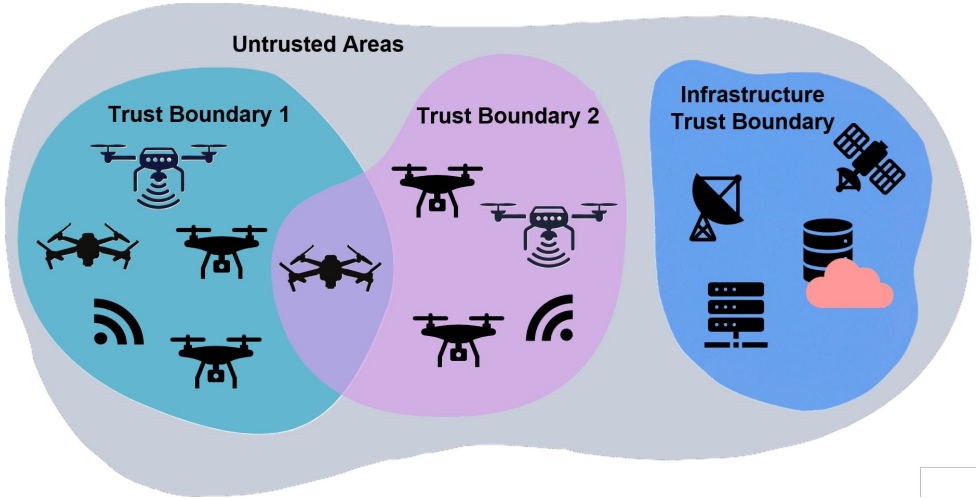
TBAC Just-in-Time Privilege Provisioning preventing excessive privileges



- TBAC on the other hand, considers the **necessity of privileges based on tasks** and the provision of these privileges are **validated by the trust boundary of RBAC** configuration
- Through TBAC configuration, network policies are assigned **Just-in-Time (JIT) access**, ensuring that communication channels remain open only for the duration they are needed, mitigating the causes for excessive privileges

S. Poduvu, R. L. Neupane, A. E. Morel, R. Mitra, V. Anand, R. Chadha, P. Calyam, "Task-Based Access Control for Computation and Communication in the Tactical Warfighting Edge". IEEE Military Communications Conference (MILCOM) 2024.

Trust Boundaries in DDIL Environments



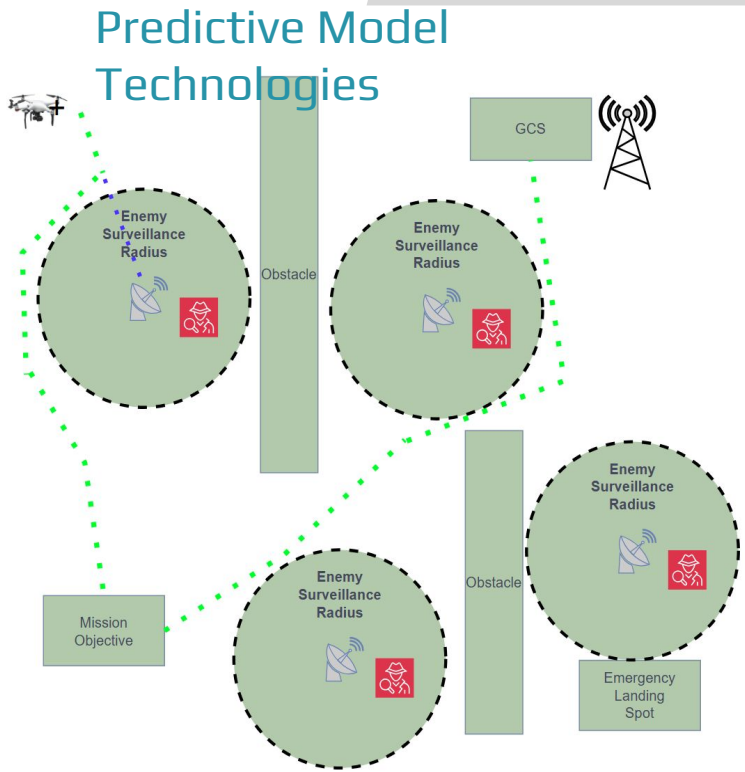
Trust boundary is an imaginary perimeter in a DDIL environment where a set of devices tasked to complete a mission have been vetted, authenticated and provisioned. As devices move between trust boundary's role hierarchies change. Tasks are determined within highly fluid trust boundaries (1 and 2)

Each trust boundary can implement

- Its own policy of device authentication
- Role hierarchy
- Policy for seeking support from Infrastructure
- Policies of data movement within the boundary, with another trusted boundary and untrusted region

Reinforcement Learning for Drone Guidance

- A novel Intelligent Drone Trajectory Management (IDTM) model to ensure optimal drone trajectory planning in scenarios of lost network connectivity with the GCS
- The drone may choose to:
  - Proceed to complete Mission Objective or,
  - Divert to an emergency landing spot or, Return to the GCS
- IDTM model uses a Reinforcement Learning with a focus on Q-learning to leverage state representations to adapt to uncertain conditions; uses:
  - Drone's position
  - Mission completion status
  - Drone proximity to Enemy Surveillance Zones
  - General drone direction
  - GCS/drone network status

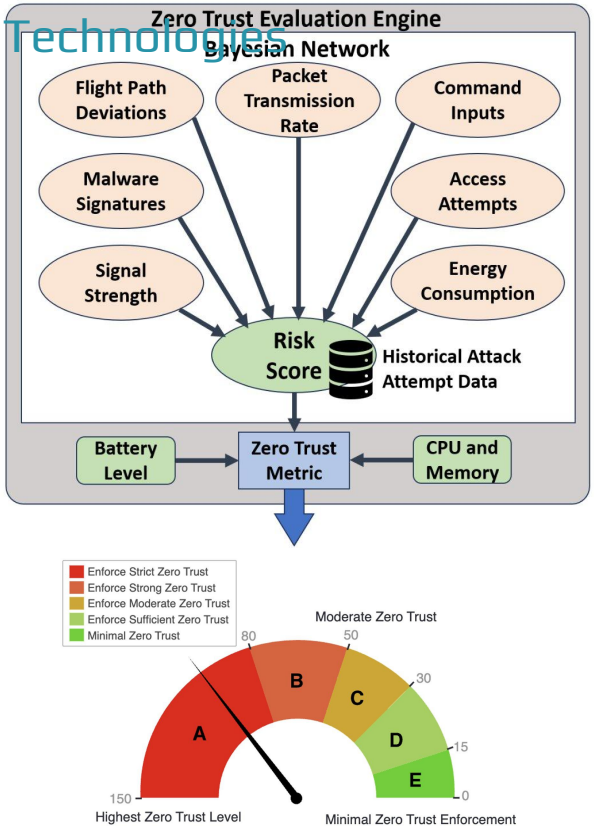


C. Bhamidipati, A. Maxwell, E. Pham, J. Zhang, Z. Murry, A. Morel, C. Qu, S. Srinivas, P. Calyam, "Q-Learning-Based Dynamic Drone Trajectory Planning in Uncertain Environments", IEEE International Conf. on Computing, Networking and Communications (ICNC), 2025.

Bayesian network for Risk Quantification

- Bayesian network for probabilistic risk scoring that assesses behavioral metrics
- Risk score, onboard battery, TWE resources, etc.
- These values help generate ZT metric to define appropriate security level
  (A: Most stringent, E: Most lenient)
- Risk score is computed by considering all possible combinations of states across the input signals
  - such as flight path deviation, packet transmission rate, etc.

Predictive Model Technologies

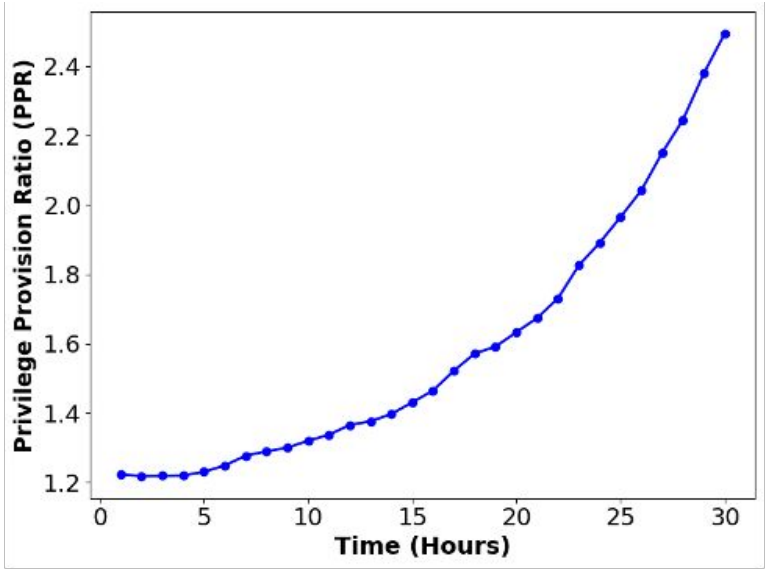


RBAC vs. TBAC Performance Evaluation

- Evaluation of TBAC's efficiency in comparison with RBAC in preventing provisioning of unnecessary privileges under the same device and mission circumstances.

- We introduce Over-provisioned Privilege Percentage (OPP) that calculates the percentage of over-provisioned privileges (RBAC vs TBAC)

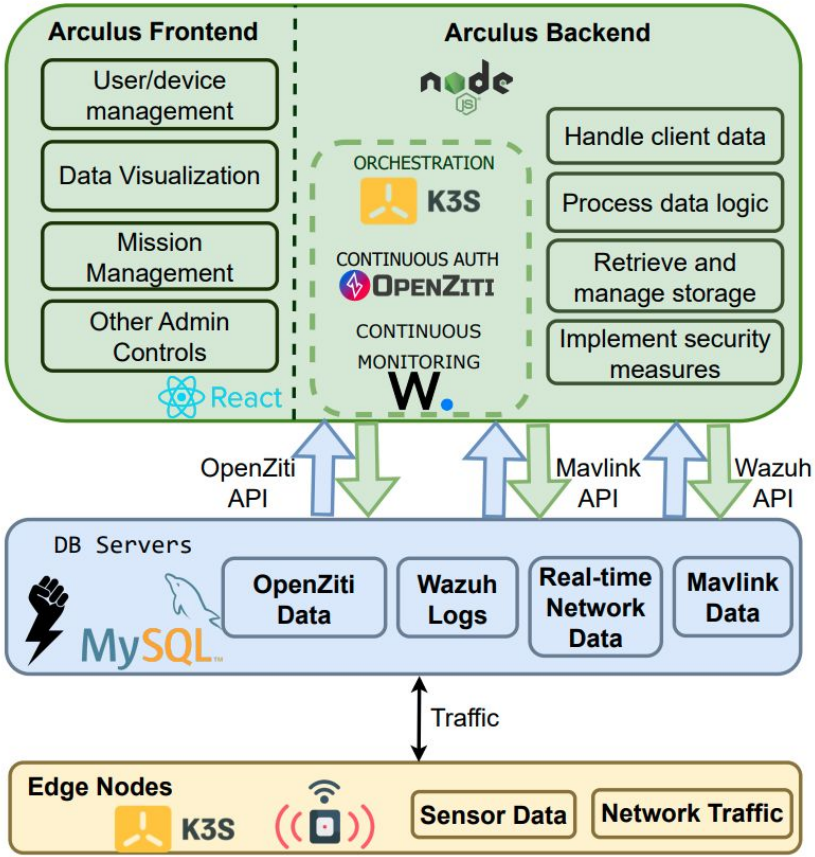
$$OPP = \frac{\sum_{t=0}^{60} P_{RBAC}(t) - \sum_{t=0}^{60} P_{TBAC}(t)}{\sum_{t=0}^{60} P_{TBAC}(t)} \times 100\%$$



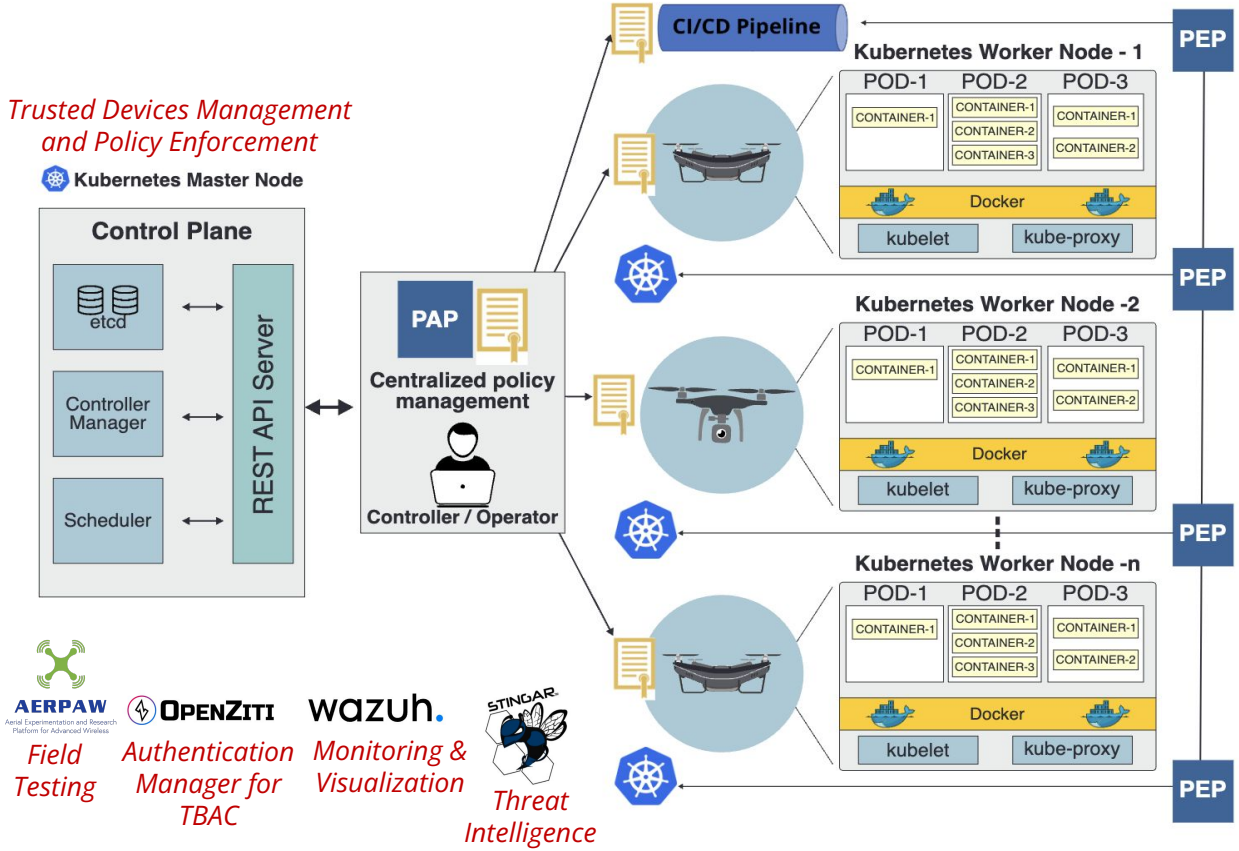
Privilege Provision Ratio (PPR) of RBAC to TBAC over a 30-hour period with gradual addition of new drones.

Technology Stack

- **Integrated Architecture**: Combines frontend user interfaces, backend processing, and edge nodes for seamless data flow
- **Lightweight Orchestration**: Uses K3s for efficient container management and scalability
- **Secure Data Handling**: Implements OpenZiti for authentication, Wazuh for monitoring, and end-to-end encryption
- **Edge and Centralized Systems**: Real-time data processing at edge nodes with centralized logging and analytics
- **APIs**: Facilitates secure communication and integration across components

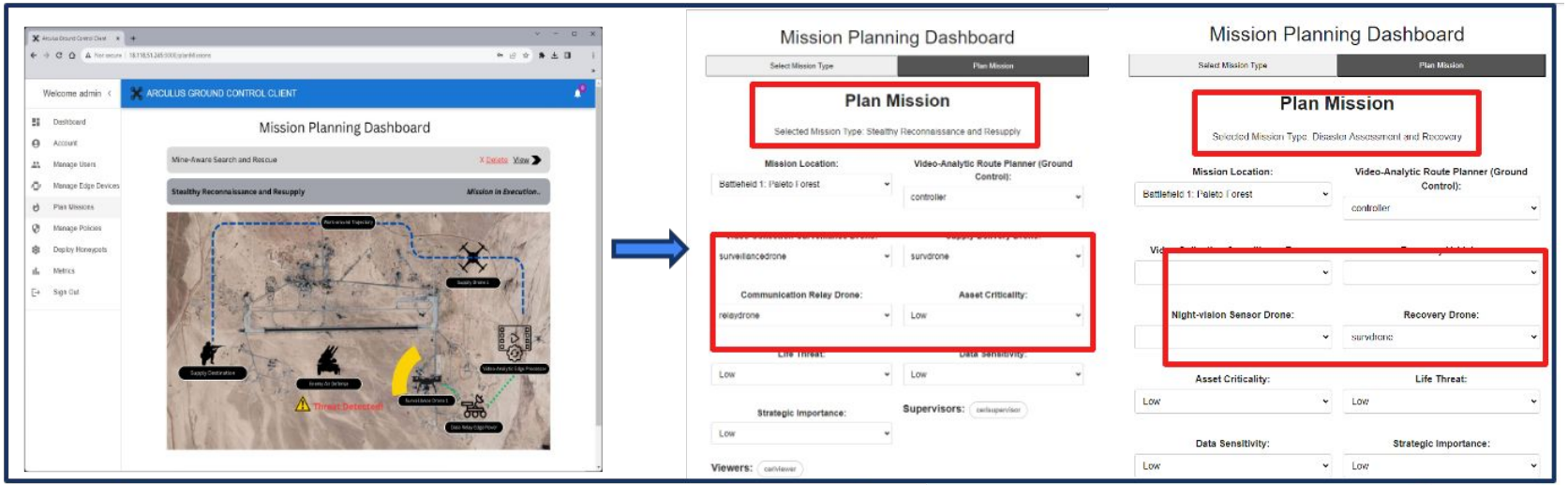


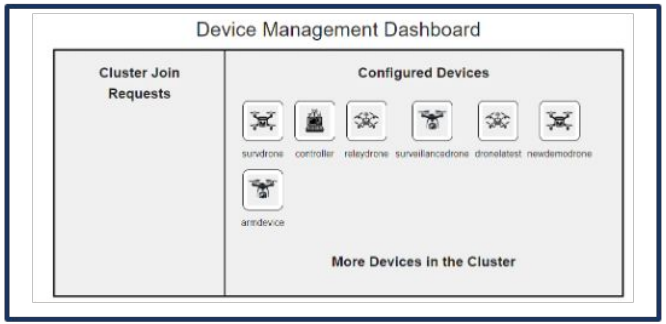
Arculus Cloud/Hardware Testbed

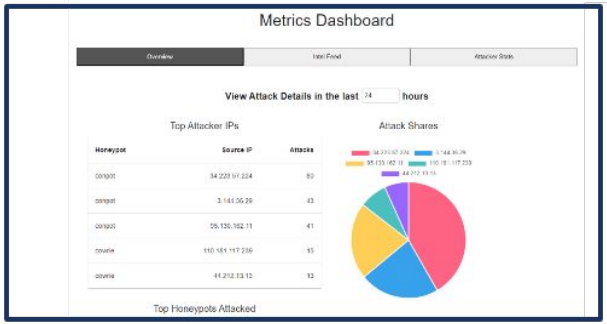


- Used for **Simulation, Field Testing, Hardware-based Experiments**
- **Monitoring methodologies** adapted for programmable network services deployment and their management, including credentials/commands used on edge devices (e.g., Raspberry pi)
- **Enforcing low overhead security controls** by using TBAC, MAVLink, & micro-segmentation using Kubernetes (k3s)
- **Integrating Defense by Pretense methodologies** with distributed honeypots that can report intrusion attempts, verify legitimate or misconfiguration actions

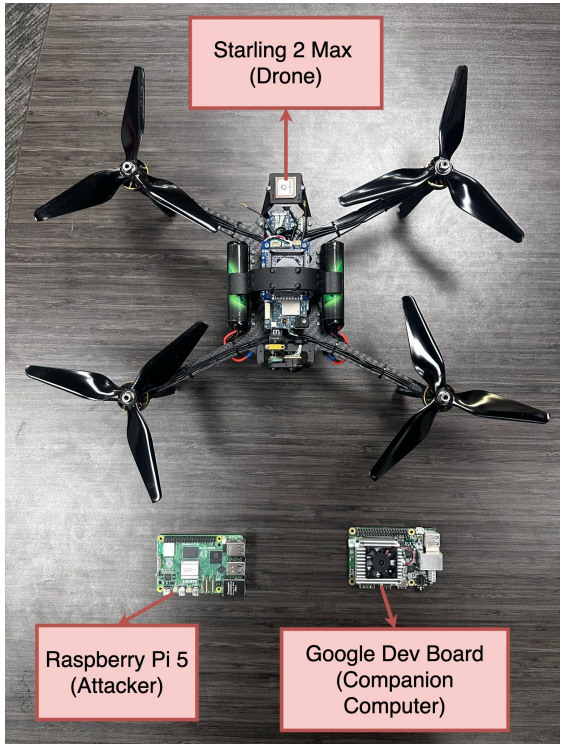
Arculus Simulation Testbed

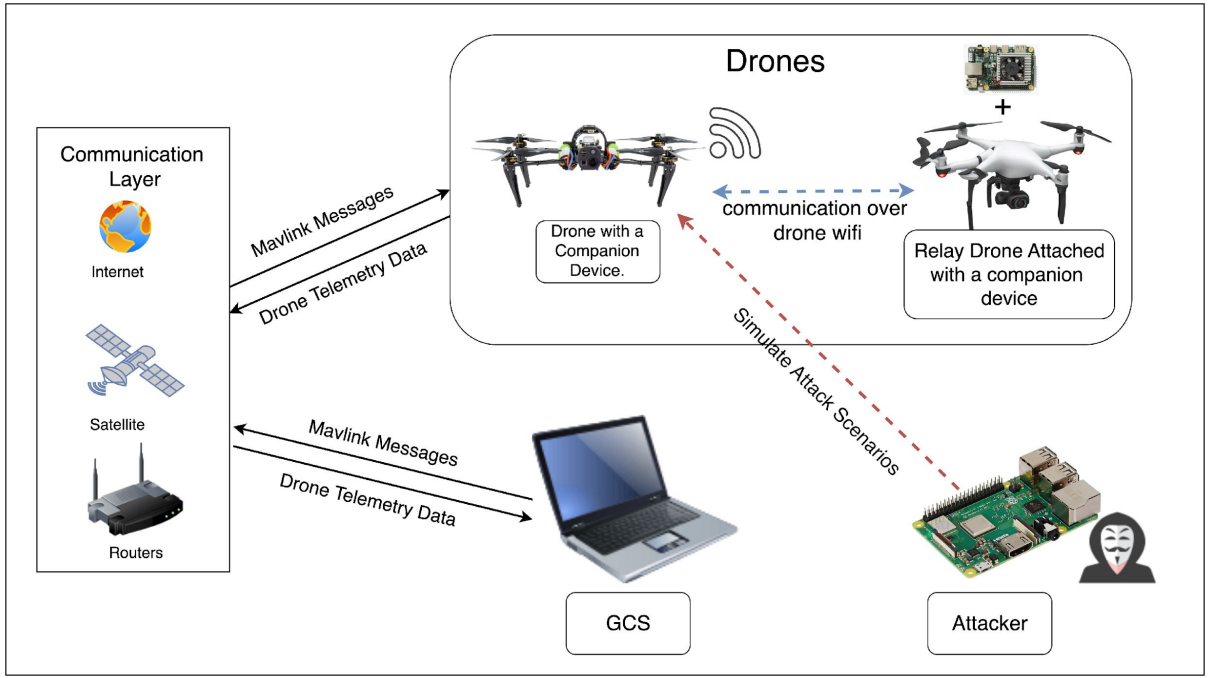




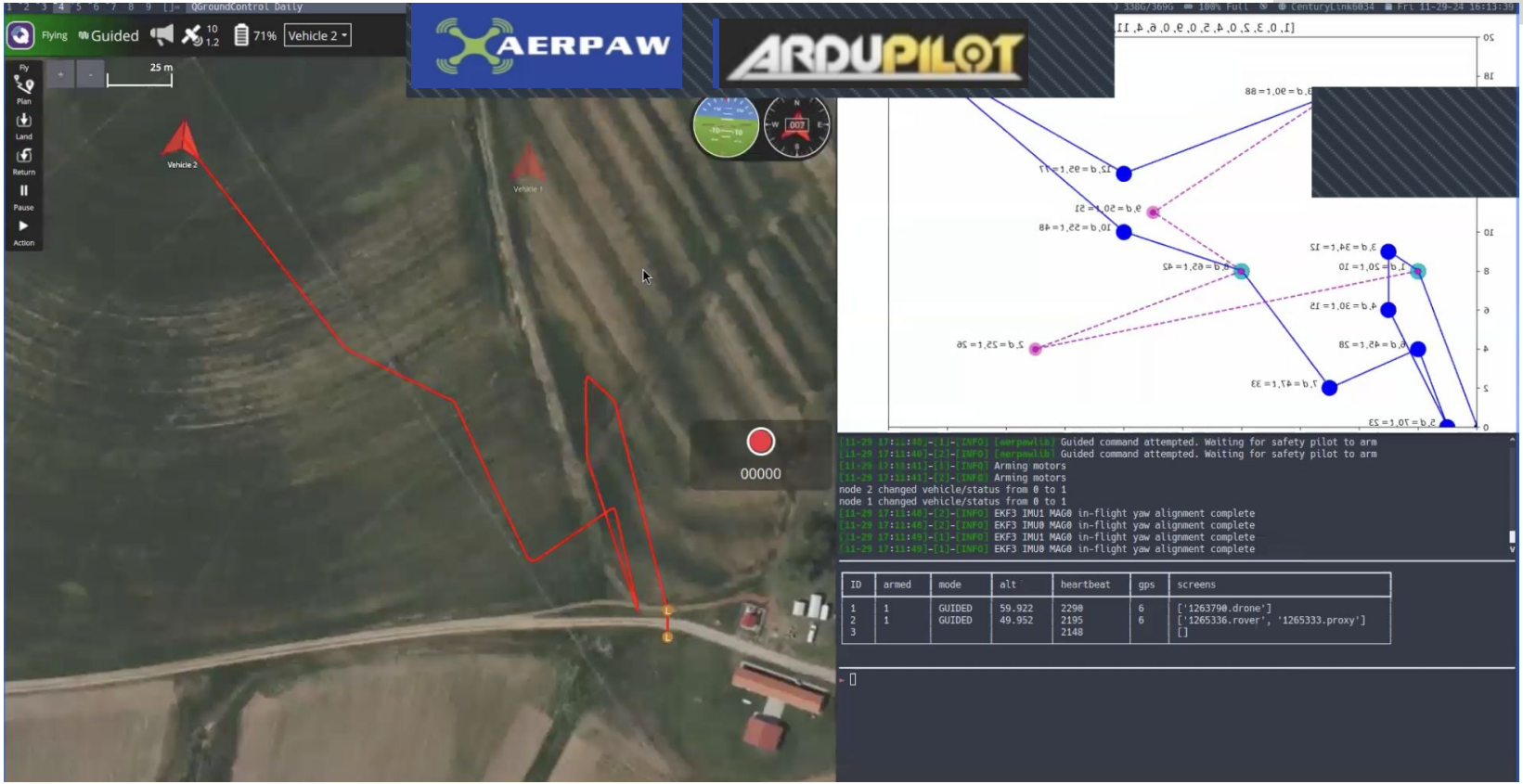


Arculus Physical Hardware Testbed

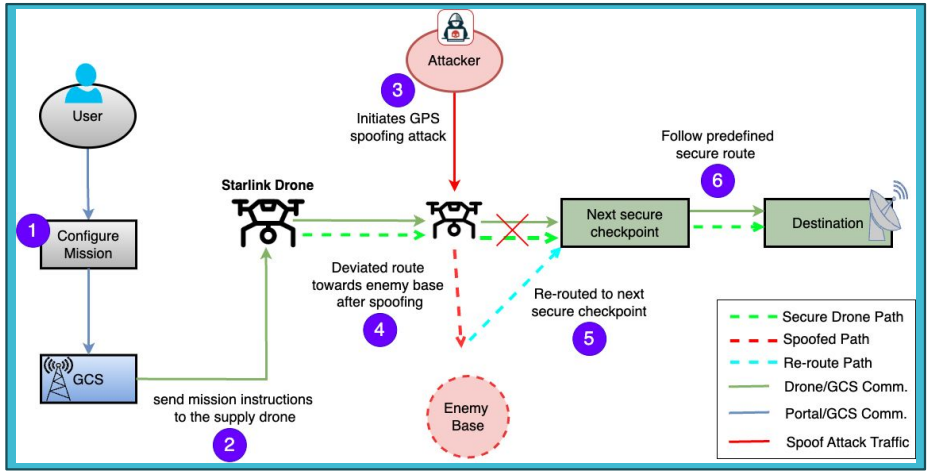




Mission Adaptation to ensure Data Integrity

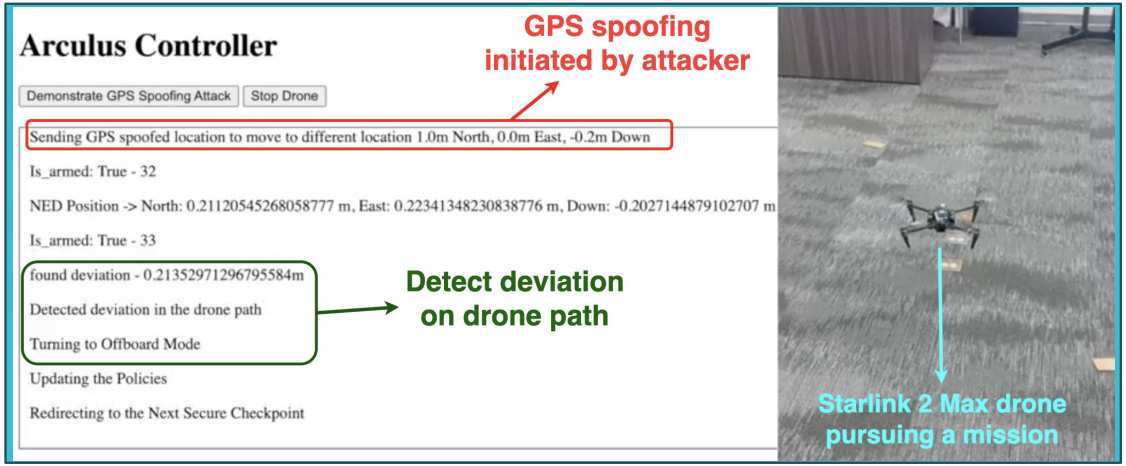


TWE Attack Scenario: Drone under GPS Spoofing

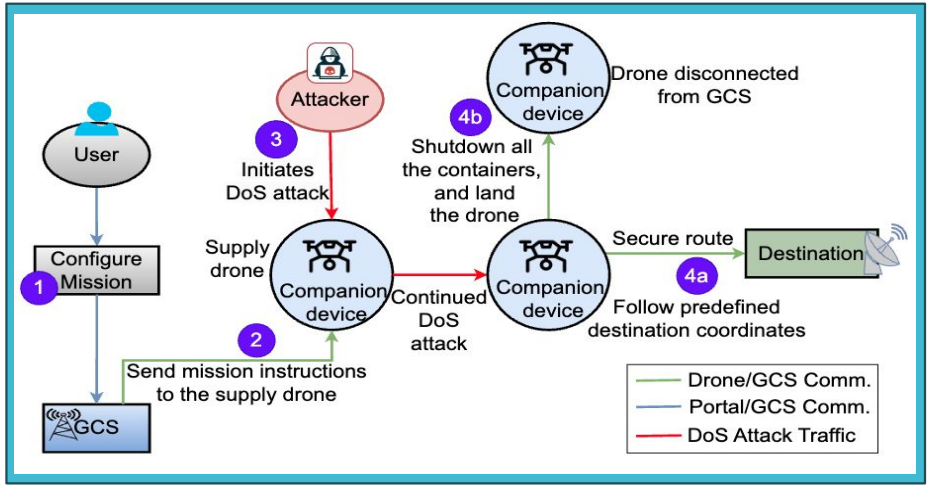


Drone mission scenario flow under GPS spoofing

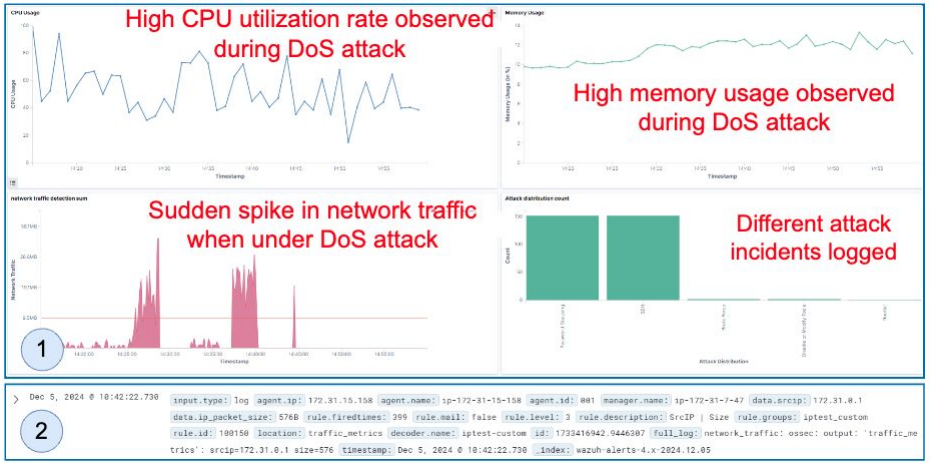
Hardware Experimentation using Starlink 2 Max Drone for GPS Spoofing Detection and Mitigation via Drone Path Adaptation



TWE Attack Scenario: Drone under DDOS



Drone mission scenario flow under DDoS attack



SIEM agent monitoring anomaly events for using mitigative measures to block attacker's IP using OpenZiti (1: visualization; 2: raw logs)

Conclusion

- Presented a novel low-overhead zero trust reference architecture to move defense strategies away from static network perimeters, and focus on users, assets, and resources at the TWE

- Presented an AI-driven predictive model featuring Reinforcement learning-based Intelligent Drone Trajectory Planning (IDTM) for safe mission recovery under adversarial threat related incidents

- Discussed software stack developed following the ZT reference architecture and hardware testbed configuration for showcasing mission under normal operation and under attack scenarios

Future directions

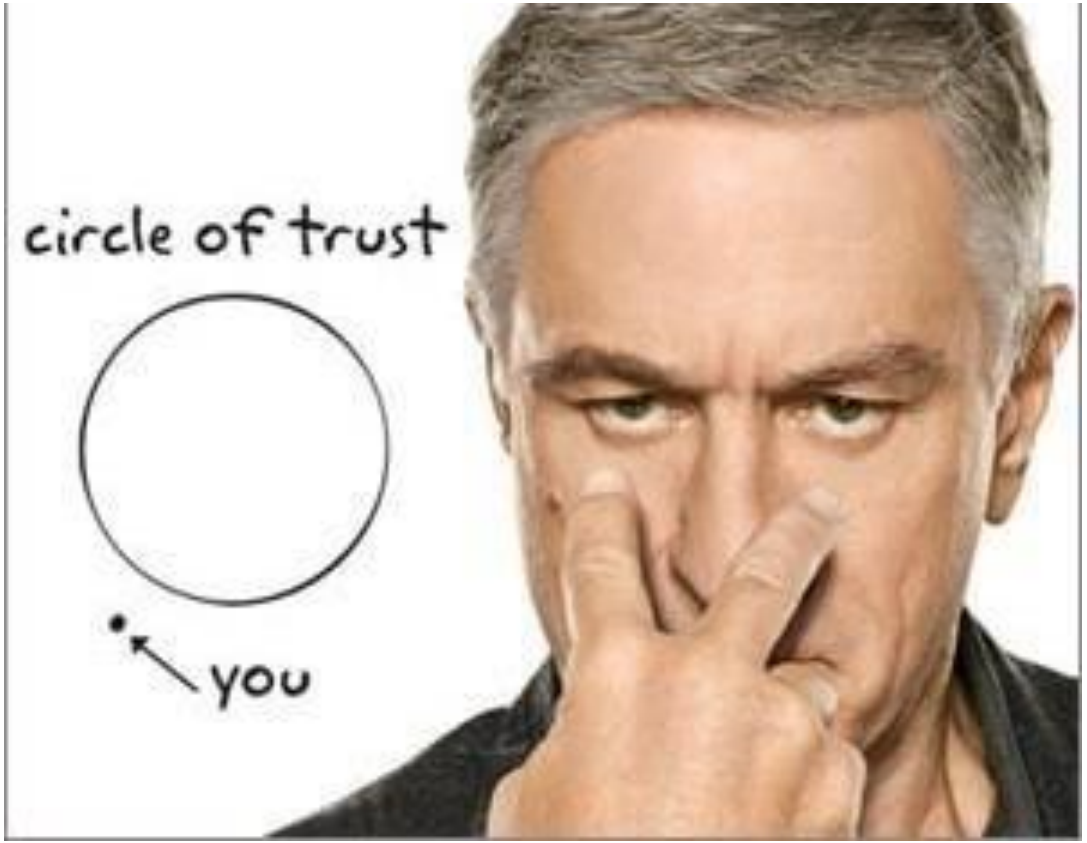
- Automating ZT with seamless control - Design effective feedback based on dynamic ZT score calculation as per battlefield situation, mission goals and device resource constraints

- Standardize the mission planning framework to make it adaptable to other critical mission


University of Missouri
Mizzou CERI
Center for Cyber Education, Research & Infrastructure
Thanks for your attention!
Any questions?
Contact: Prof. Prasad Calyam (PI)
(calyamp@missouri.edu)
Department of Electrical Engineering and Computer Science, University of Missouri-Columbia

Steven Turner

Zero Trust: Because Trust Issues Aren't Just for Relationships

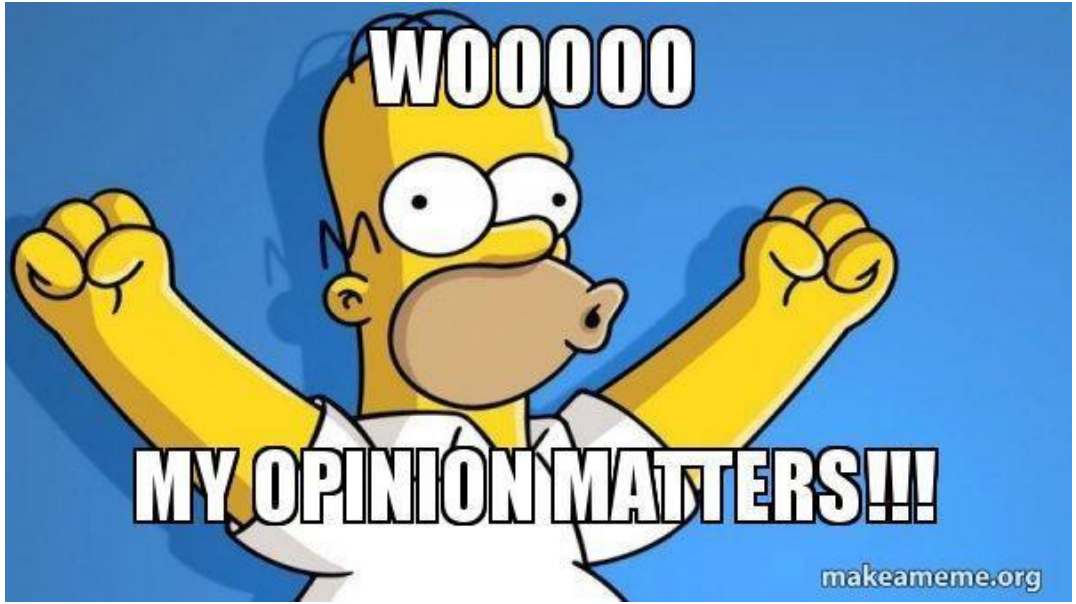




whoami

- Current: Security @ Microsoft
- 17 years in cybersecurity
- Previous industries: financial, managed services, waste management, research, and tech
- Experience: Identity, Endpoints, Cloud, and more!

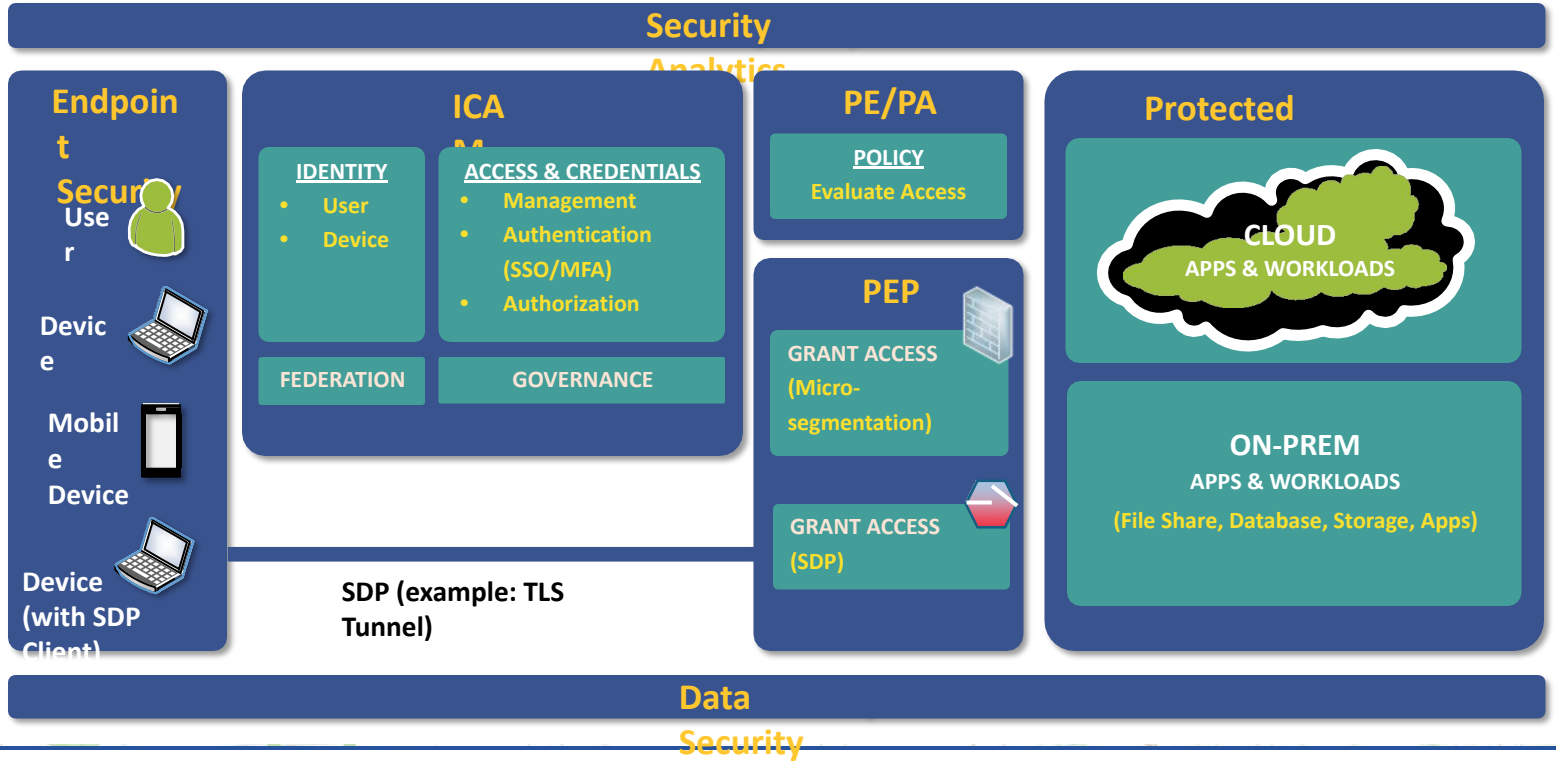
All Opinions s Statement s Are My Own



How’s implementation going? It’s complicated



Notional ZTA Architecture



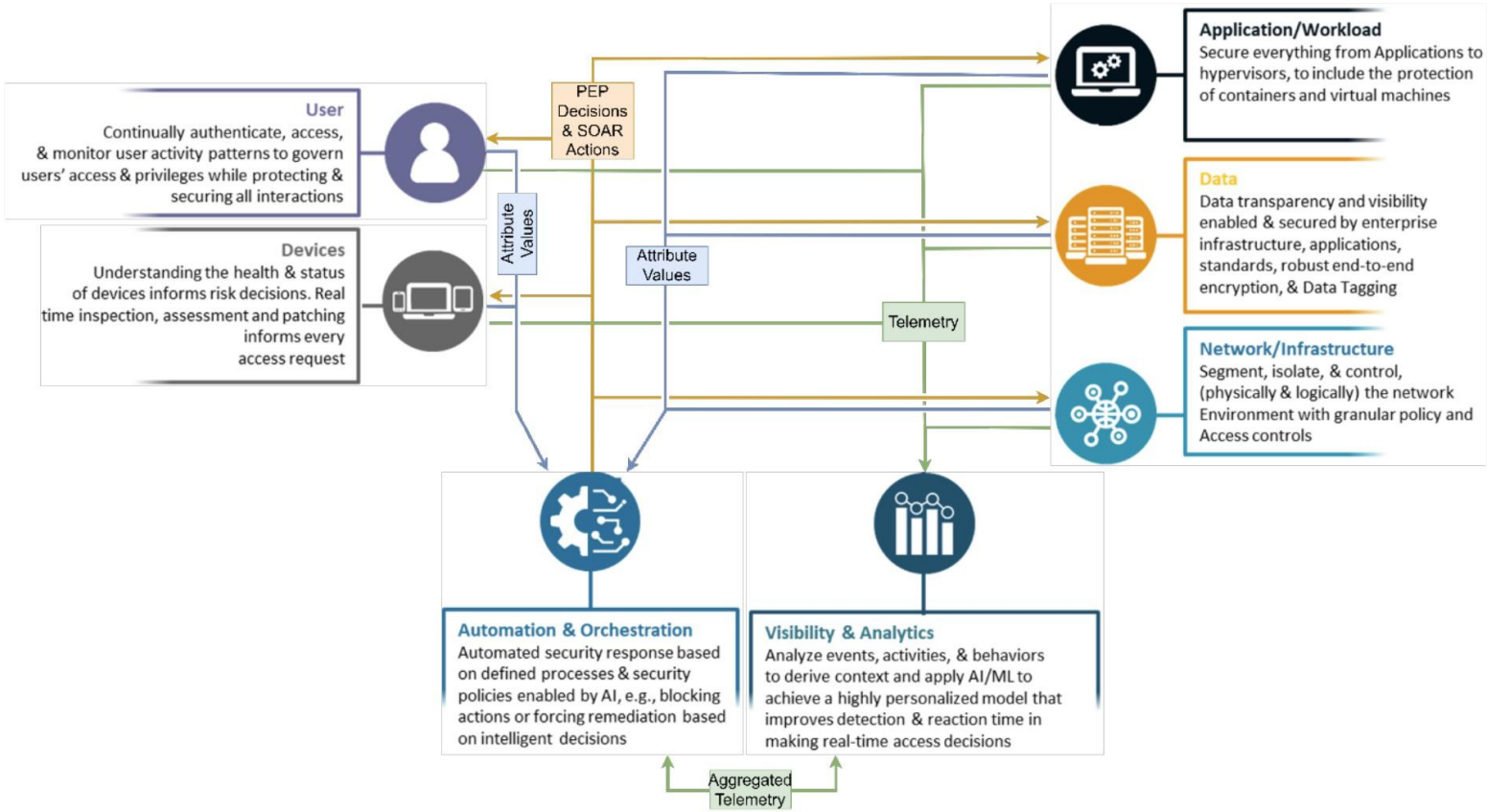
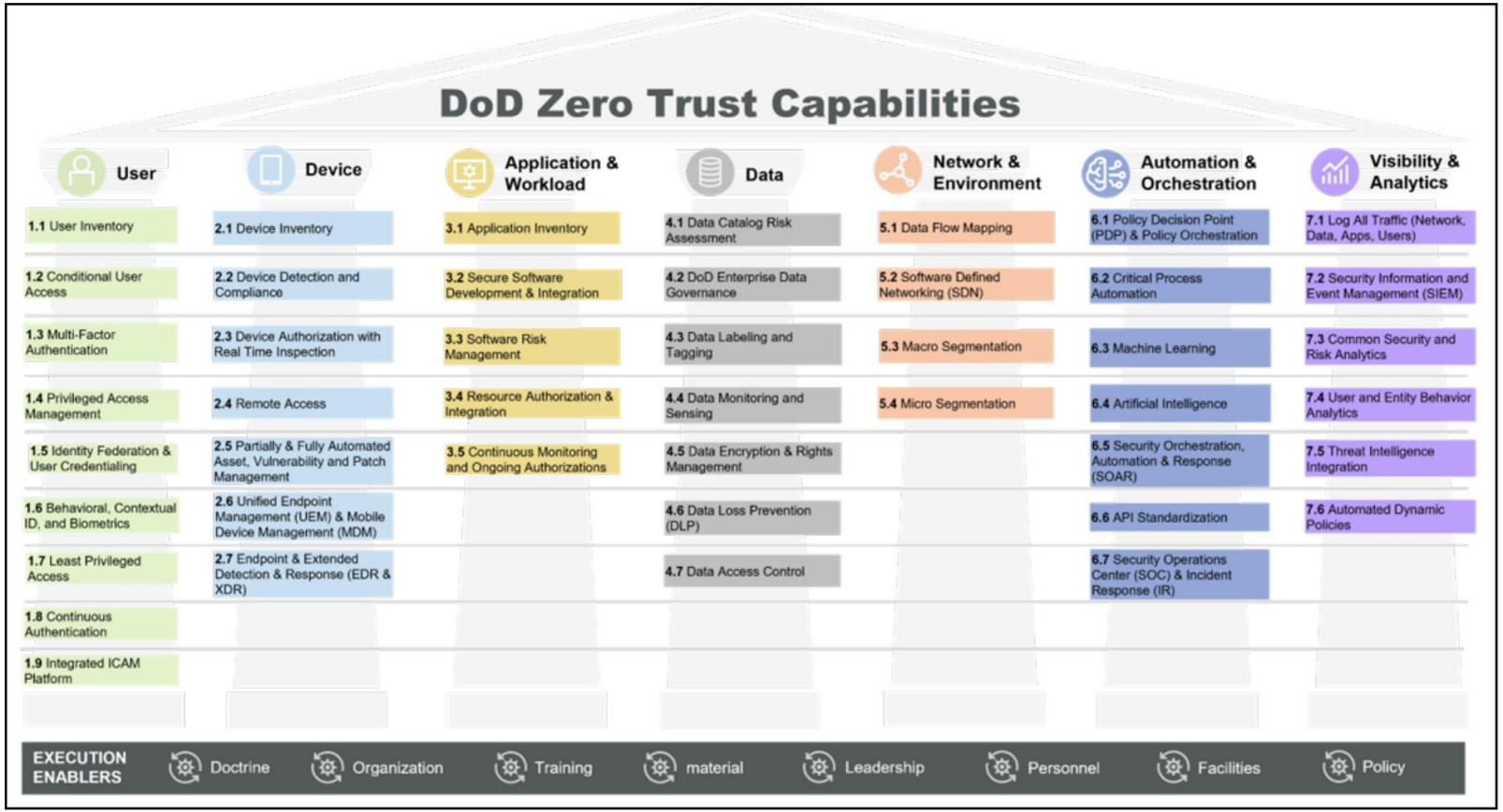
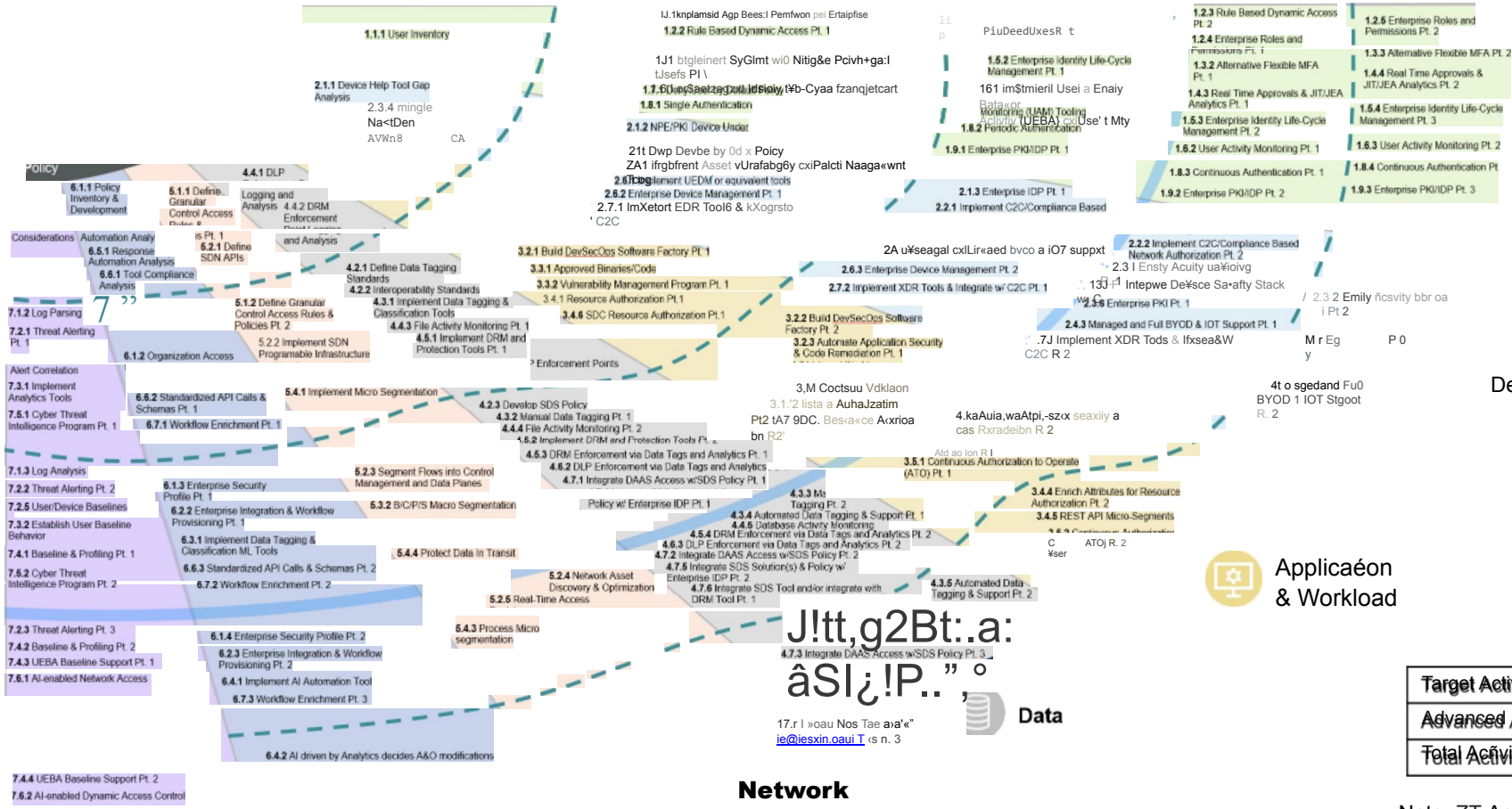


Figure 3. Zero Trust Integration and Interoperability


DoD Zero Trust Capabilities
User
1.1 User Inventory
1.2 Conditional User Access
1.3 Multi-Factor Authentication
1.4 Privileged Access Management
1.5 Identity Federation & User Credentialing
1.6 Behavioral, Contextual ID, and Biometrics
1.7 Least Privileged Access
1.8 Continuous Authentication
1.9 Integrated ICAM Platform
Device
2.1 Device Inventory
2.2 Device Detection and Compliance
2.3 Device Authorization with Real Time Inspection
2.4 Remote Access
2.5 Partially & Fully Automated Asset, Vulnerability and Patch Management
2.6 Unified Endpoint Management (UEM) & Mobile Device Management (MDM)
2.7 Endpoint & Extended Detection & Response (EDR & XDR)
Application & Workload
3.1 Application Inventory
3.2 Secure Software Development & Integration
3.3 Software Risk Management
3.4 Resource Authorization & Integration
3.5 Continuous Monitoring and Ongoing Authorizations
Data
4.1 Data Catalog Risk Assessment
4.2 DoD Enterprise Data Governance
4.3 Data Labeling and Tagging
4.4 Data Monitoring and 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
5.2 Software Defined Networking (SDN)
5.3 Macro Segmentation
5.4 Micro Segmentation
Automation & Orchestration
6.1 Policy Decision Point (PDP) & Policy Orchestration
6.2 Critical Process Automation
6.3 Machine Learning
6.4 Artificial Intelligence
6.5 Security Orchestration, Automation & Response (SOAR)
6.6 API Standardization
6.7 Security Operations Center (SOC) & Incident Response (IR)
Visibility & Analytics
7.1 Log All Traffic (Network, Data, Apps, Users)
7.2 Security Information and Event Management (SIEM)
7.3 Common Security and Risk Analytics
7.4 User and Entity Behavior Analytics
7.5 Threat Intelligence Integration
7.6 Automated Dynamic Policies
EXECUTION ENABLERS
Doctrine
Organization
Training
material
Leadership
Personnel
Facilities
Policy



Target Activities	91
Advanced Activities	61
Total Activities	152

Note: ZT Activities are group as either Target or Advanced - Dotted Lines signi@ the original 5 phases

Implementation Challenges

- Technology Choices (lack of differentiation)
- Policies
- Actions
- Organization
- Processes



Technology Choices

- Platform vs Point Solution
- Lack of standard API’s
- Device Risk vs User Risk vs Session Risk
- Continuing to use known vulnerable technology

Policy Enforcement

- Still so many policies and configurations
- Policy Administration/Decision/Enforc ement Uniformity
- Lack of information still informing access decisions



Actions

- Taking a bludgeoning approach to enforcing security (whack a mole, heavy handed)
- Security is the enemy of the mission
- Operational impact



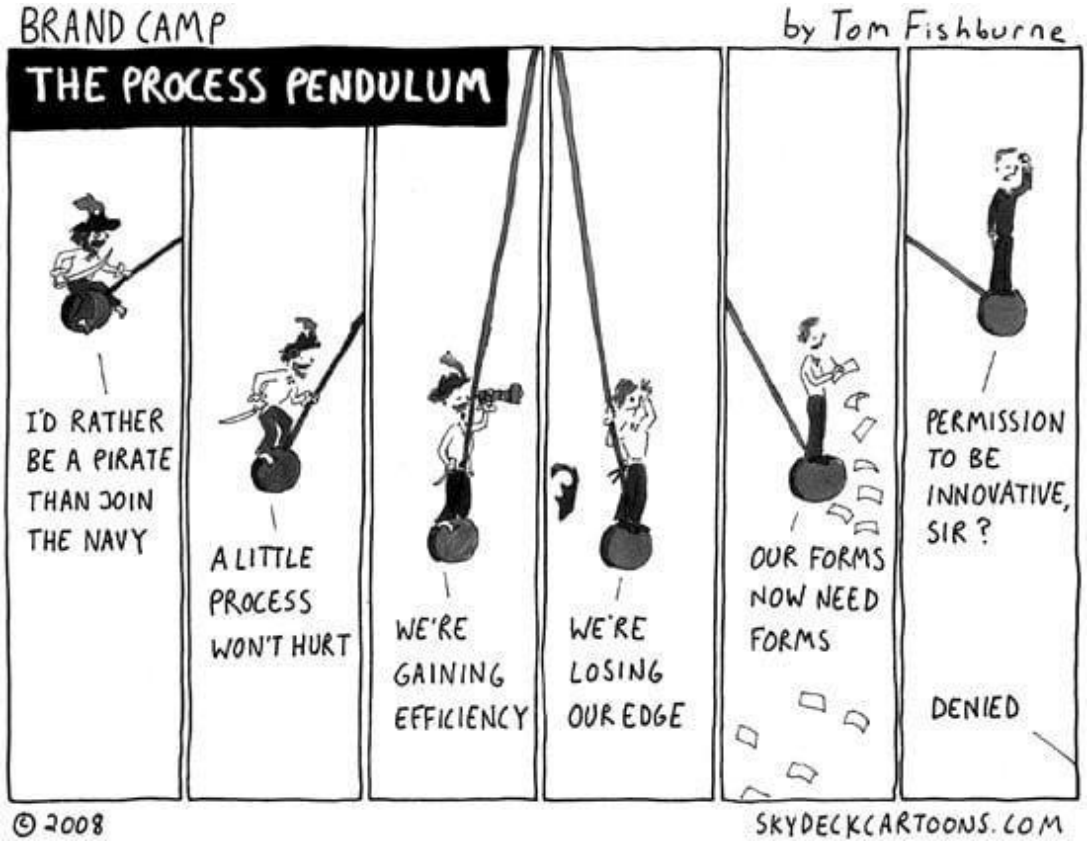
Organizatio
n

- Silos galore
- Misaligned priorities
- Stopping before even starting
- Politics



Processes

- Process for the sake of process
- Don't lift and shift should apply to process
  - Processes getting in the way of progress



Commitment is Hard, Boundaries are okay



1. Define your Protect Surface

2. Map the Transaction Flows

3. Architect a Zero Trust Environment

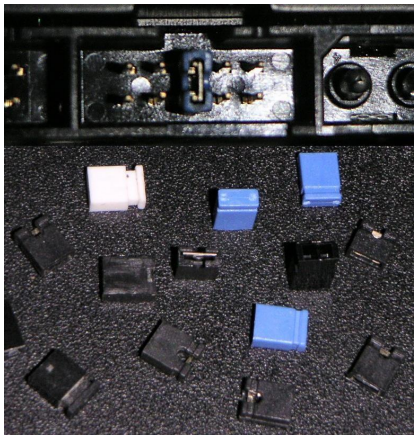
4. Create Zero Trust Policy

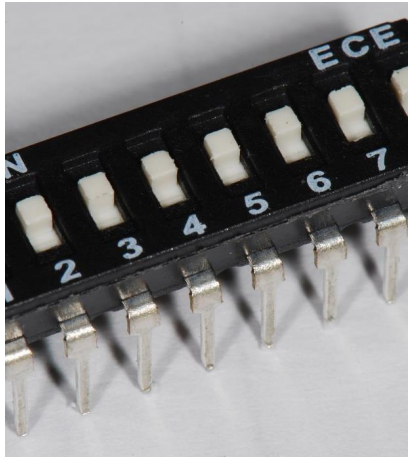
5. Monitor and Maintain the Network

Modular Architectu

re

- , use existing tools where possible, but you aren’t stuck with it
- Integrations of value vs closed ecosystem w/ minimal integration
- Don’t box yourself into something kludgy
- THERE ARE SOLUTIONS OUT THERE **THAT FIT THIS**







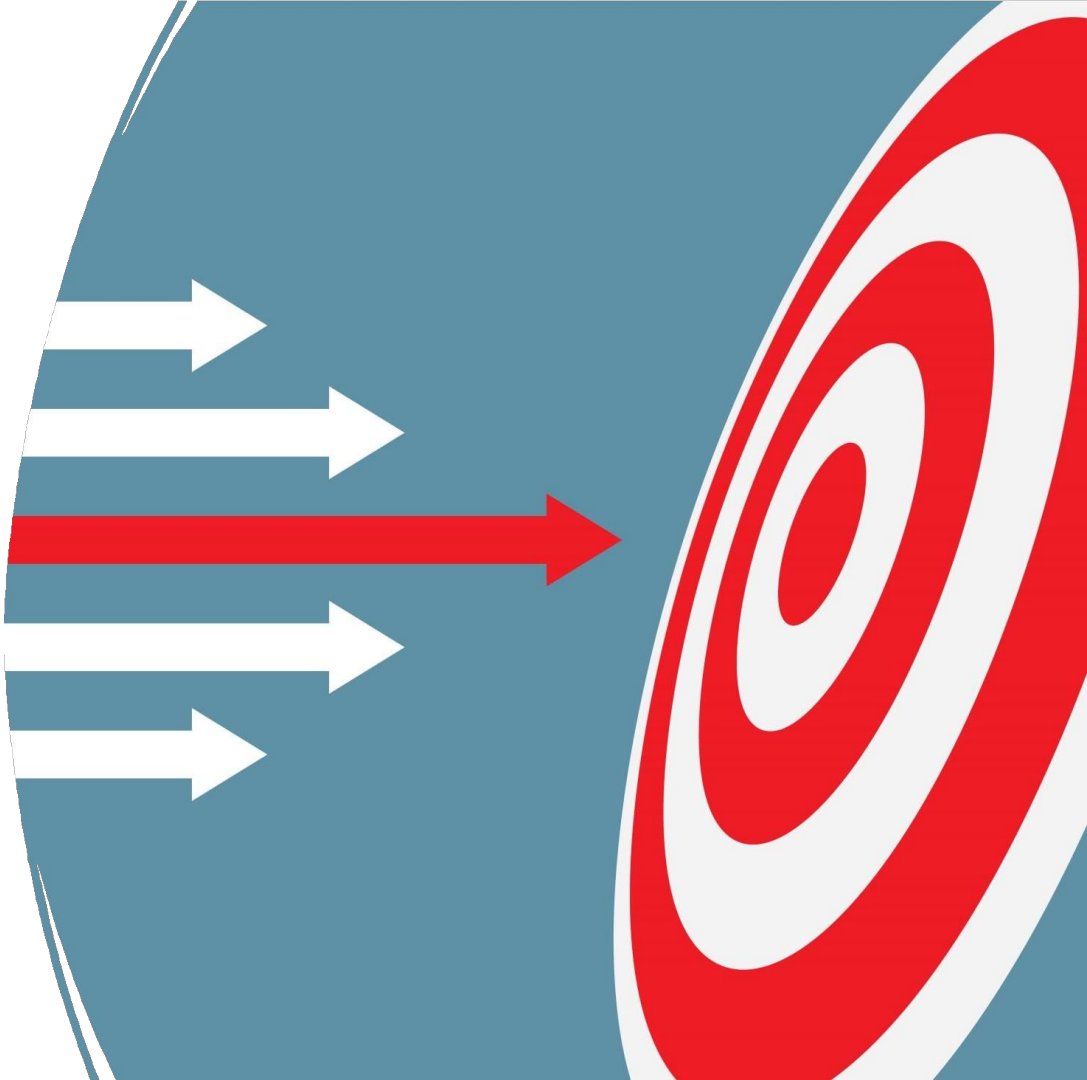
True Partnership

- Taking the full stack development model to security
- People who understand the mission, securing the mission, and how technology intersects with that
- Subject matter experts are still critical
- Cross functional teams reign supreme



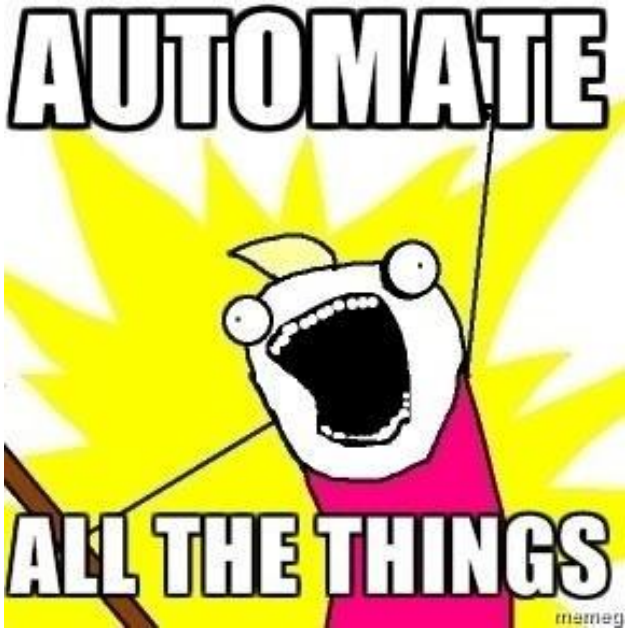
Innovation

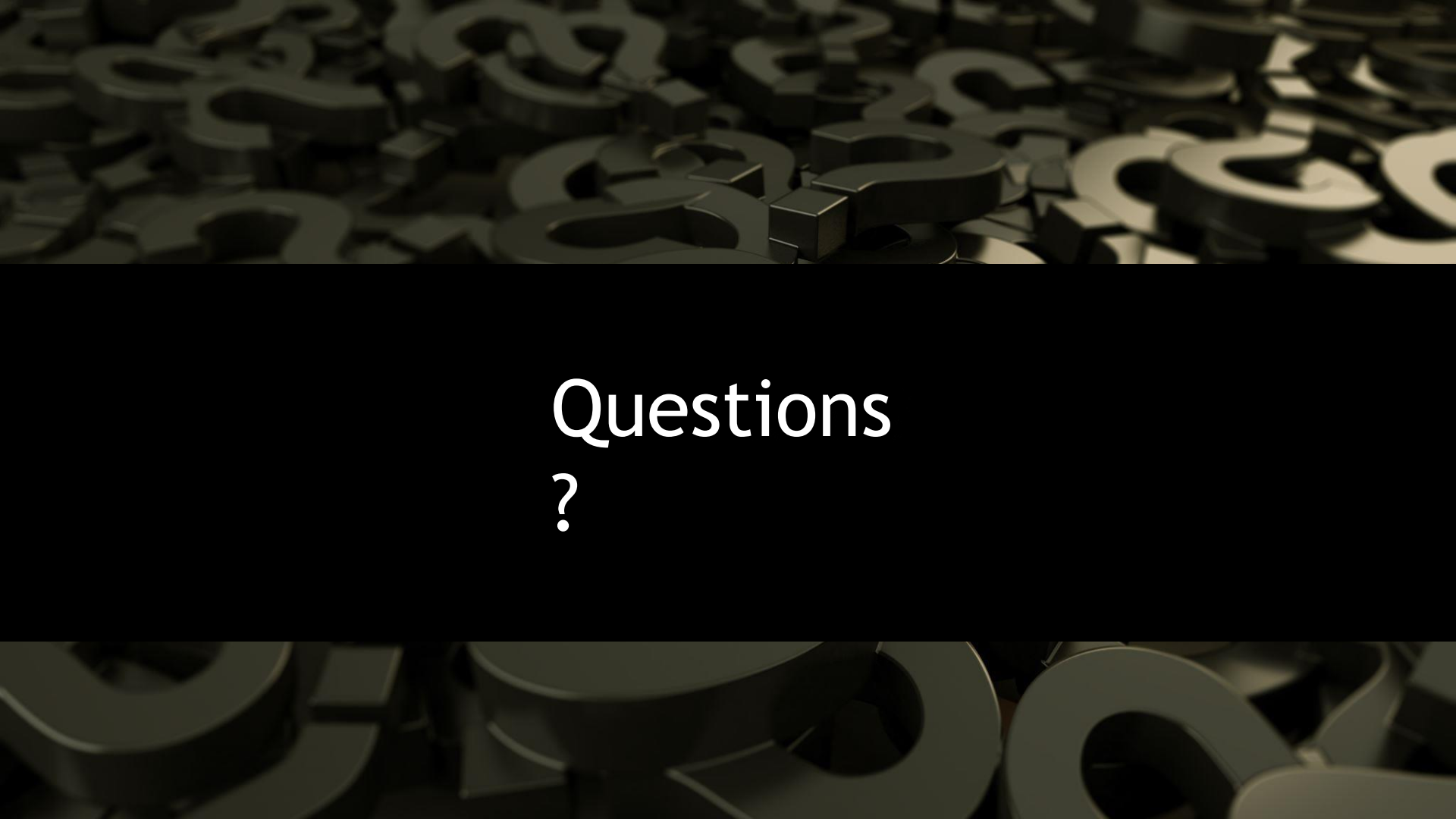
- Automated Moving Target Defense (Attack Disruption)
- Data Security Posture Management (DSPM)
- Exposure Management (CTEM, CNAPP, CSPM, etc)
- Automated Context (empty subscriptions, HR system, permutations of access)

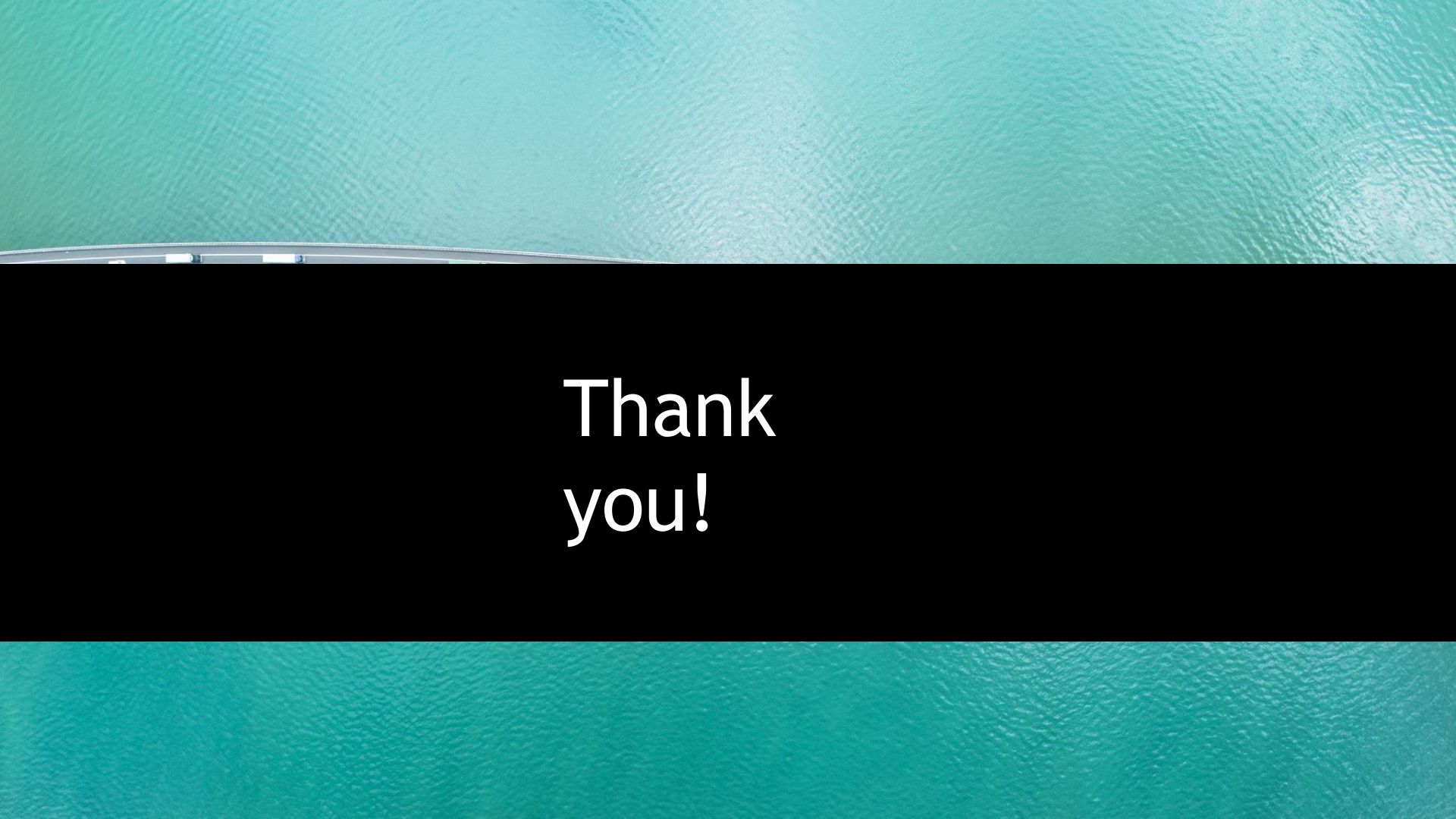


AI, Automation, those things

- Evolve automations built to replace human processes to a process rebuilt for automation
- Leveraging LLMs + Agents for reasoning and context PLUS validating policy and expected outcomes
- Adversaries don’t have to follow regulations, compliance, or anything else




Questions
?


Thank
you!

Resources / Keep in Touch

- Defender's Best Friend: https://aka.ms/defendersbestfriend
- LinkedIn: https://linkedin.com/beingageek
- Bluesky: https://bsky.app/profile/beingageek.com

Paul Coggin

Securing the Control, Data and Management Planes with Zero Trust

3rd Annual DoD Virtual Zero Trust Symposium 2025

Paul Coggin
nou Systems, Inc



Secure the Control, Data and Management Plane

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Da Re
1	P



Separation of services for each layer of OSI must be considered!

Application
Transport
Internet
k Interface

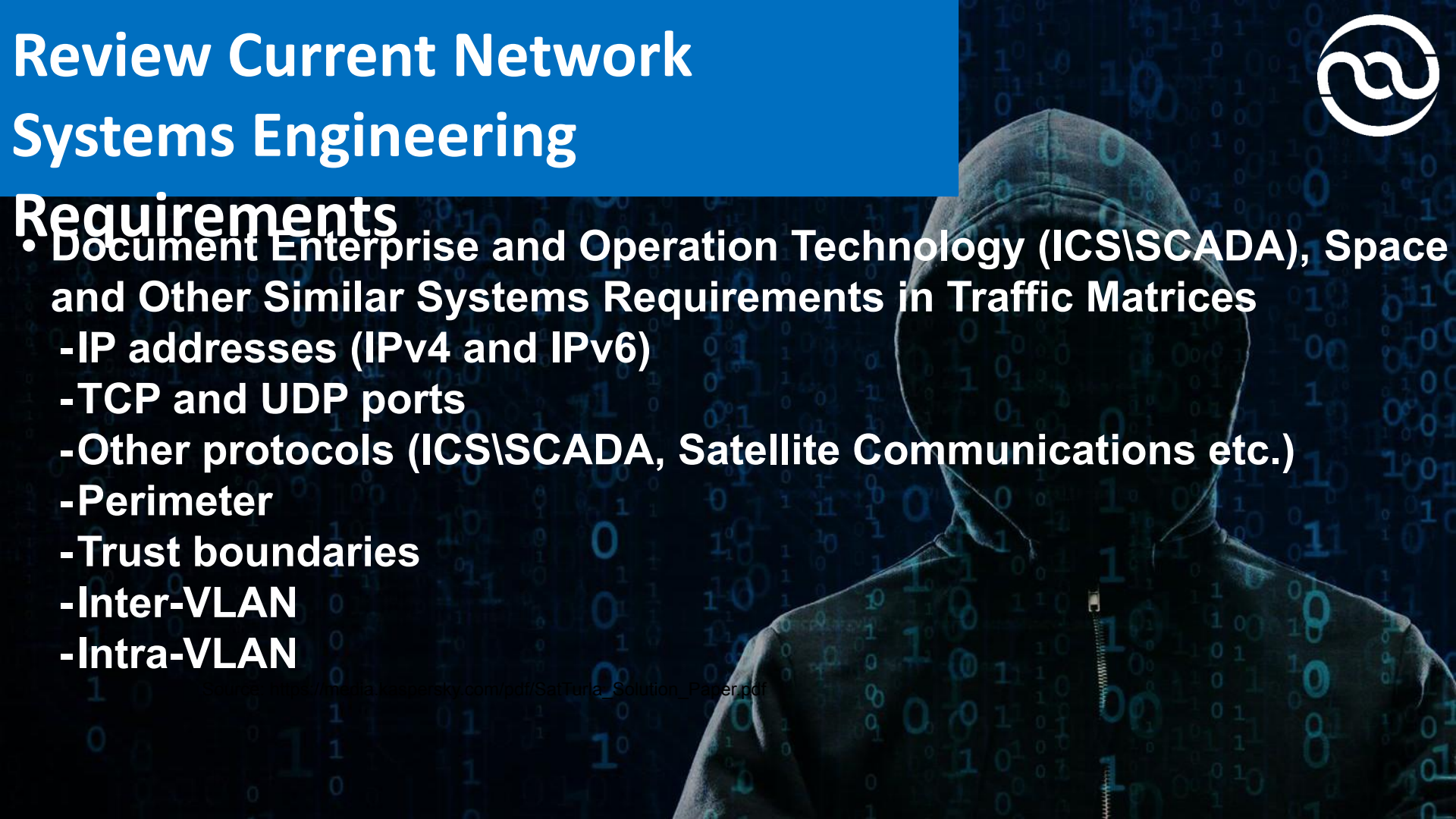
Analyze for offense and defense each layer of he OSI

- Trust t lationships
- Dependencies
- Interdependencies
- Integration

Review Current Network Systems Engineering Requirements

- Document Enterprise and Operation Technology (ICS\SCADA), Space and Other Similar Systems Requirements in Traffic Matrices
  - -IP addresses (IPv4 and IPv6)
  - -TCP and UDP ports
  - -Other protocols (ICS\SCADA, Satellite Communications etc.)
  - -Perimeter
  - -Trust boundaries
  - -Inter-VLAN
  - -Intra-VLAN

Source: https://media.kaspersky.com/pdf/SatTurla_Solution_Paper.pdf

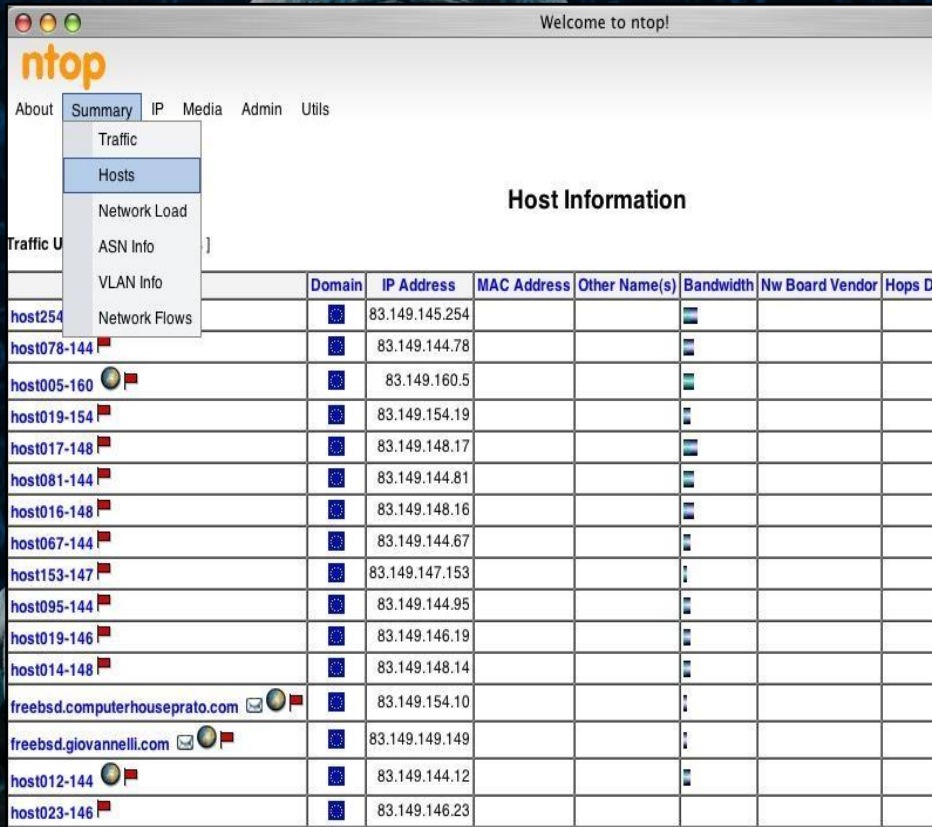


Network Trust System Engineering
Traffic Matrix (Utilities Network Example)

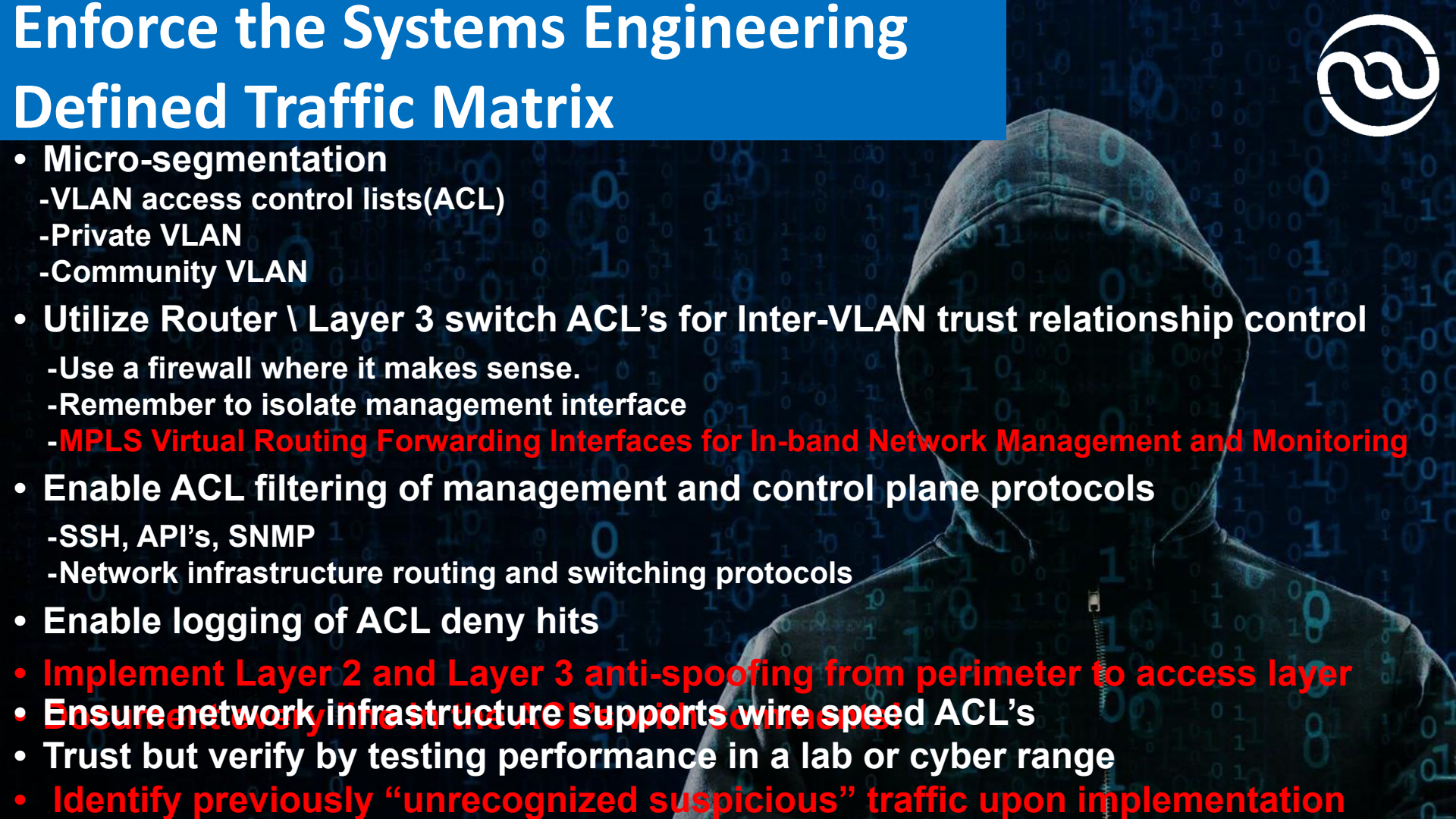
Source VLAN Name	VLAN Number	IP Subnet	Destination VLAN Name	VLAN Number	IP Subnet	Application Port/Service	Access Control List	Comments
Printers & Copiers			Printer Server					
Users-Bldg_Name			Internet, Email, print server, server resources					
Servers			IP Storage					
Server			Server					
AMI			AMI					
AMI One-way Diode			Billing, Engineering					
Jump Box - AMI			AMI					
OT - ICS/SCADA			OT - ICS/SCADA					
OT - ICS/SCADA Diode			Billing, Engineering					
Jump Box - OT ICS\SCADA			OT ICS\SCADA					
Badge Reader			Badge server					
Security-Cameras			Video surveillance server					
Facilities-Monitoring			Facilities-Monitoring server					
Jump Box - Facilities Monitoring & Managmeent			Facilities Monitoring and Management					
Public WIFI			Internet					
Internal WIFI			Internet, server resources					
Network Managment			Network Managment					
Jump Box - Network Management			Network Management					
VoIP			VoIP					
Jump Box - Voice			Voice					
HR			HR Resources					
Engineering			Engineering Servers					
GIS			GIS Server					
DMZ			Internet					
Internet			DMZ					
FINANCE								

Critical to Verify and Baseline Current Business and Mission Traffic Flows

- Does the current network infrastructure support NetFlow\SFLOW\IPFIX from the Perimeter to the communications closets access layer
- Important to have both Layer 2 and Layer 3 visualization and instrumentation
- Utilize NetFlow, IPFIX, SFLOW, JFLOW to verify and validate documentation and update as required
- Use Network TAPS alternatively to port mirroring\span where possible from perimeter to access switches for VLAN and Inter-VLAN visibility.
- Network TAPS provide separation of duties
  - -Electrical bump in the wire(no configuration)
  - -Utilize TAPS that fail open, won't block traffic in case of failure

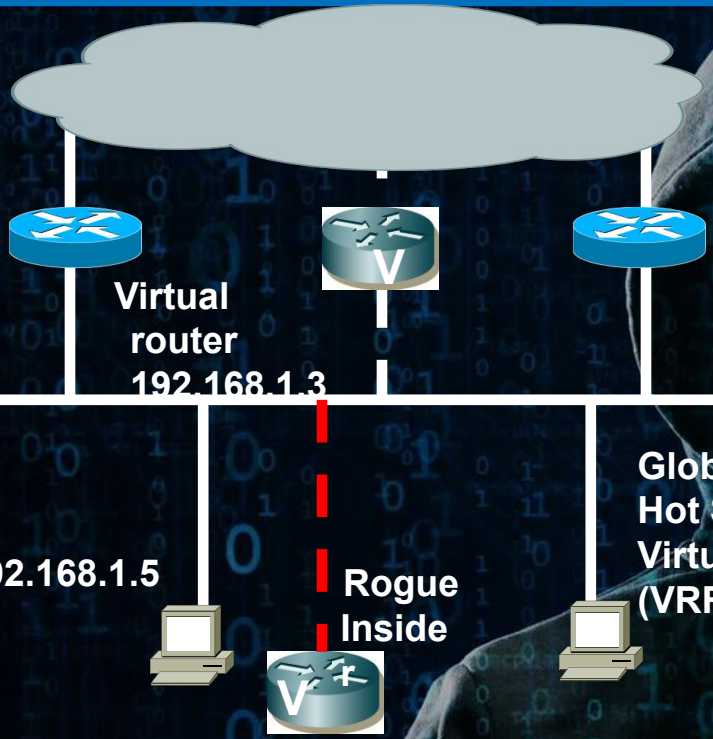


Enforce the Systems Engineering Defined Traffic Matrix



- Micro-segmentation
  - -VLAN access control lists(ACL)
  - -Private VLAN
  - -Community VLAN
- Utilize Router \ Layer 3 switch ACL's for Inter-VLAN trust relationship control
  - -Use a firewall where it makes sense.
  - -Remember to isolate management interface
  - -MPLS Virtual Routing Forwarding Interfaces for In-band Network Management and Monitoring
- Enable ACL filtering of management and control plane protocols
  - -SSH, API's, SNMP
  - -Network infrastructure routing and switching protocols
- Enable logging of ACL deny hits
- Implement Layer 2 and Layer 3 anti-spoofing from perimeter to access layer
- Ensure network infrastructure supports wire speed ACL's
- Trust but verify by testing performance in a lab or cyber range
- Identify previously "unrecognized suspicious" traffic upon implementation

First Hop Redundancy Protocols



Multicast protocol
Priority elect's role
MD5, clear, no authentication

Global Load Balancing Protocol (GLBP)
Hot Standby Router Protocol (HSRP)
Virtual Redundant Router Protocol (VRRP)

Packet Hacking Tools
GSN3
SCAP
Y
Colasoft Packet Builder
(Many others to enable IP forwarding)

Utilize Encrypted Authentication
Implement Port Security Preventing Spoofing

Secure The Routing Protocols



Relationships

Capturing from Standard input — R5 GigabitEthernet4/0 to R4 GigabitEthernet4/0

Apply a display filter ... <⌘/>

Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.1.1.5	224.0.0.5	OSPF	134	Hello Packet
2	0.211393	10.1.1.6	224.0.0.5	OSPF	134	Hello Packet
3	0.412977	ca:05:0b:91:00:70	ca:05:0b:91:00:70	LOOP	60	Reply
4	1.018420	10.1.1.5	224.0.0.10	EIGRP	74	Hello
5	1.119108	10.1.1.6	224.0.0.2	LDP	76	Hello Message
6	1.331238	10.1.1.5	224.0.0.2	LDP	76	Hello Message
7	1.492291	10.1.1.6	224.0.0.10	EIGRP	74	Hello

```
▶ Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▶ Ethernet II, Src: ca:04:0b:82:00:70 (ca:04:0b:82:00:70), Dst: IPv4mcast_0a (01:00:5e:00:00:0a)
▶ Internet Protocol Version 4, Src: 10.1.1.5, Dst: 224.0.0.10
▼ Cisco EIGRP
    Version: 2
    Opcode: Hello (5)
    Checksum: 0xeecb [correct]
  ▶ Flags: 0x00000000
    Sequence: 0
    Acknowledge: 0
    Virtual Router ID: 0 (Address-Family)
    Autonomous System: 1
  ▼ Parameters
      Type: Parameters (0x0001)
      Length: 12
      K1: 1
      K2: 0
      K3: 1
      K4: 0
      K5: 0
      K6: 0
      Hold Time: 15
  ▶ Software Version: EIGRP 12.4, TLV 1.2
```

```
0000  01 00 5e 00 00 0a ca 04  0b 82 00 70 08 00 4
0010  00 3c 00 00 00 00 02 58  cc 9a 0a 01 01 05 e
0020  00 0a 02 05 ee cb 00 00  00 00 00 00 00 00 0
0030  00 00 00 00 00 01 00 01  00 0c 01 00 01 00 0
0040  00 0f 00 04 00 08 0c 04  01 02
```

TLV Type (eigrp.tlv.type), 2 bytes

Capturing from Standard input — R5 GigabitEthernet4/0 to R4 GigabitEthernet4/0

Apply a display filter ... <⌘/>

Expression...

No.	Time	Source	Destination	Protocol	Length	Info
9	7.360951	10.1.1.6	224.0.0.5	OSPF	94	Hello Packet
10	7.763386	10.1.1.6	224.0.0.2	LDP	76	Hello Message
11	8.367859	10.1.1.5	224.0.0.2	LDP	76	Hello Message
12	9.647466	10.1.1.5	224.0.0.5	OSPF	94	Hello Packet
13	11.471831	ca:05:0b:91:00:70	ca:05:0b:91:00:70	LOOP	60	Reply
14	11.763747	ca:04:0b:82:00:70	ca:04:0b:82:00:70	LOOP	60	Reply
15	12.076072	10.1.1.6	224.0.0.2	LDP	76	Hello Message

```
▶ Frame 12: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
▶ Ethernet II, Src: ca:04:0b:82:00:70 (ca:04:0b:82:00:70), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
▶ Internet Protocol Version 4, Src: 10.1.1.5, Dst: 224.0.0.5
▼ Open Shortest Path First
  ▼ OSPF Header
      Version: 2
      Message Type: Hello Packet (1)
      Packet Length: 48
      Source OSPF Router: 10.10.10.1
      Area ID: 0.0.0.0 (Backbone)
      Checksum: 0xad78 [correct]
      Auth Type: Simple password (1)
      Auth Data (Simple): cisco
  ▶ OSPF Hello Packet
  ▶ OSPF LLS Data Block
```

Utilize Encrypted Authentication

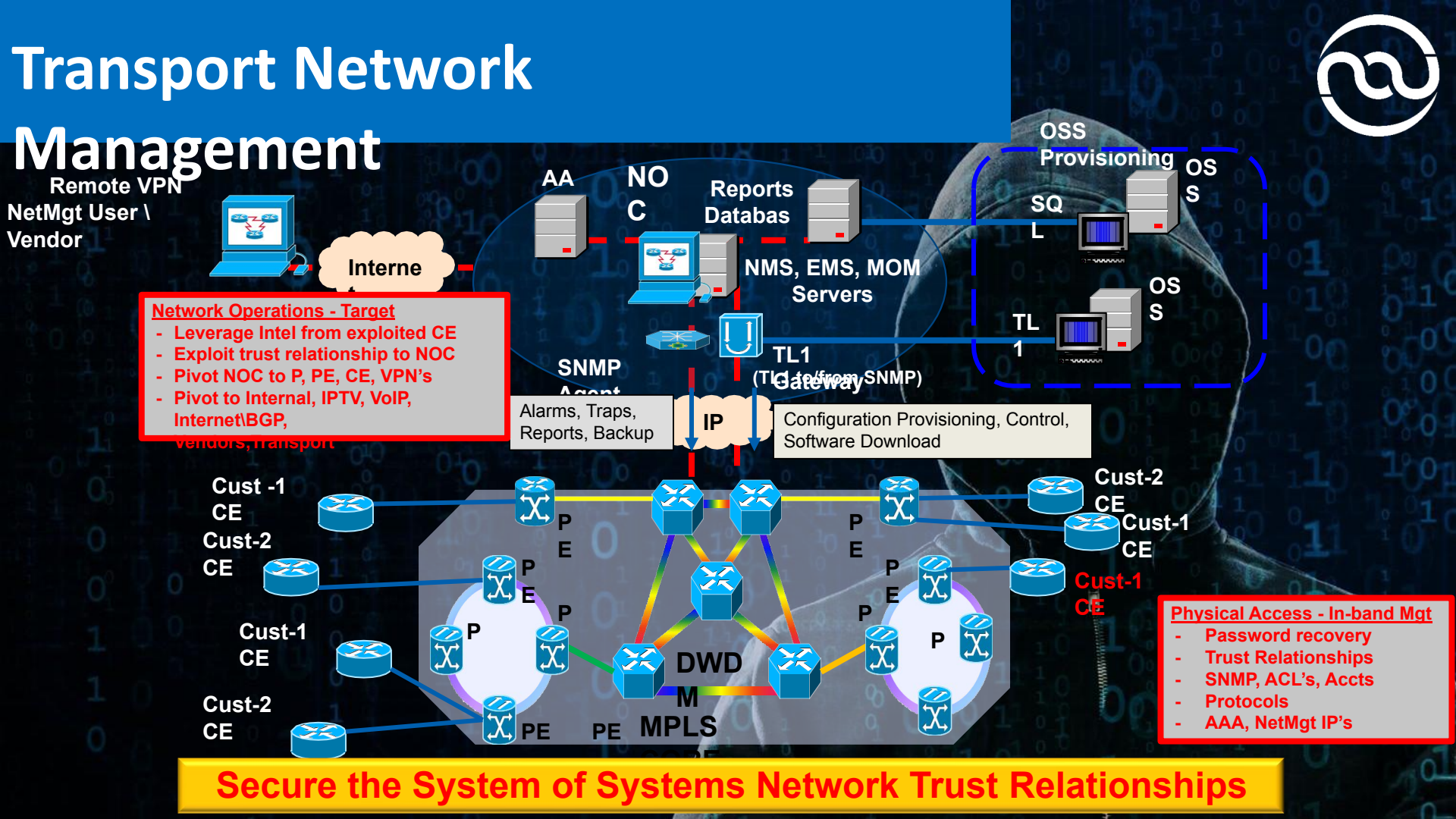
Configure Passive Interface for Access VLAN Segments

Utilize Access Control Lists to Specify Trusted Router IP Addresses

Packets: 82 · Displayed: 82 (100.0%) Profile: Default Ready to load or capture

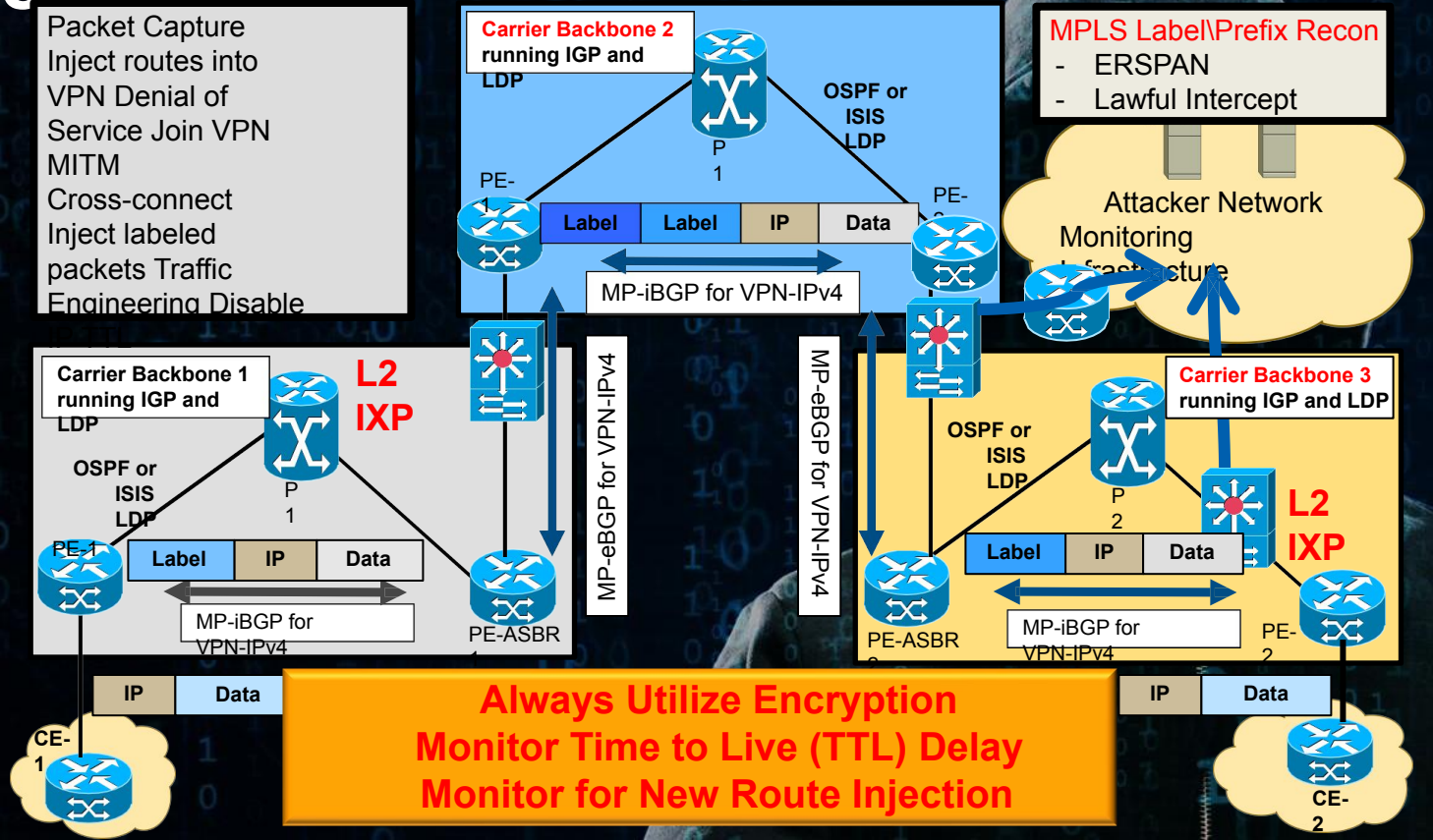
Packets: 84 · Displayed: 84 (100.0%) Profile: Defau

Transport Network Management



Secure the System of Systems Network Trust Relationships

Service Provider Transport Networks



In-band Management

Business and Network Management Traffic Uses Common Infrastructure

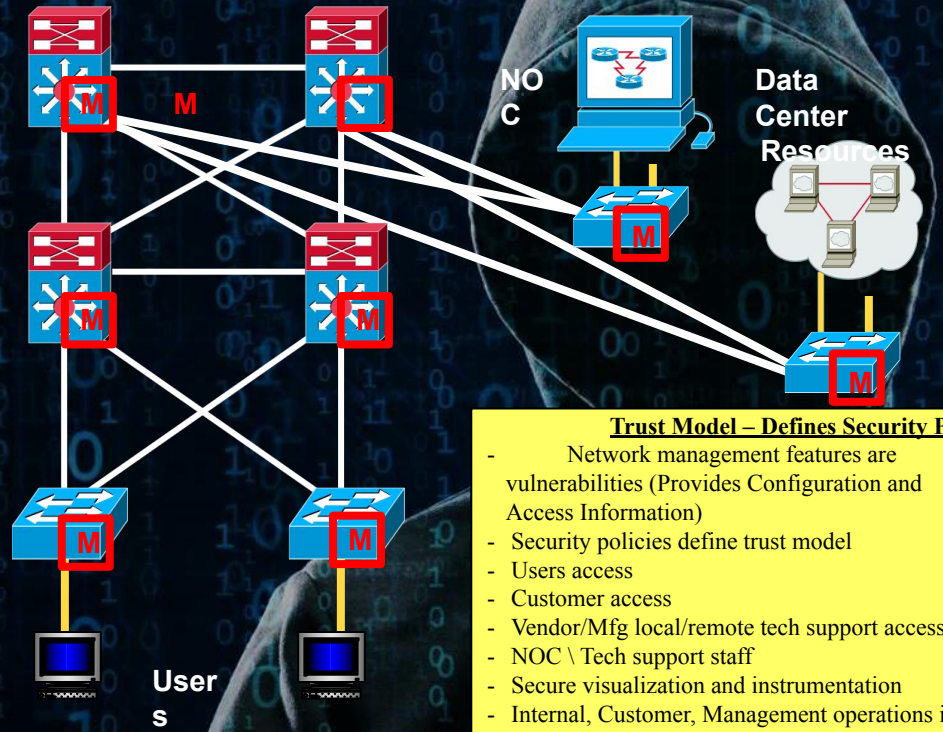
Network Management Protocols
- SNMP
- HTTP/s – XML
- NETCONF
- TL1
- SSH

Network Management Security
- Access List
- Firewalls
- VPN
- IDS/IPS
- AAA
- Trust levels

Management VLAN M

User VLAN's

VLAN Trunks



Utilize MPLS VPN's and VRF's for Management Network

Trust Model – Defines Security Posture

- Network management features are vulnerabilities (Provides Configuration and Access Information)
- Security policies define trust model
- Users access
- Customer access
- Vendor/Mfg local/remote tech support access
- NOC \ Tech support staff
- Secure visualization and instrumentation
- Internal, Customer, Management operations in separate IP subnets/VLAN's/PVC's etc over shared network infrastructure.
- Log everything
- 2 Factor authentication

Out-of-band Management

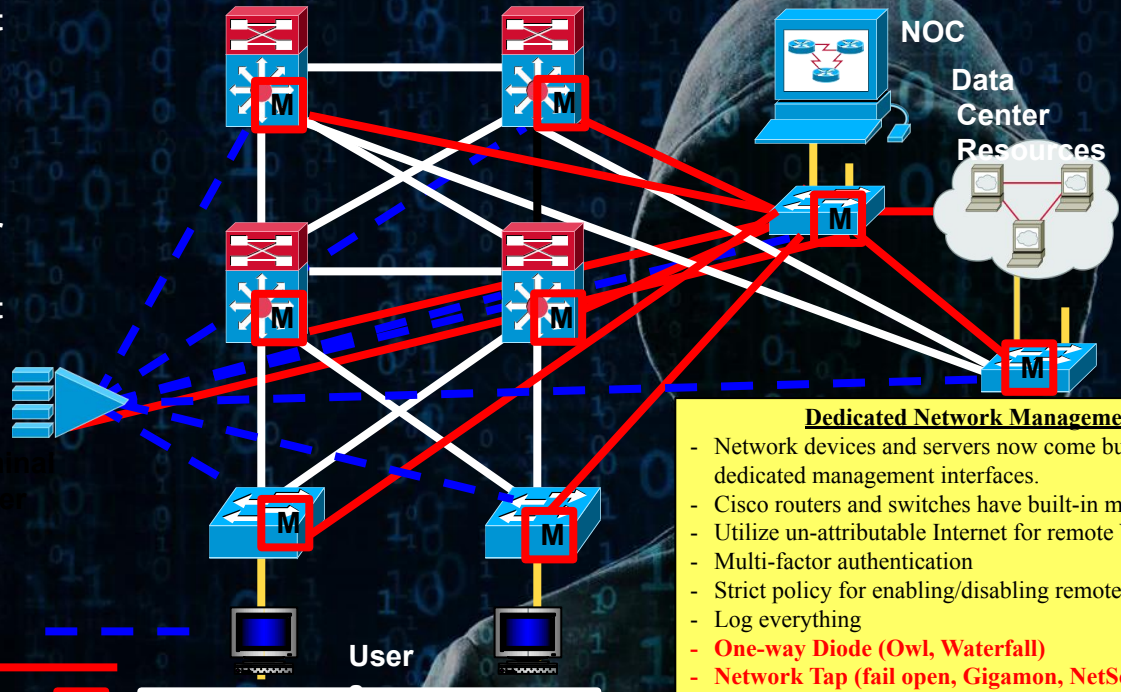
Network Management Protocols
- SNMP
- HTTPS – XML
- NETCONF
- TL1
- SSH
- Custom\Proprietary

Network Management Security Access Lists
- VACL's
- Firewalls
- VPN
- IDS/IPS
- AAA
- Trust levels

Terminal Server/Console Network

Dedicated Mgmt Interface

VLAN's

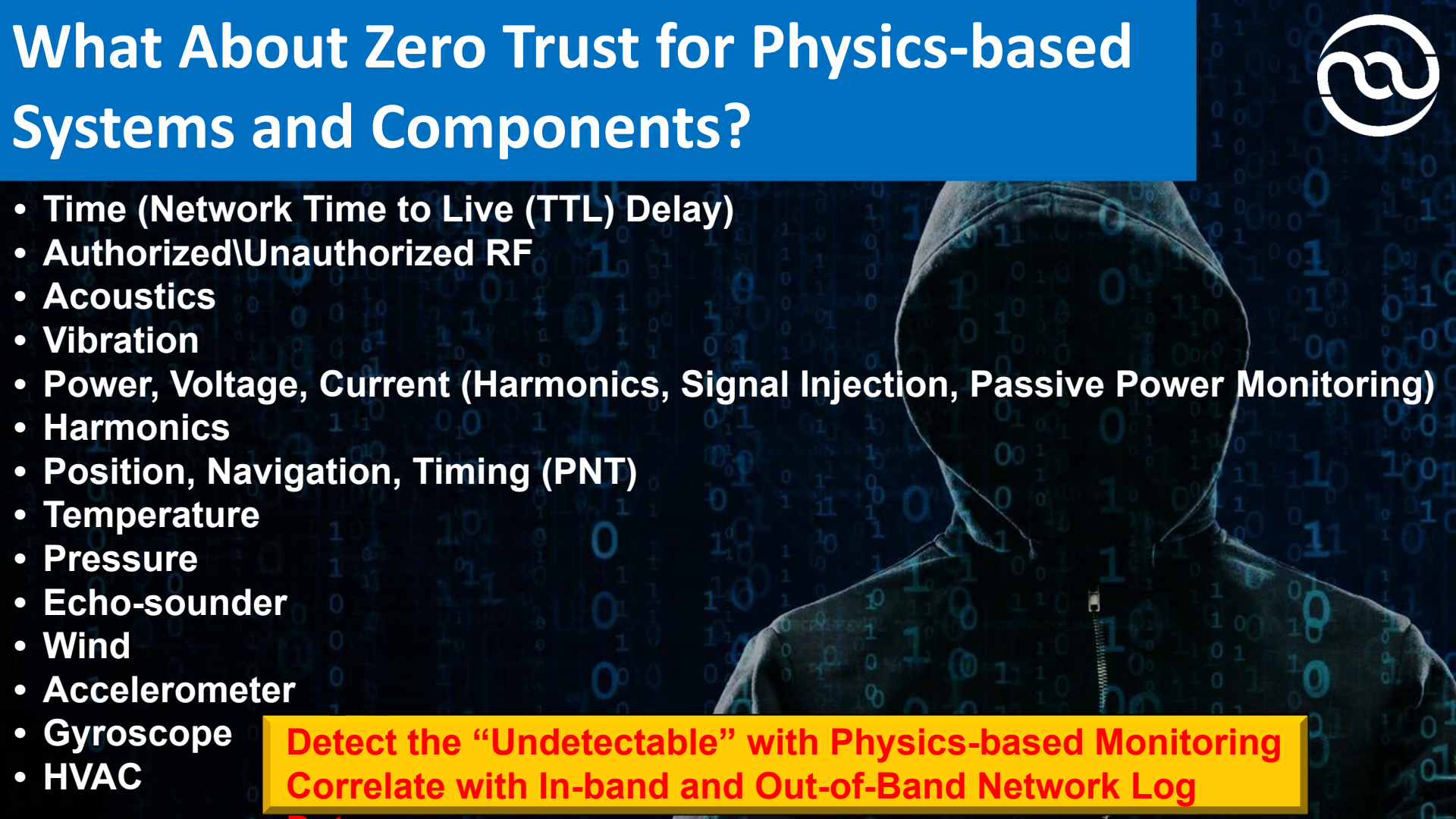


Dedicated Network Management Network

- Network devices and servers now come built with dedicated management interfaces.
- Cisco routers and switches have built-in mgt. int.
- Utilize un-attributable Internet for remote VPN access
- Multi-factor authentication
- Strict policy for enabling/disabling remote vendor access
- Log everything
- **One-way Diode (Owl, Waterfall)**
- **Network Tap (fail open, Gigamon, NetScout)**
  Separation of roles and responsibilities NOC\SOC
- **Utilize hardened jump box with MFA for management network access, extensive monitoring, network trust hardened**
- **Correlate in-band and out-of-band monitoring data**

Utilize One-way Diodes and Network Taps to Further Lock Down Trust Between Network and SOC

What About Zero Trust for Physics-based Systems and Components?

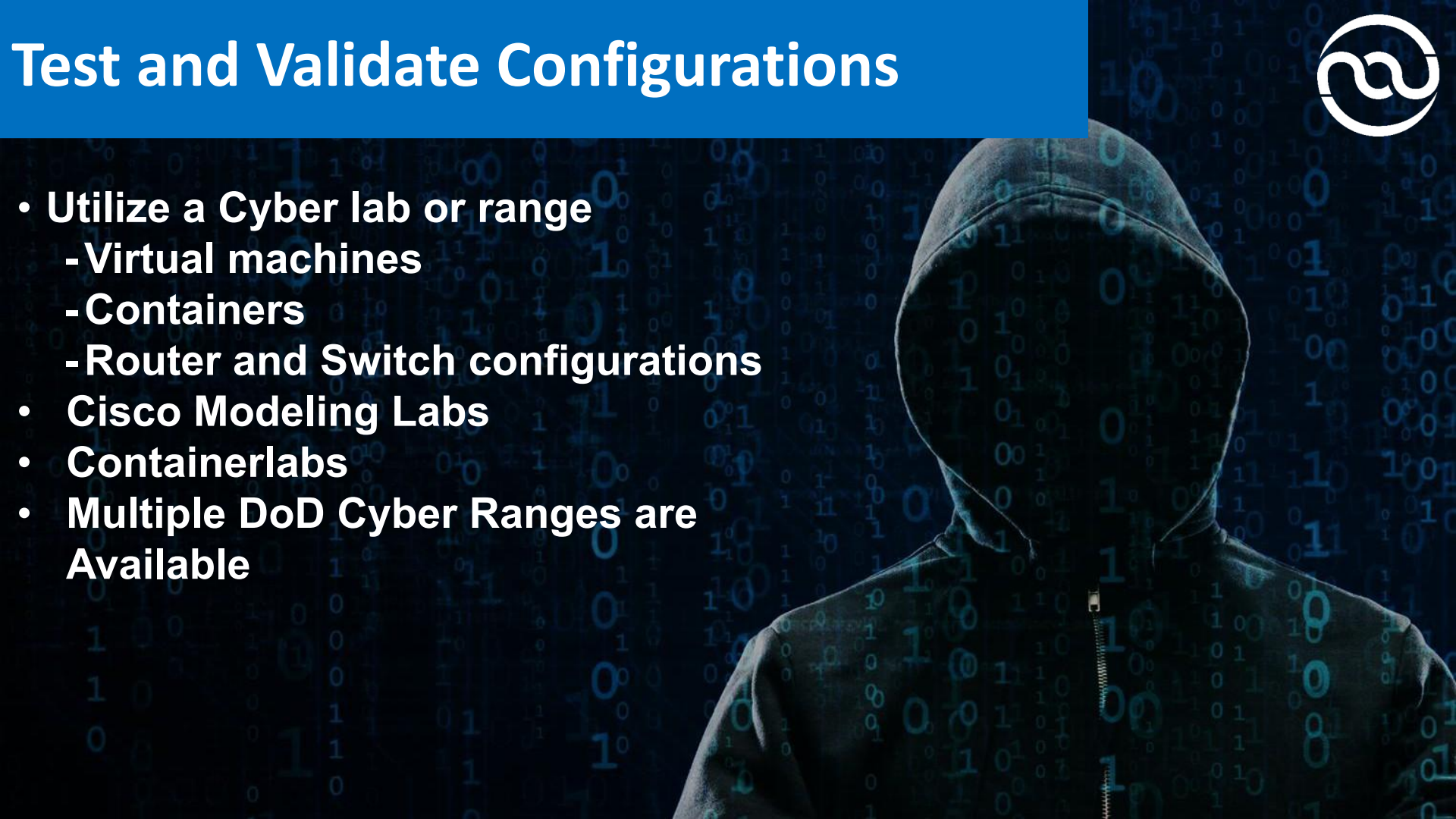


- Time (Network Time to Live (TTL) Delay)
- Authorized\Unauthorized RF
- Acoustics
- Vibration
- Power, Voltage, Current (Harmonics, Signal Injection, Passive Power Monitoring)
- Harmonics
- Position, Navigation, Timing (PNT)
- Temperature
- Pressure
- Echo-sounder
- Wind
- Accelerometer
- Gyroscope
- HVAC

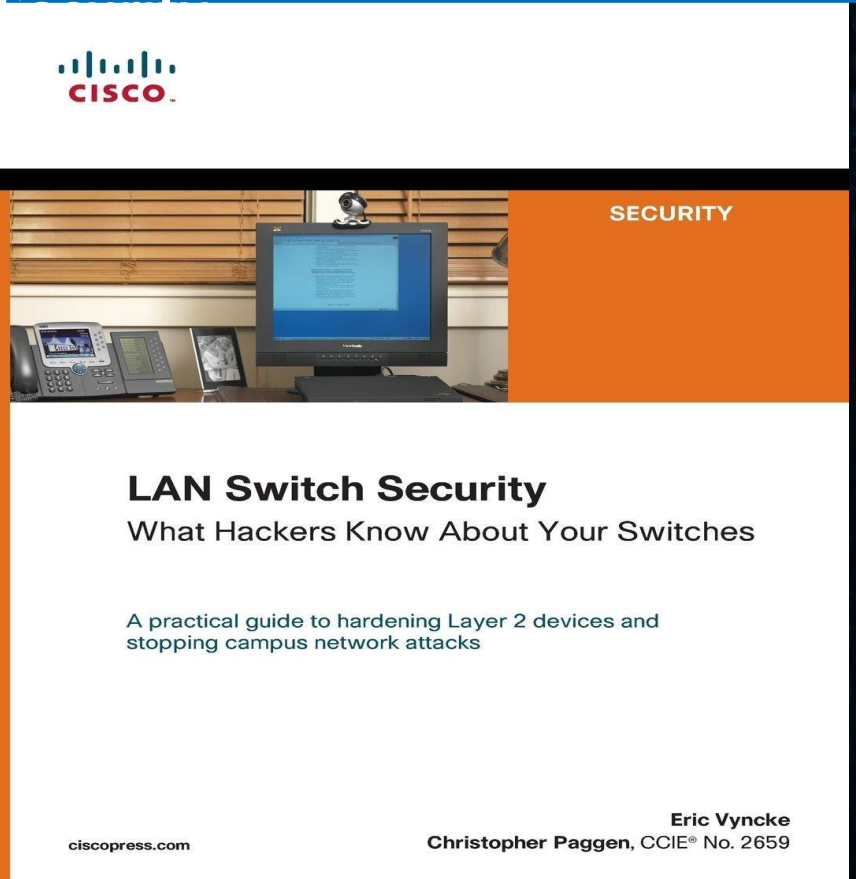
Detect the "Undetectable" with Physics-based Monitoring
Correlate with In-band and Out-of-Band Network Log

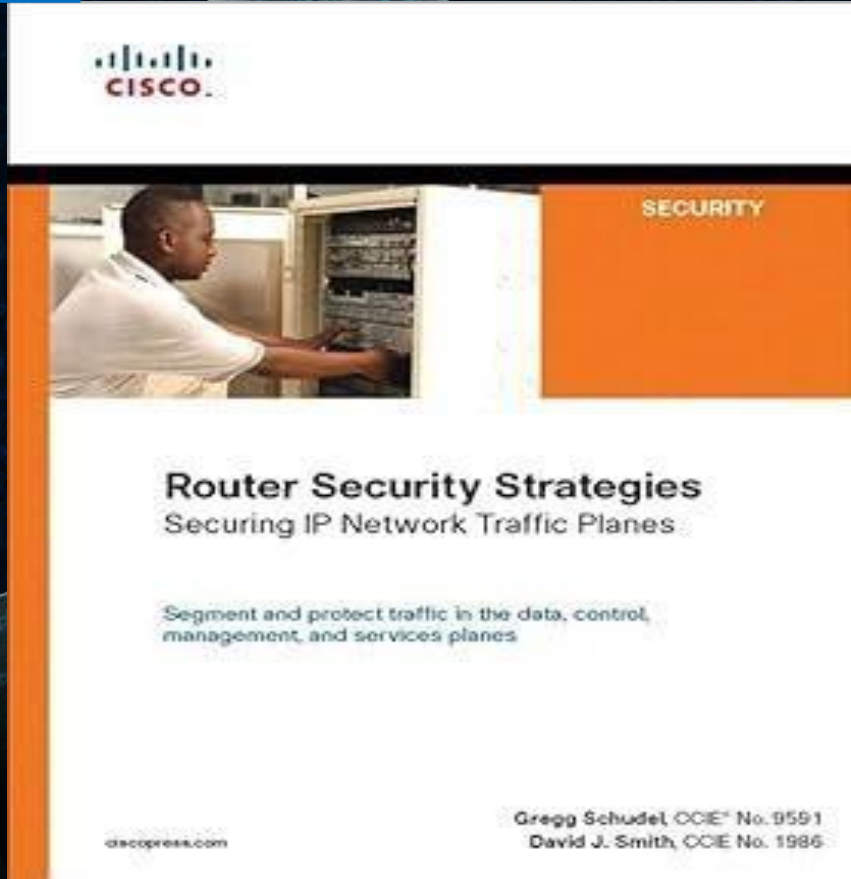
Test and Validate Configurations

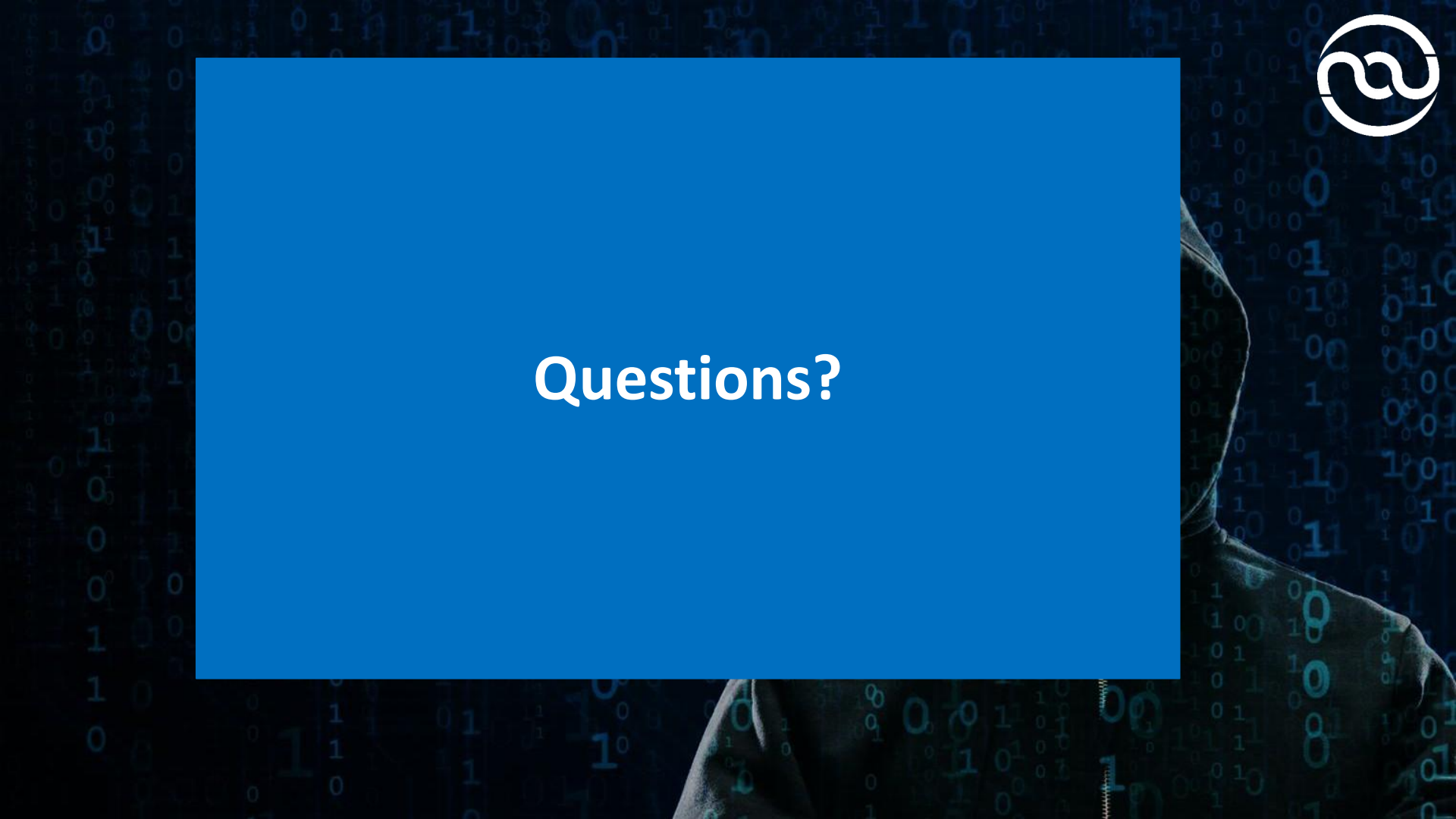
- Utilize a Cyber lab or range
  - Virtual machines
  - Containers
  - Router and Switch configurations
- Cisco Modeling Labs
- Containerlabs
- Multiple DoD Cyber Ranges are Available



Excellent References for Layer 2 and Layer 3 Protocols and Infrastructure Security





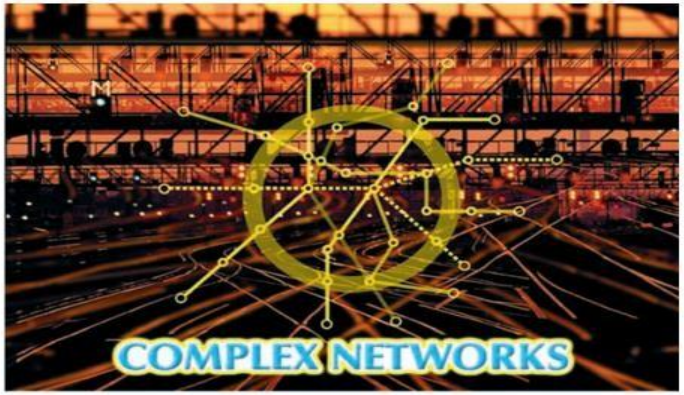

Questions?

References

Gregg Schudel, David J. Smith (2007), Router Security Strategies – Securing IP Network Traffic Planes, Cisco Press
Eric Vyncke, Christopher Paggen (2005), LAN Switch Security – What Hackers Know About Your Switches, Cisco Press Halabi (2000), Internet Routing Architectures, Cisco Press
Beau Williamson (1999), Developing IP Multicast Networks, Cisco Press
Michael H. Behringer, Monique J. Morrow (2005), MPLS VPN Security, Cisco Press
Barry Raveendran Greene, Philip Smith (2002), ISP Essentials, Cisco Press
Jim Guichard, Ivan Papelnjak (2000), MPLS and VPN Architectures, Cisco Press
Lancy Lobo, Umesh Lakshman (2005), MPLS Configuration on Cisco IOS Software, Cisco Press Eric Osborne, Ajay Simha (2002), Traffic Engineering with MPLS, Cisco Press
Richard Bejtlich (2004), The Tao Network Security Monitoring: Beyond Intrusion Detection
Paul Coggin (2012), Own the Network, Own the Data, From https://www.youtube.com/watch?v=NazPPQZjMTk Paul Coggin (2014), Bending and Twisting Networks, From https://www.youtube.com/watch?v=cdc6dL9pd6k Paul Coggin (2014), Digital Energy – BPT, From https://www.youtube.com/watch?v=ng6pzewVG24
Paul Coggin (2015), Hijacking Label Switch Networks in the Cloud, From https://www.youtube.com/watch?v=XqvG_mts6hY
Paul Coggin (2016), Defending the Enterprise Against Network Attacks, From www.youtube.com/watch?v=K0X3BB5XK8
Paul Coggin (2016), Exploiting First Hop Protocols to Own the Network, From www.youtube.com/watch?v=bcvnJzle6G0&t=14s Paul Coggin (2017), Hallowed Be Thy Packets
Paul Coggin (2019), SS7 for INFOSEC, From https://www.youtube.com/watch?v=op70k_1uCRU
Paul Coggin (2023), Threating Hunting Space and Digital Energy with Physics, From https://www.youtube.com/watch?v=-HFh8ipmyq4
Ravie Lakshmanan (2025), Cisco Confirms Salt Typhoon Exploited CVE-2018-0171 to Target U.S. Telecom Networks, https://thehackernews.com/2025/02/cisco-confirms-salt-typhoon-exploited.html
Matt Kapko (2025), Salt Typhoon remains active, hits more telecom networks via Cisco routers, https://cyberscoop.com/salt-typhoon-china-ongoing-telecom-attack-spree/
CISA, (2024), Enhanced Visibility and Hardening Guidance for Communications Infrastructure, https://www.cisa.gov/resources-tools/resources/enhanced-visibility-and-hardening-guidance-communications-infrastructure
Insikt Group (2025), RedMike (Salt Typhoon) Exploits Vulnerable Cisco Devices of Global Telecommunications Providers, https://www.recordedfuture.com/research/redmike-salt-typhoon-exploits-vulnerable-devices


Backups

Excellent Paper

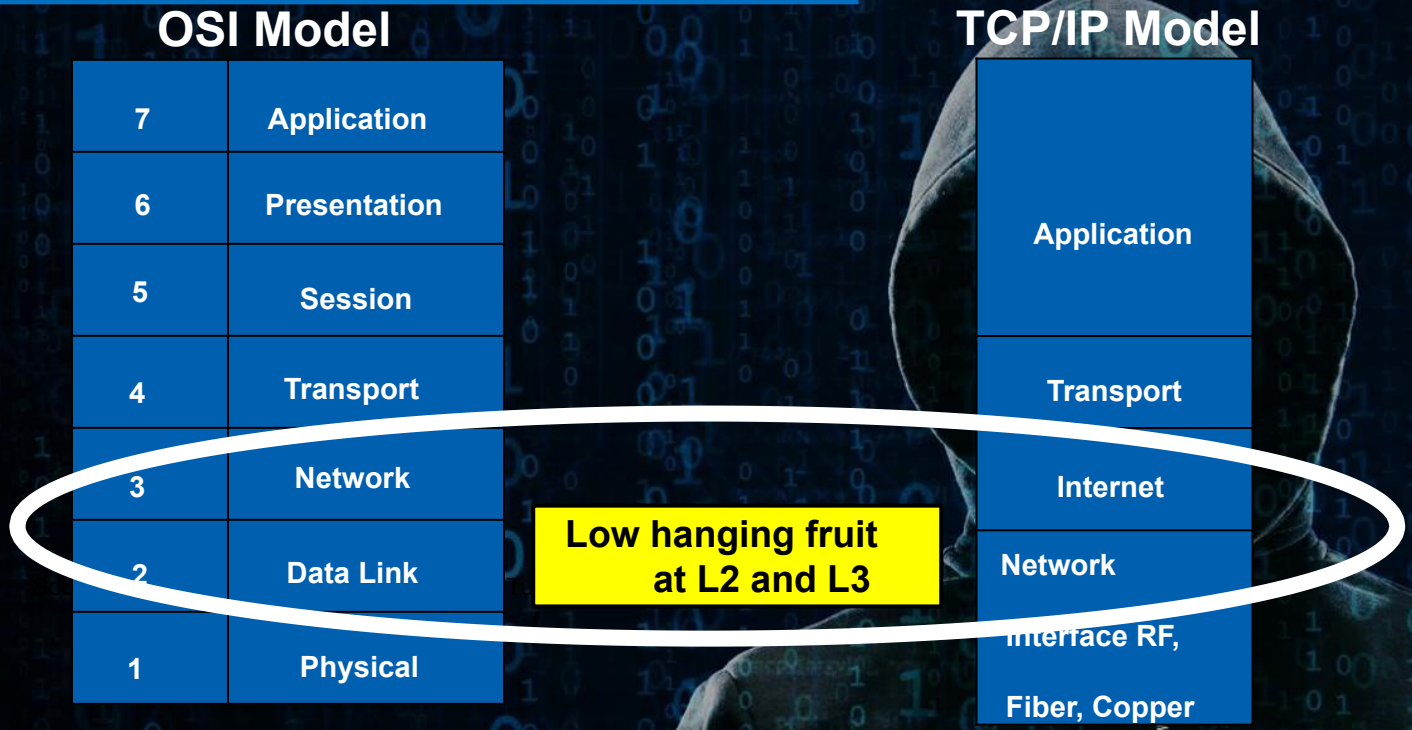


Identifying, Understanding, and Analyzing

Critical Infrastructure Interdependencies

By Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly

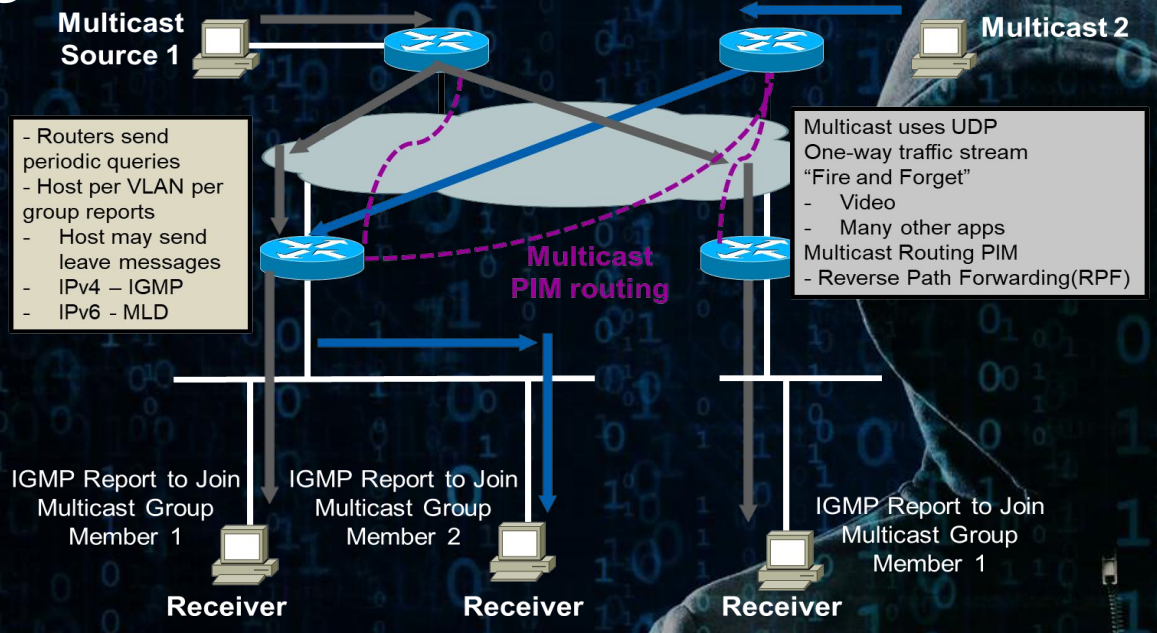
OSI Model


OSI Model
7
Application
6
Presentation
5
Session
4
Transport
3
Network
2
Data Link
1
Physical
TCP/IP Model
Application
Transport
Internet
Network
Interface RF,
Fiber, Copper
Low hanging fruit
at L2 and L3

Multicast Protocols

-Routers send periodic queries
-Host per VLAN per group reports
- Host may send leave messages
- IPv4 – IGMP

Multicast uses UDP One-way traffic stream "Fire and Forget"
- Video
- Many other apps Multicast Routing PIM
- Reverse Path



Secure Multicast Control Protocol Trust Relationships

Craft Router PIM Packets
- SCAPY
- Colasoft Packet Builder
- Possible to use GNS3 or Quagga etc to add PIM router

Local VLAN Segement
- Hello packets
- Join/Prune packets
- Assert

Unicast PIM Packets
- Register
- Register-Stop
- C-RP-Advertisement

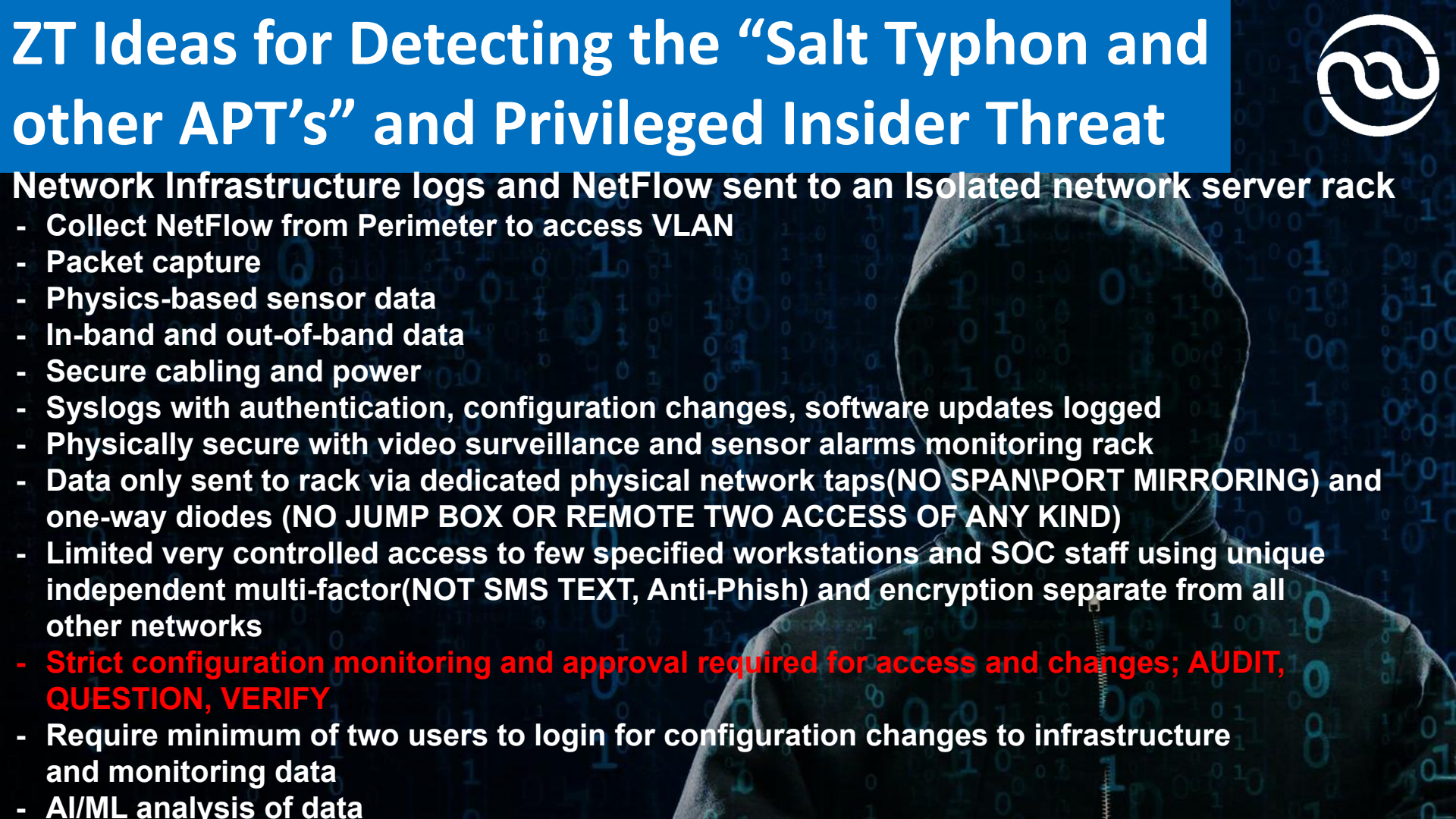
Craft IGMP/MLD
- SCAPY
- Collasoft Packet Builder
- IGMP Leaves
- IGMP Queries
- Spoof IGMP Source

Summary of Recommendations

- Define traffic matrix with required intra-VLAN and inter-VLAN trust relationships
- Verify and baseline with detailed NetFlow analysis
- Implement anti-spoofing from perimeter to access layer at both layer 2 and 3
- Management Plane
  - SNMPv3
  - SSH
  - Secure API's
  - Secure trust relationships with layer 2 and layer 3 access lists with logging
  - Isolate management network using VLANs, VRFs, MPLS\segment routing(SR-MPLS\SRv6), out-of-band network
  - Utilize network taps (Gigamon, NetScout, etc) and one-way diodes(Owl, Waterfall)
  - Where remote external network access is required utilize VPN, multi-factor authentication, and a hardened jump box combined with strict access control and monitoring
  - Collect NetFlow from perimeter to access layer communications closets for intra-VLAN and Inter-VLAN visibility
  - Utilize physics-based sensors to collect data out-of-band and compare to in-band data from network infrastructure
  - Correlate and compare in-band and out-of-band data: Actual vs Expected: traffic patterns, paths, latency, bandwidth utilization
  - Configuration monitoring, role-based control, notification
- Control Plane
  - Monitor internal routing protocols (OSPF, ISIS, EIGRP) for new routes being injected into routing table
  - Monitor global Internet BGP for IP prefix hijacking attempts
  - Implement BGP RPKI and BGP-Sec
  - Monitor external service provider transport networks for traffic engineering attacks leveraging TTL baseline
  - Route authentication, encryption, filtering
  - Encrypt service provider MPLS and segment routing network services and monitor TTL behavior
- For security
  - 802.1X
  - Dynamic ARP
  - DHCP snooping
  - MACsec
  - DHCP Option 82
- Secure and monitor both IPv4 and IPv6
- Disable protocols and features where not required such as http/s, telnet, CDP, HSP, LLDP, smart install,

inspection

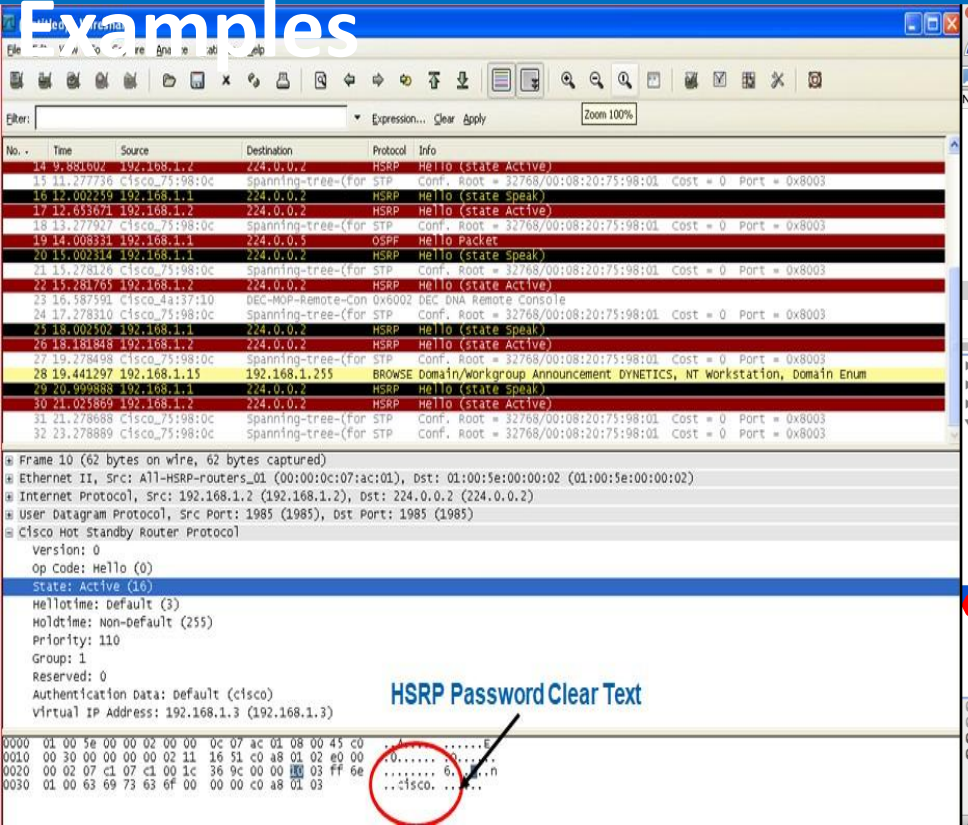
ZT Ideas for Detecting the “Salt Typhon and other APT’s” and Privileged Insider Threat

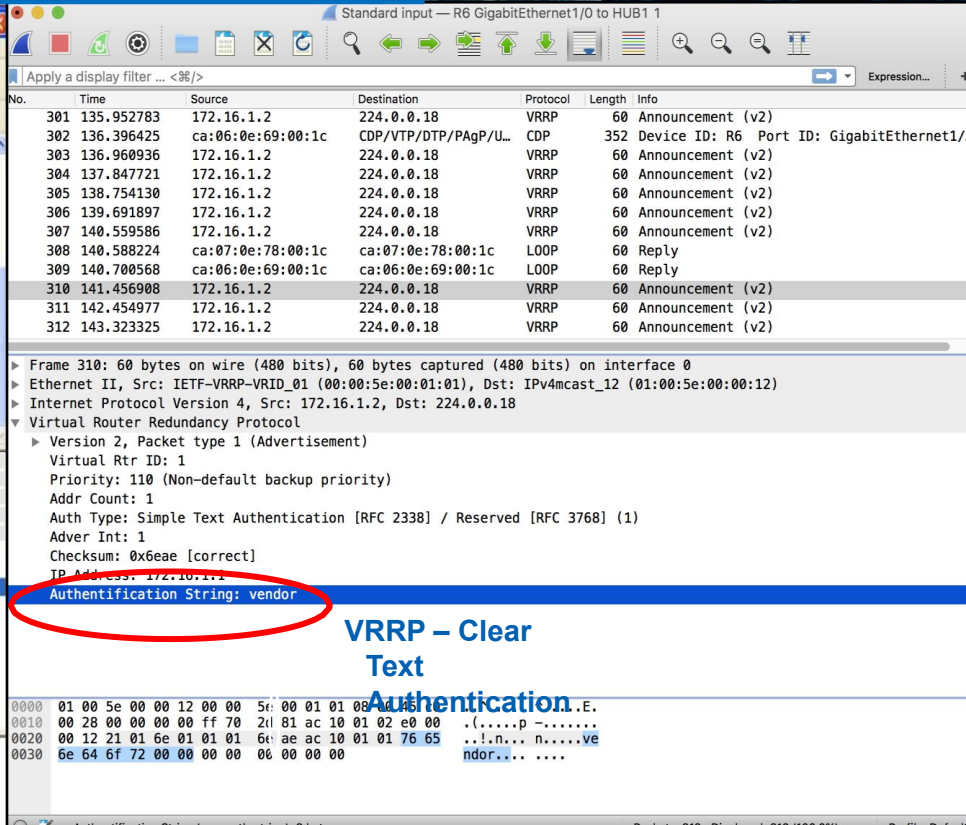


Network Infrastructure logs and NetFlow sent to an Isolated network server rack

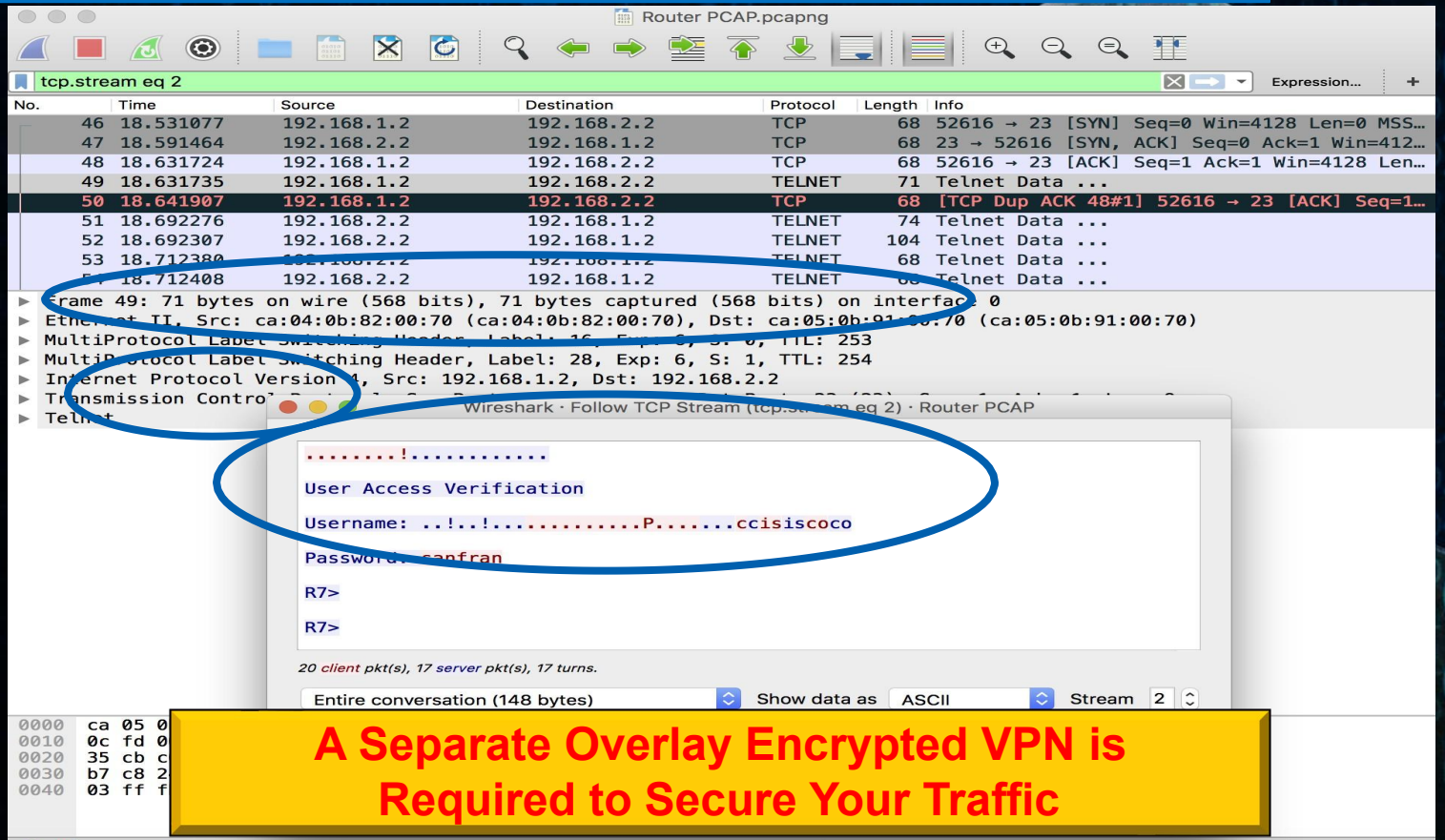
- Collect NetFlow from Perimeter to access VLAN
- Packet capture
- Physics-based sensor data
- In-band and out-of-band data
- Secure cabling and power
- Syslogs with authentication, configuration changes, software updates logged
- Physically secure with video surveillance and sensor alarms monitoring rack
- Data only sent to rack via dedicated physical network taps(NO SPAN\PORT MIRRORING) and one-way diodes (NO JUMP BOX OR REMOTE TWO ACCESS OF ANY KIND)
- Limited very controlled access to few specified workstations and SOC staff using unique independent multi-factor(NOT SMS TEXT, Anti-Phish) and encryption separate from all other networks
- Strict configuration monitoring and approval required for access and changes; AUDIT, QUESTION, VERIFY
- Require minimum of two users to login for configuration changes to infrastructure and monitoring data
- AI/ML analysis of data

First Hop Redundancy Protocol Packet Capture Examples





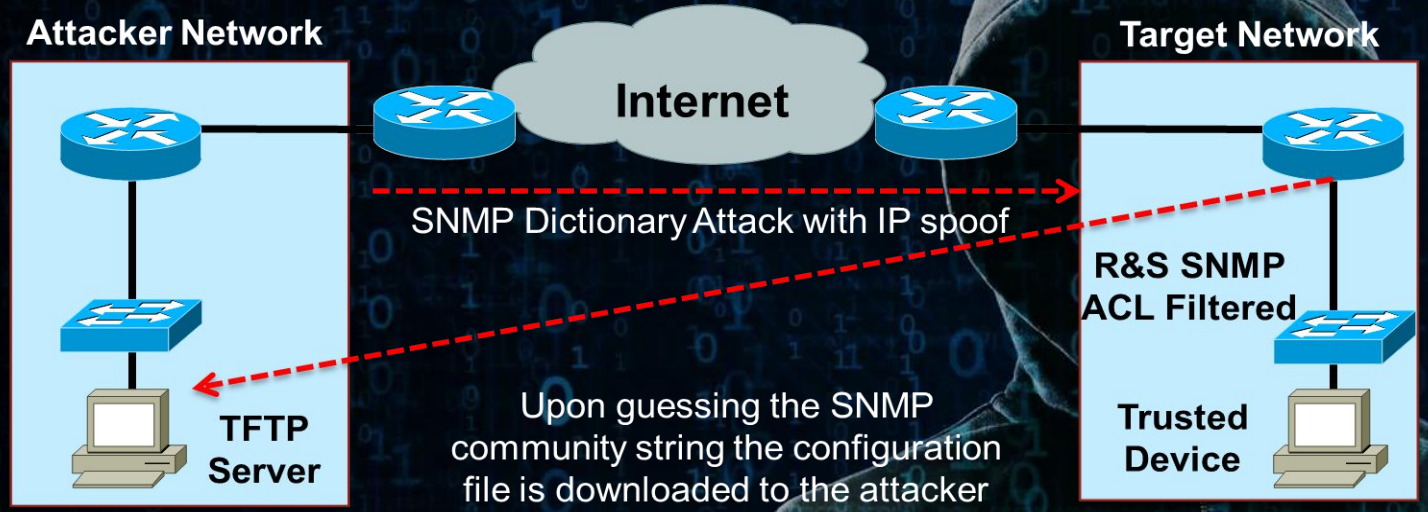
MPLS VPN Packet Capture



A Separate Overlay Encrypted VPN is Required to Secure Your Traffic

UDP Spoofing to target SNMP
Defeat router ACL trust securing SNMP

```
$ snmpblow.pl -s <NetMgt IP> -d <Target IP> -t <TFTP IP> -f cfg.txt < communities.txt
```

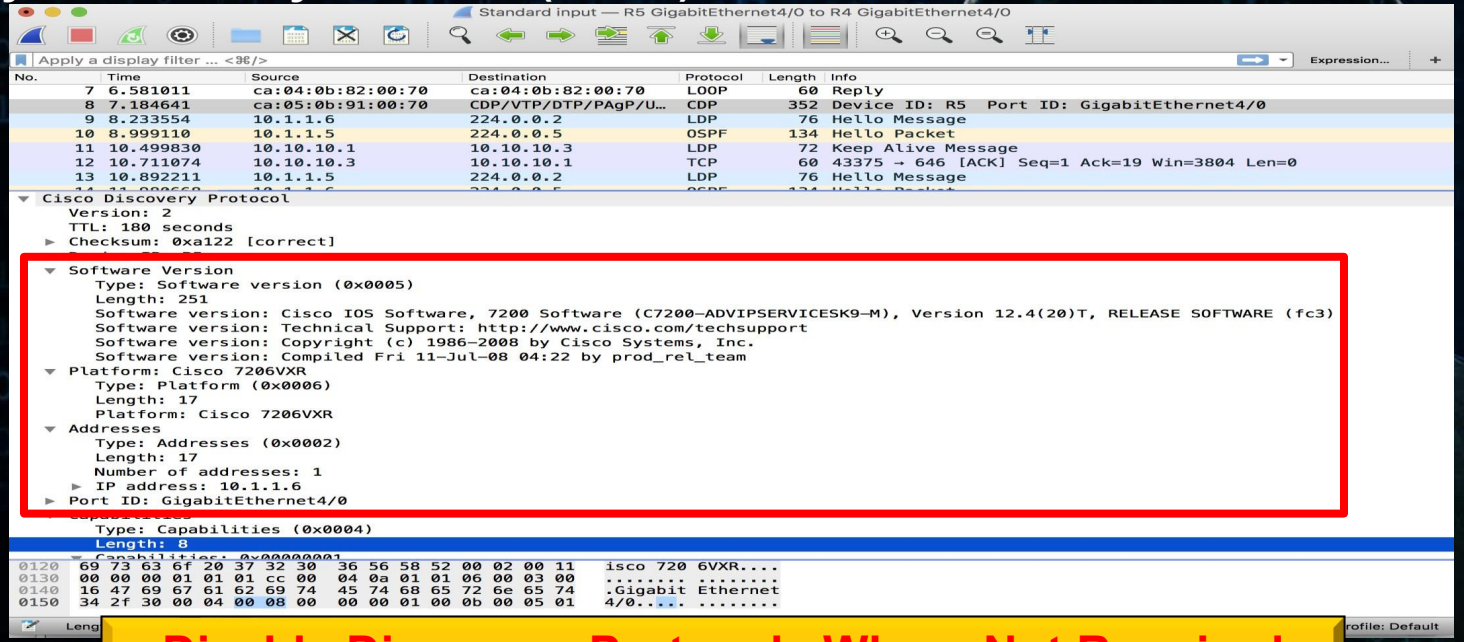


Layer 2 and L3 anti-spoof protection with a complex SNMP community string is recommended. SNMPv3 is strongly encouraged.

Reference: http://www.scanit.be/en_US/snmpblow.html

Network Discover Protocol Information Leakage

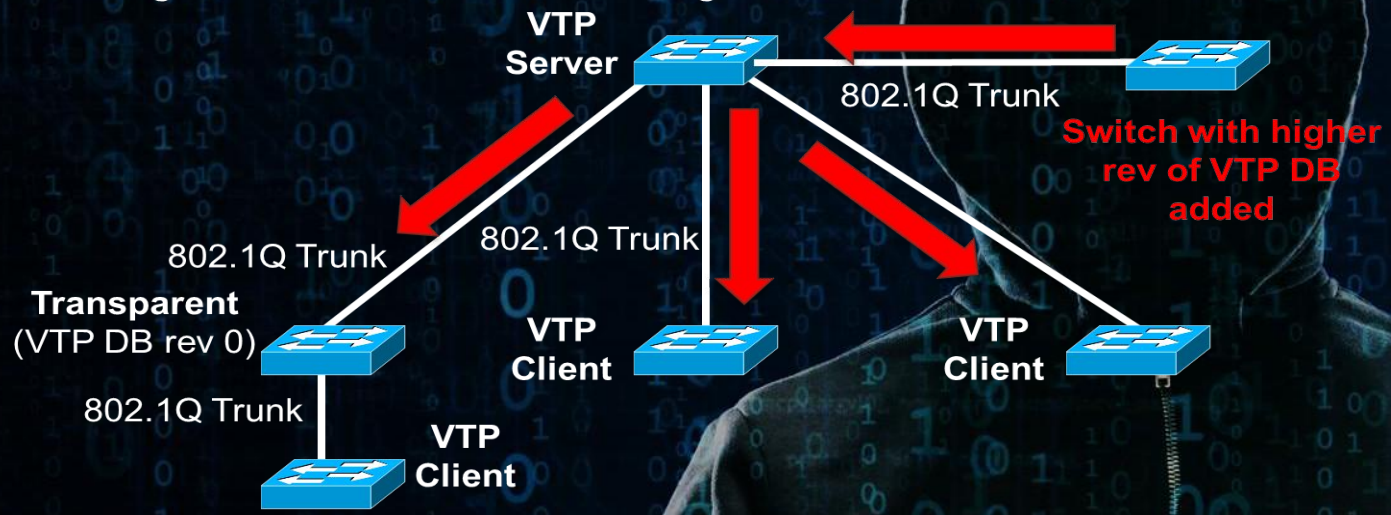
- Cisco Discovery Protocol (CDP)
- HP Switch Protocol (HSP)
- Link Layer Discovery Protocol (LLDP)



Disable Discovery Protocols Where Not Required

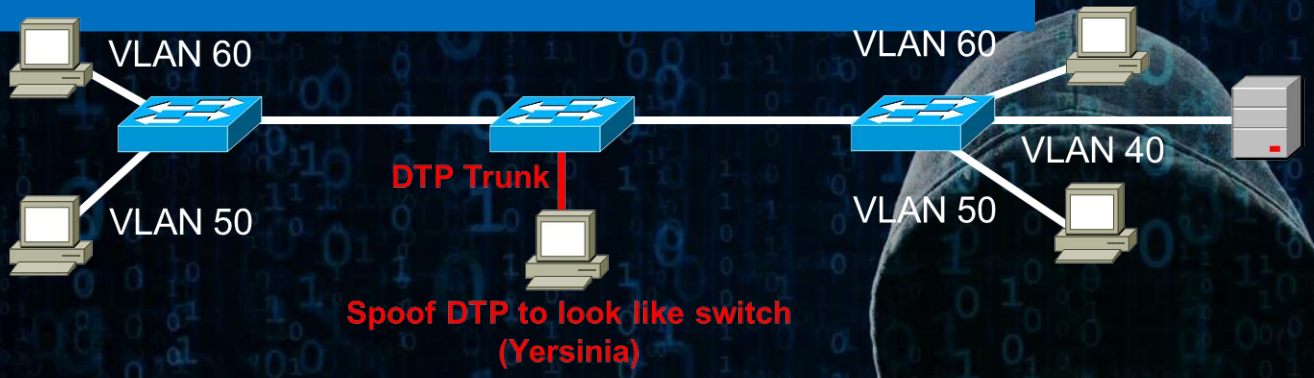
VLAN Trunking Protocol (VTP)

- Existing network running default VTP settings
- Switches sync to higher rev VTP DB resulting in VLAN config being lost!!
- Everyone has a current VLAN.DAT backup right??
- Configure a password for VTP Domain (NOT Cisco….SanFran….)
- Delete VLAN.DAT before connecting a new switch
- Change the native VLAN to something other than 1



Secure the Switch VTP Before Installing on Network!
Always Verify Network Device Configurations Offline

Dynamic Trunking



- Dynamic Trunk Protocol (DTP) Modes : Auto, On, Off, Desirable, Non-negotiate
- IP Phones, Wireless Access Points
- All VLANs are trunked by default
- Native VLAN (untagged); Default Native VLAN 1 and required by DTP
- Yersinia or other packet crafting tools
- Disable trunking on interfaces where not in use
- Specify VLANs to be allowed on trunk interfaces
- Do not use Native VLAN 1

Disable Auto-negotiation
Don't Trust Connected Devices

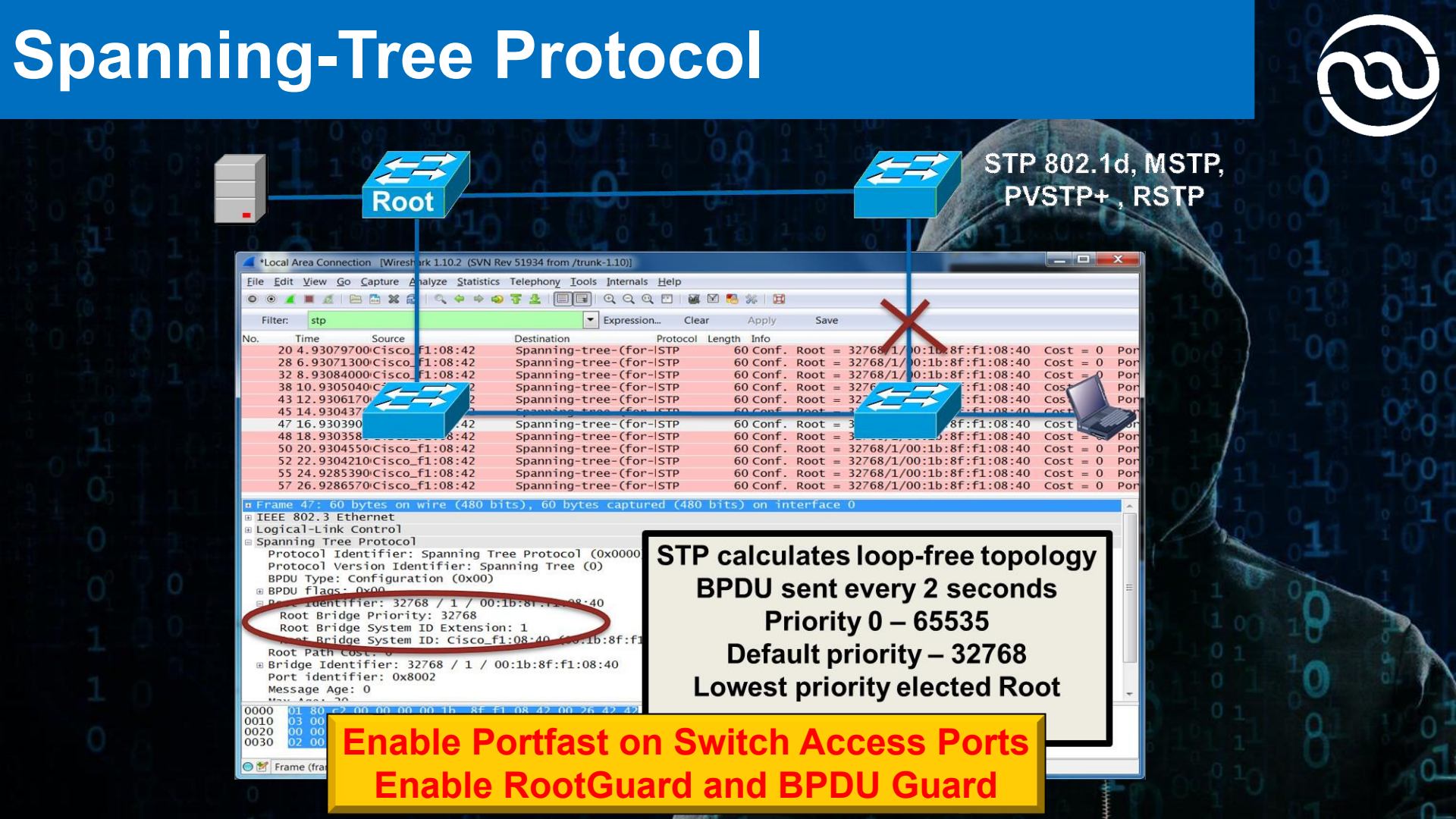
VLAN Hopping Double VLAN Tag



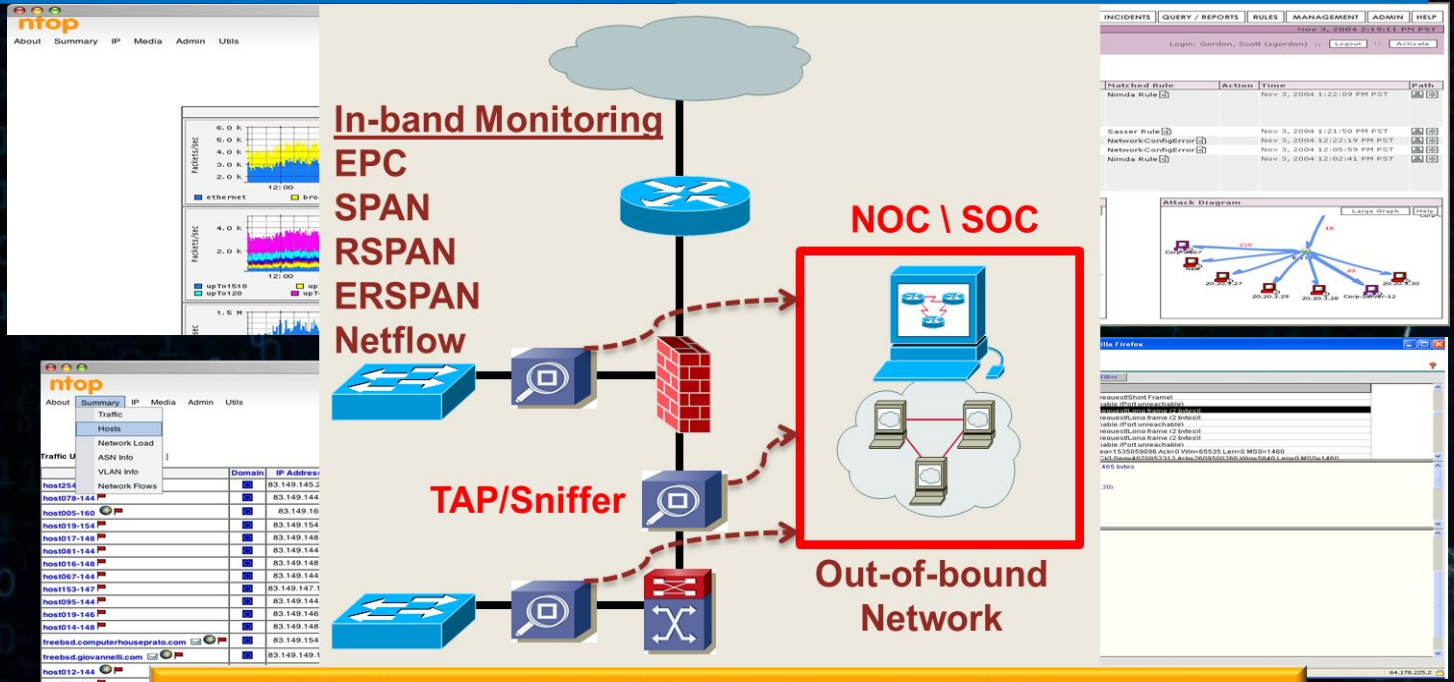
- No two-way communication. Frames sent to target with no response to sender.
- Craft Frames with double encapsulated frames
- VLAN trunking is not required in this scenario
- Disable AUTO\DYNAMIC NEGOTIATION!
- Don’t use native VLAN 1. Use tagged mode for native VLAN x on trunks
- Disable interfaces not in use

Disable Auto-negotiation
Don’t Trust Connected Devices

Spanning-Tree Protocol



Layer 2 – Secure Visualization and Instrumentation (SVI)

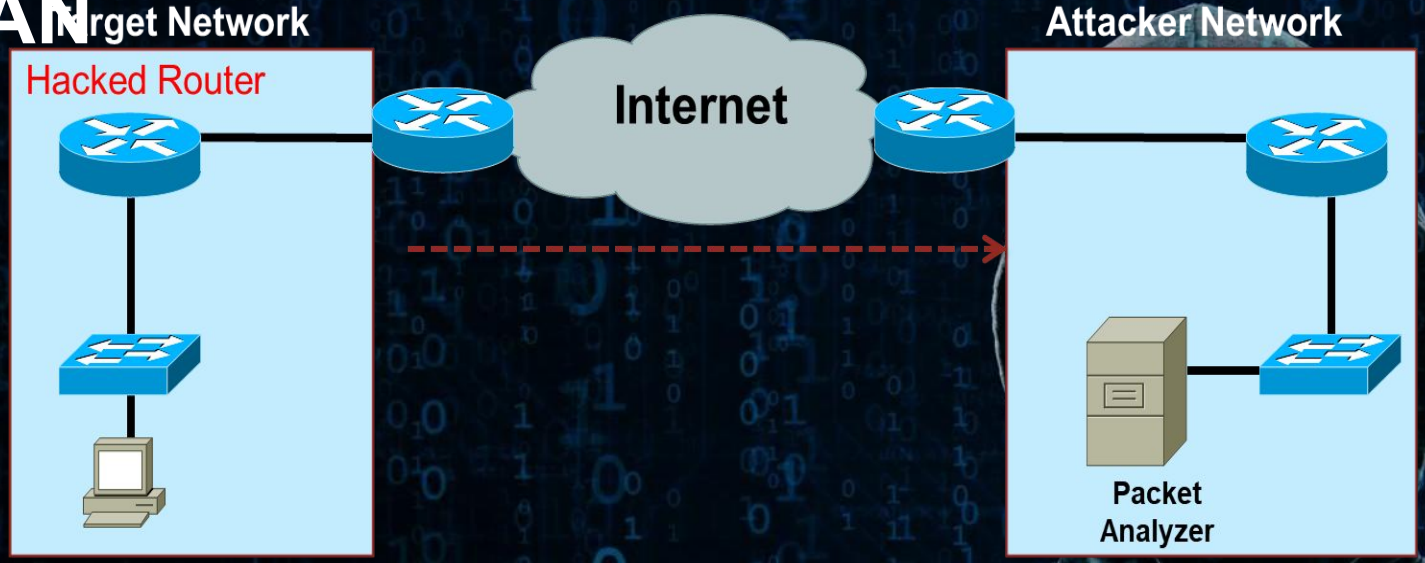


Whitelist the Layer 2 Network Trust Relationships

Whitelist Trusted Information Flows in Monitoring

Secure Control, Management, Data Planes

GRE Tunnel Utilized to Sniff Across WAN

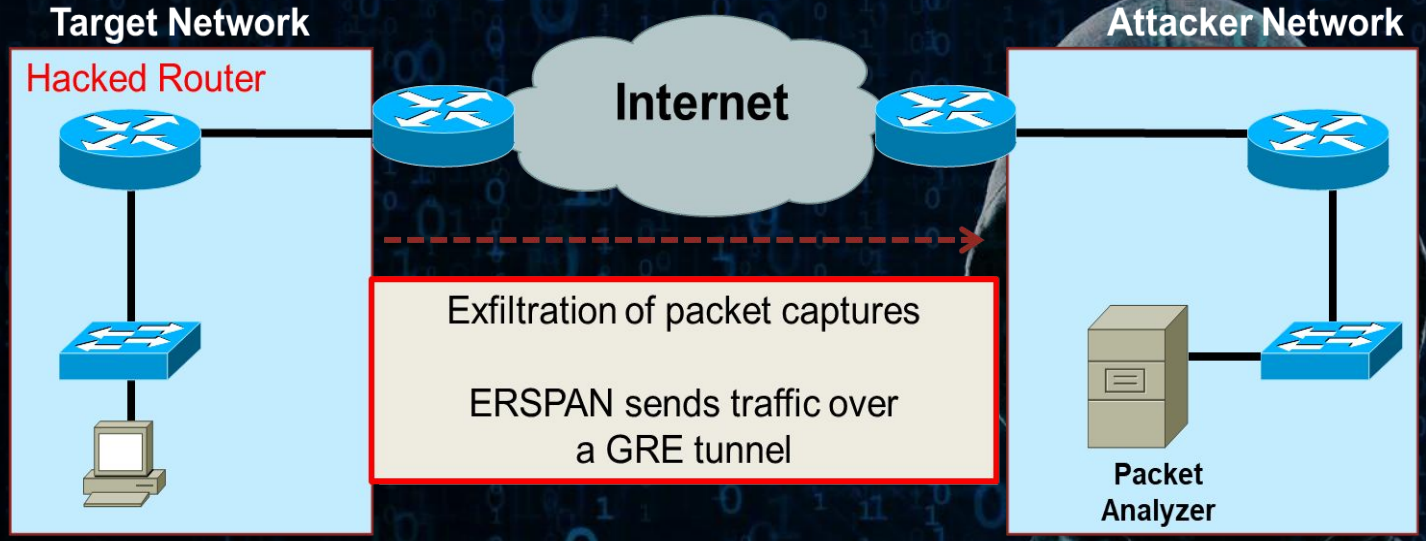


- GRE Tunnel is configured on the hacked router and the attacker's router
- GRE Tunnel interfaces must be in common subnet
- Configure ACL to define traffic of interest on the hacked router
- Define a route map with the ACL and set the next hop to the attacker's GRE tunnel interface IP address
- Similarly define an ACL & route map on the attacker router to redirect traffic to the packet analyzer

Reference: http://www.symantec.com/connect/articles/cisco-snmp-configuration-attack-gre-tunnel

ERSPAN

Enable Packet Capture Across Routed Network

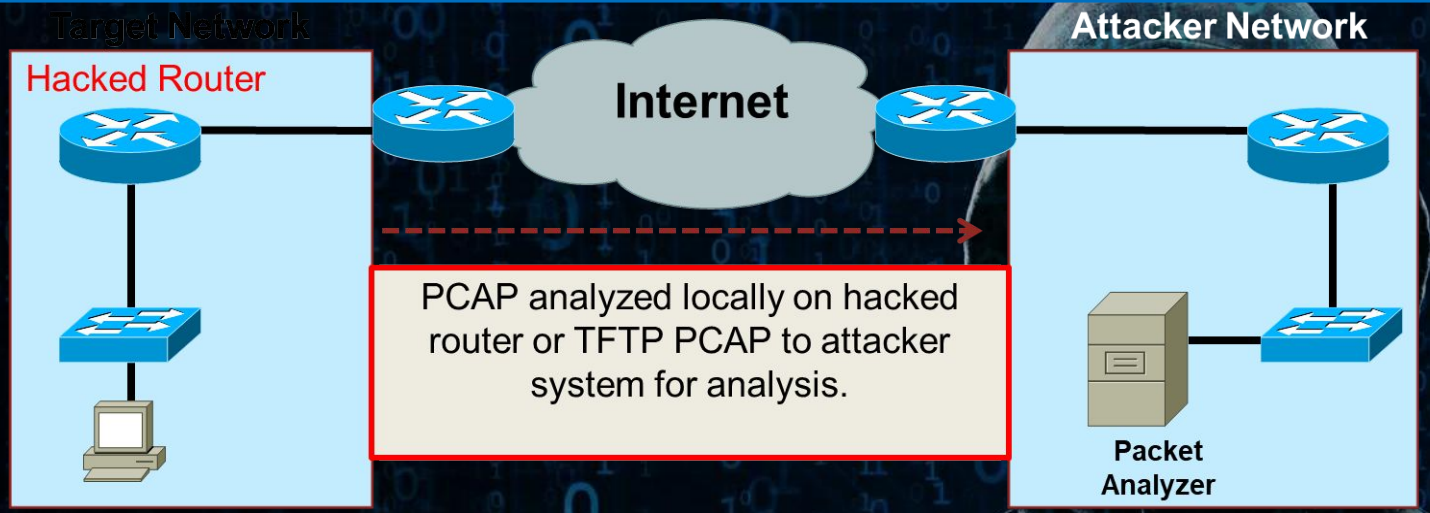



```
monitor session < session ID > type erspan-source
source interface GigabitEthernet1/0/1 rx
source interface GigabitEthernet1/0/2 tx
source interface GigabitEthernet1/0/3 both
destination
  erspan-id < erspan-flow-ID >
  ip address < remote ip >
  origin ip address < source IP >
```

```
monitor session < session ID > type erspan-destination
Source
  ip address < source IP >
  erspan-id < erspan-flow-ID >
  destination interface GigabitEthernet2/0/1
```

References: http://www.cisco.com/en/US/docs/ios/ios_xe/lanswitch/configuration/guide/span_xe.pdf

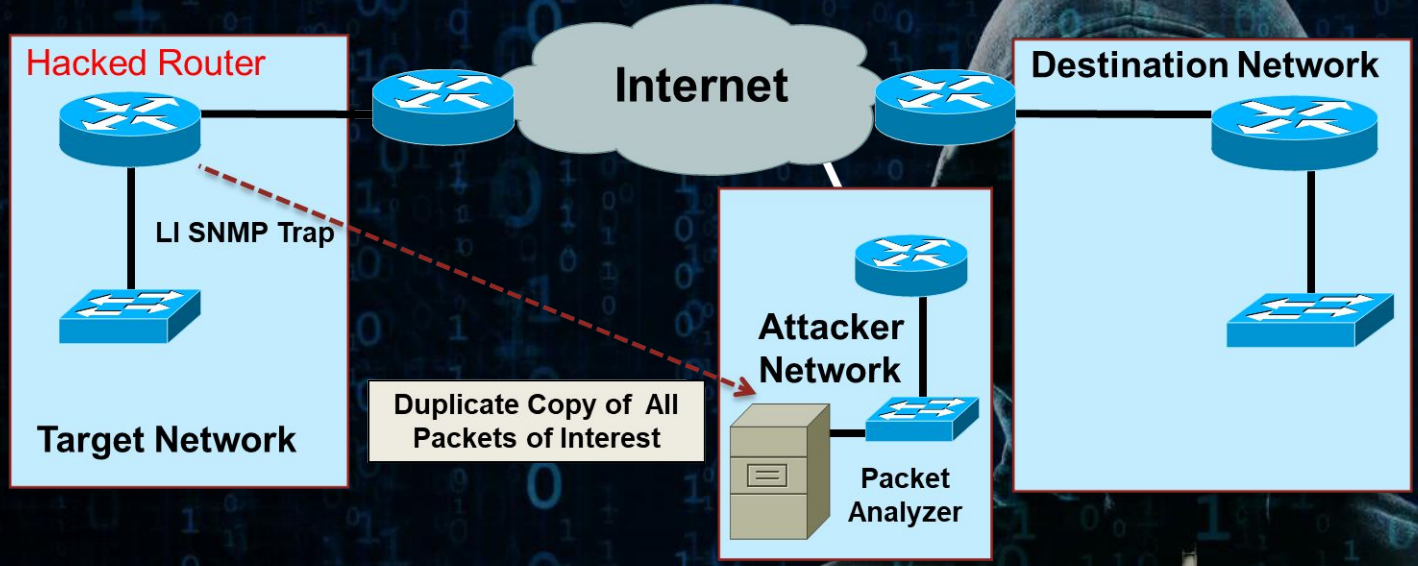
EPC
Embedded Packet Capture - Router



- EPC is an excellent tool for network administrators
- Router is an even higher value target for adversary with inline sniffing capability
- Lockdown management plane trust relationships (SSHv2, SNMPv3)
- Implement 2 factor authentication
- Utilize Netflow, syslog, monitor for unauthorized configuration changes

References: https://supportforums.cisco.com/document/139686/configuration-example-embedded-packet-capture-cisco-ios-and-ios-xe

Lawful Intercept Exploit Scenario



Snmp-server view <*view-name*> ciscoTap2MIB included
Snmp-server view <*view-name*> ciscoIpTapMIB included
Snmp-server group <*group-name*> v3 auth read <*view-name*> *write* <*view-name)* notify <*view-name*>
Snmp-server host <*ip-address*> traps version 3 priv <*username*> udp-port <*port-number*>
Snmp-server user <*mduser-id*> <*groupname*> v3 auth md5 <*md-password*>

References:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/lawful/intercept/65LI.pdf
http://www.cisco.com/en/US/docs/routers/asr9000/software/asr9k_r4.1/security/configuration/guide/syssec_cg41asr9k_chapter3.pdf

Routers Hacked to Sell VoIP Services



“On his way to federal prison, the 23-year-old hacker says breaking into computers at telecom companies and major corporations was "so easy a caveman could do it.”

“Assistant U.S. Attorney Erez Liebermann said Pena allegedly stole and then sold more than 10 million minutes of service at deeply discounted rates, netting more than $1 million from the scheme.”

“The government identified more than 15 VoIP service providers that were hacked into, adding that Moore scanned more than 6 million computers just between June and October of 2005. AT&T reported to the court that Moore ran 6 million scans on its network alone.”

“Moore said what made the hacking job so easy was that 70% of all the companies he scanned were insecure, and 45% to 50% of VoIP providers were insecure. The biggest insecurity? Default passwords.

"I'd say 85% of them were misconfigured routers. They had the default passwords on them," said Moore.“

Source: http://www.informationweek.com/interview-with-a-convicted-hacker-robert-moore-

Salt Typhoon Campaign Identified Telco Network Issues Are Not New Lack of Management Plane Zero Trust Configuration and

Alex Sharpe



Guiding Principles for Resilient ZT Implementations

Alex Sharpe, Managing Director, Sharpe 42 LLC

2 April 2025

Guiding Principles for Resilient ZT Implementations

PRESENTED BY



Alex Sharpe

Managing Director, Sharpe42

1. The Principles
2. Castles & Moats
3. Inside Out not Outside In
4. Continuously Monitor/ Breaches Happen
5. Next Steps
6. Resources

Copyright Sharpe 42

Alex Sharpe “Sharpe like a knife”™

Big 4 Trained Management Consultant with Real World Operational Experience

Practitioner, Consultant, Speaker, Author

35+ years Cybersecurity
25+ years Digital

Transformation AI Governance,

Resilience

Zero Trust, GRC, National Security, Compliance™

alex@SharpeLLC.com

www.linkedin.com/in/alex-sharpe-3rd/



Copyright Sharpe 42

Acknowledgements

Lead Authors

- Alex Sharpe

Contributors

- Robin Basham
- Madhav Chablani
- Frank DePaola
- Jonathan Flack
- Sai Honig
- Shamik Kacker
- Andrea Knoblauch
- Alice Muravin
- Rajesh Murthy
- Denis Nwanshi
- Lars Ruddigkeit
- Lauren Wojno Wise
- Paul Simmonds
- Nelson Spessard
- Bernd Wegmann
- Heverin Joy Williams

Reviewers

- Sam Aiello
- Jason Garbis
- Brett James
- Yves Le Gelard
- Jennifer Minella
- Chandrasekaran Rajagopalan
- Aaron Robel
- Michael Roza
- Vaibhav(VB) Malik
- Meghana Parwate
- Sven Olensky,
- Annabelle Lee
- Himanshu Sharma

CSA Staff

- Erik Johnson
- Stephen Lumpe
- Stephen Smith,
- Marina Bregkou

Copyright Sharpe 42

Audience

- As guiding principles, they cut across all Zero Trust and Resilience initiatives.
- Information protection practitioners and their executive management.
- Industry bodies and standards organizations to:
  - Progress thought leadership
  - build out the Zero Trust and Resilience body of knowledge (BOK).

Copyright Sharpe 42

Zero Trust

Zero trust (ZT) is the term for an evolving set of **cybersecurity paradigms** that move defenses from static, network-based perimeters to **focus on users, assets, and resources**. A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows. 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)…Zero trust is a **response to enterprise network trends** that include **remote users**, bring your own device (**BYOD**), and **cloud-based assets** that are not located within an enterprise-owned network boundary. Zero trust focuses on **protecting resources (assets, services, workflows, network accounts, etc.)…**

NIST SP 800-207, "Zero Trust Architecture"

Copyright Sharpe 42

Resilience

"…the ability to remain viable amidst adversity and to be better for it."

The lens of Zero Trust:

- 80% Identity and Access Management (IAM)
- 20% Limiting the Blast Radius (e.g., segmentation)
- Presume incidents (like ZT) ***but remain operational***

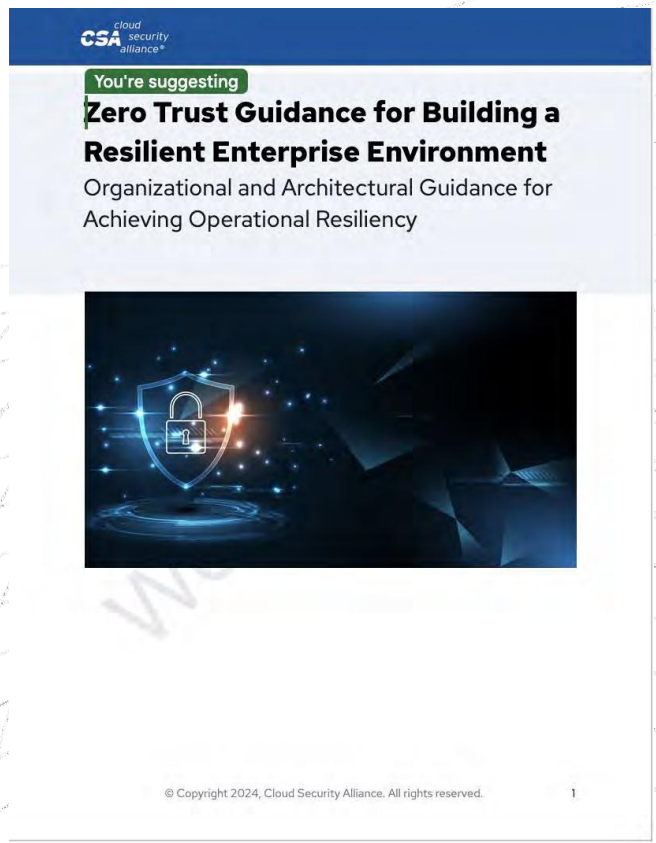
Resilience is a major focus for government, businesses, legislatures, and regulators

ISACA Journal, Volume 4
What is Resilience and How Does It Promote Digital Trust
https://www.isaca.org/resources/isaca-journal/issues/2024/volume-4/what-is-resilience-and-how-does-it-promote-digital- trust

Copyright Sharpe 42

Zero Trust Guiding Principles

- Originally released, July 2023
- Version 1.1 Released Sept 2024 https://cloudsecurityalliance.org/artifacts/zero-trust-principles-v- 1-1
  - AI
  - Readability
  - Visuals
- Zero Trust for Small and Medium Sized Businesses (SMB) released January 2025 https://cloudsecurityalliance.org/artifacts/zero-trust-guidance- for-small-and-medium-size-businesses-smbs
- Coming Soon:"Zero Trust Guidance for Building a Resilient Enterprise Environment"
  Organizational and Architectural Guidance for Achieving Operational Resiliency
- Always looking for contributors



Drivers

- Zero Trust is a simple approach that is **often misunderstood and overcomplicated**
- Historically, InfoSec relied heavily on technical controls, with security models based on the ability to collect assets and surround them within a **controlled physical perimeter**
- Traditional Security Models are based on Castle and Moat strategies – **no longer the way we work and live**
- **Full cyber lifecycle**: Protect, Detect, Recover
- **“never trust, always verify”**
- **Reduce** Total Cost of Ownership (**TCO**), damage from incidents, and **promote** faster recovery times
- Harmonize with a **single voice**
- Zero Trust – done once, benefits many

Copyright Sharpe 42

Zero Trust Is/ Is Not

- Don’t over think
- ZT is a philosophy/ a way of thinking
- ZT is NOT a set of products
- ZT is NOT an architecture
- ZT is a collaboration between Process, People,Technology and Organization
- ZT is part of your Cyber Risk Management
- Many standards originated for an On-Prem world; ZT is hybrid cloud



Copyright Sharpe 42

Zero Trust Guiding Principles

- Begin with the End in Mind (Business / Mission Objectives)
- Do Not Overcomplicate
- Products are Not the Priority
- **Access is a Deliberate Act**
- **Inside Out, not Outside In**
- **Breaches Happen**
- Understand your Risk Appetite
- Ensure the tone from the top
- Instill a Zero Trust Culture
- Start Small and Focus on Quick Wins
- **Continuously Monitor**



Guiding Principles Broad Categories

1. Established principles applied to Zero Trust
2. To provide clarity
3. Myth Busting

Many fit into more than one category.

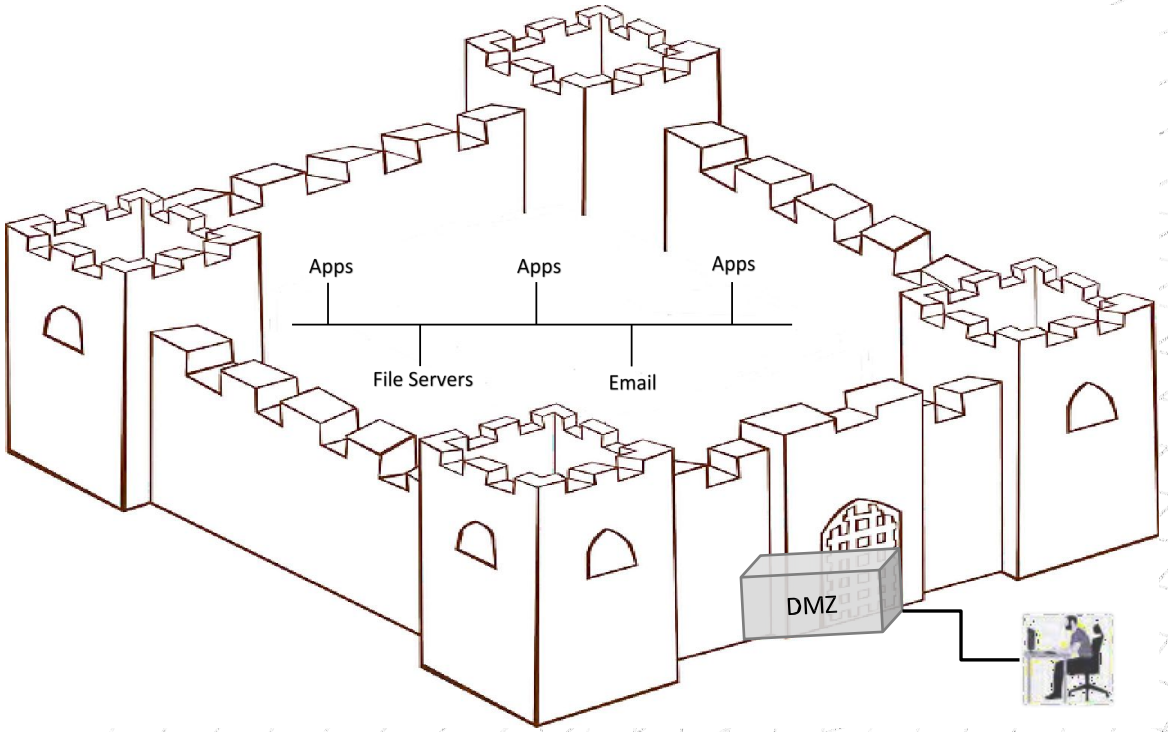
Copyright Sharpe 42

Castles & Moats

Copyright Sharpe 42

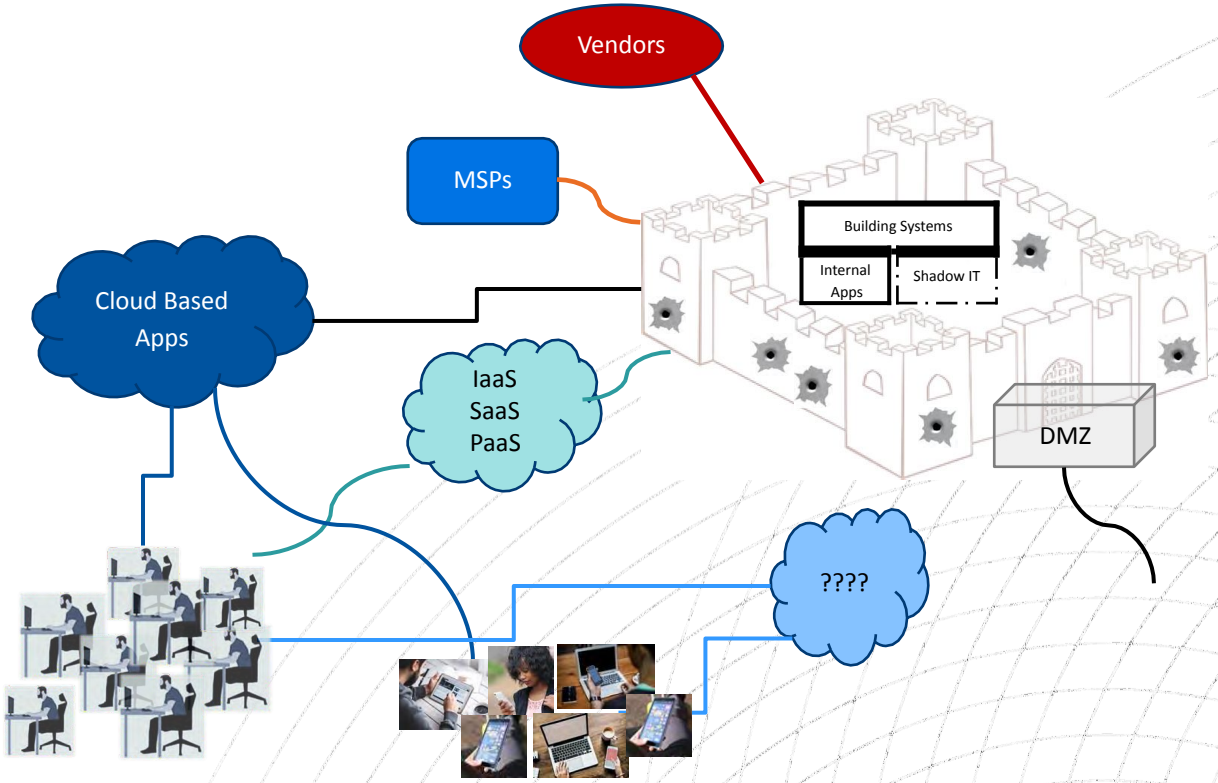
15

Traditional



Copyright Sharpe 42

POST COVID-19



Inside Out not Outside In

Copyright Sharpe 42

Inside Out

DAAS

- **D**ata — Credit card information (PCI), protected health information (PHI), personally identifiable information (PII) and Intellectual Property (IP)
- **A**pplications — Custom, COTS, GOTS, SaaS
- **A**ssets — Devices, SCADA controls, point-of-sale terminals, medical equipment, manufacturing assets, IoT devices
- **S**ervices — DNS, DHCP and Identity source of truth

Focusing on Assets also promotes alignment with Strategy and Desired Outcomes

Copyright Sharpe 42

Data Flows

Flows to and from DAAS

- Useful in identifying your *Protect Surface*
- Data flow diagrams are becoming increasingly required (e.g., CMMC)
- Understand interdependencies
- Secure entry and exit points
- Secure paths to and from

Copyright Sharpe 42

Executive Key Questions

Are we focused on the right

things? Are we investing

adequately?

=> Capital Allocation.

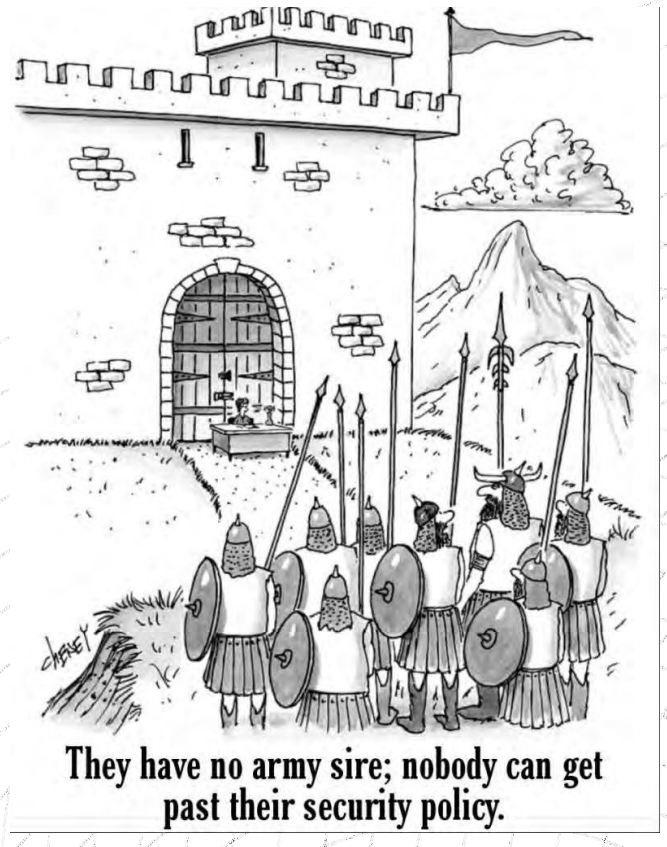
Business Impact Assessment (BIA) to drive priorities.

Consistent with:

- National Cybersecurity Strategy
- SEC Cyber Rule(s)
- NIST Cybersecurity Framework (CSF) 2.0
- EO 14028
- Digital Operational Resilience Act (DORA)
- New York State Department of Financial Services

Corporate Policy

- Corporate Direction
- Communication
- “Kiplinger”
  - Who
  - What
  - Where
  - When
  - Why
  - How

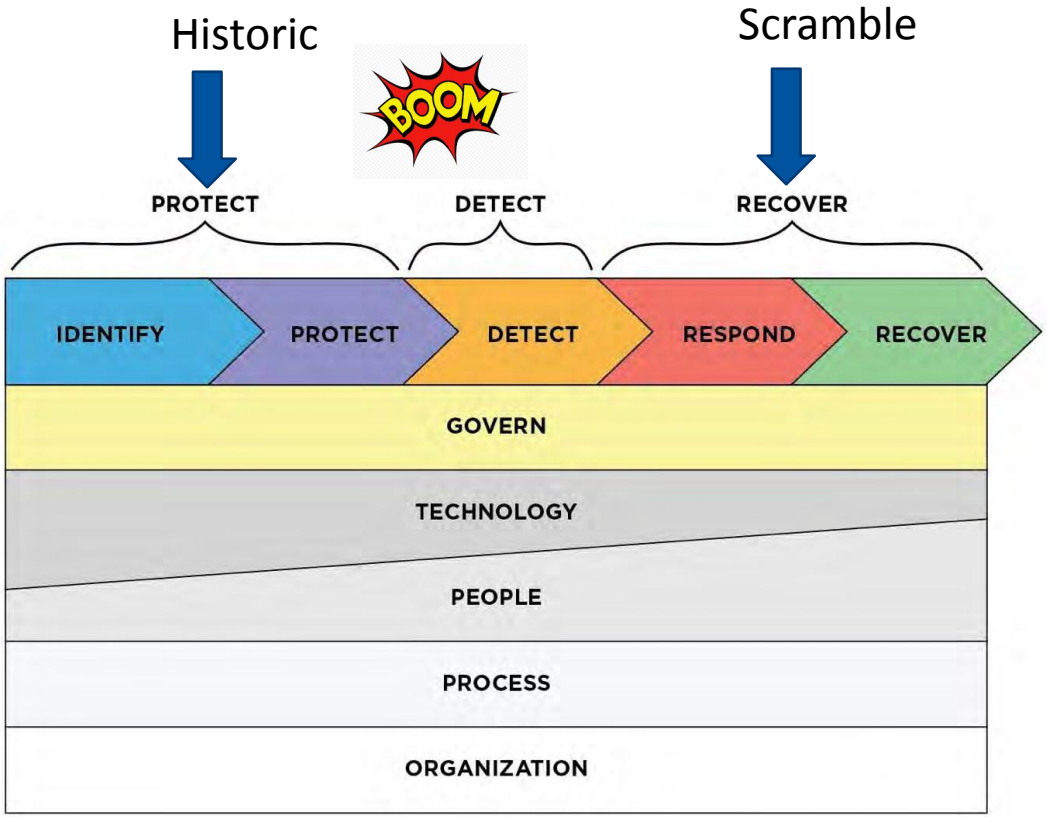


Copyright Sharpe 42

Incidents Happen/ Continuously Monitor

Reduce Impact, Detect Faster, Recover Faster

Copyright Sharpe 42



Greatest damage to Digital Trust

Average time to detect a breach is pushing 300 days (not including hackers telling you)

Continuously Monitor

Who Detects a Breach?

- 33% Internal teams and tools
- 27% Attacker as part of Ransomware
- 40% Benign third parties and outsiders IBM Cost of Data Breach Report

Globally, across sectors:

- 204 days to identify and 73 days to contain a breach. Financial sector:
- 177 days to identify and 56 days to contain. Security Intelligence



Closer to 300 days when not notified by the attacker (ransomware)

Malware attacks are deadly

A Machine infected with malware affects 22 others (on average)

Hop 1:	22
Hop 2:	484
Hop 3:	10,648
Hop 4:	234,256

Reduce the Blast Radius

Detect faster

Recover quicker

Segmentation/ Micro-segmentation prevents the spread

Copyright Sharpe 42

Want to get involved?

Frank DePaola
frank@fadepaola.com
https://www.linkedin.com/in/frankdepaola/

Erik Johnson
ejohnson@cloudsecurityalliance.org
https://www.linkedin.com/in/erikjohnson2/

Alex Sharpe
alex@SharpeLLC.com
https://www.linkedin.com/in/alex-sharpe-3rd/

Resources

Copyright Sharpe 42

Zero Trust Resources

Federal Zero Trust Resource Hub
https://zerotrust.cyber.gov/

Zero Trust Advancement Center
https://cloudsecurityalliance.org/zt/

NSA Cybersecurity Advisories & Guidance
https://www.nsa.gov/Press-Room/Cybersecurity-Advisories-Guidance/

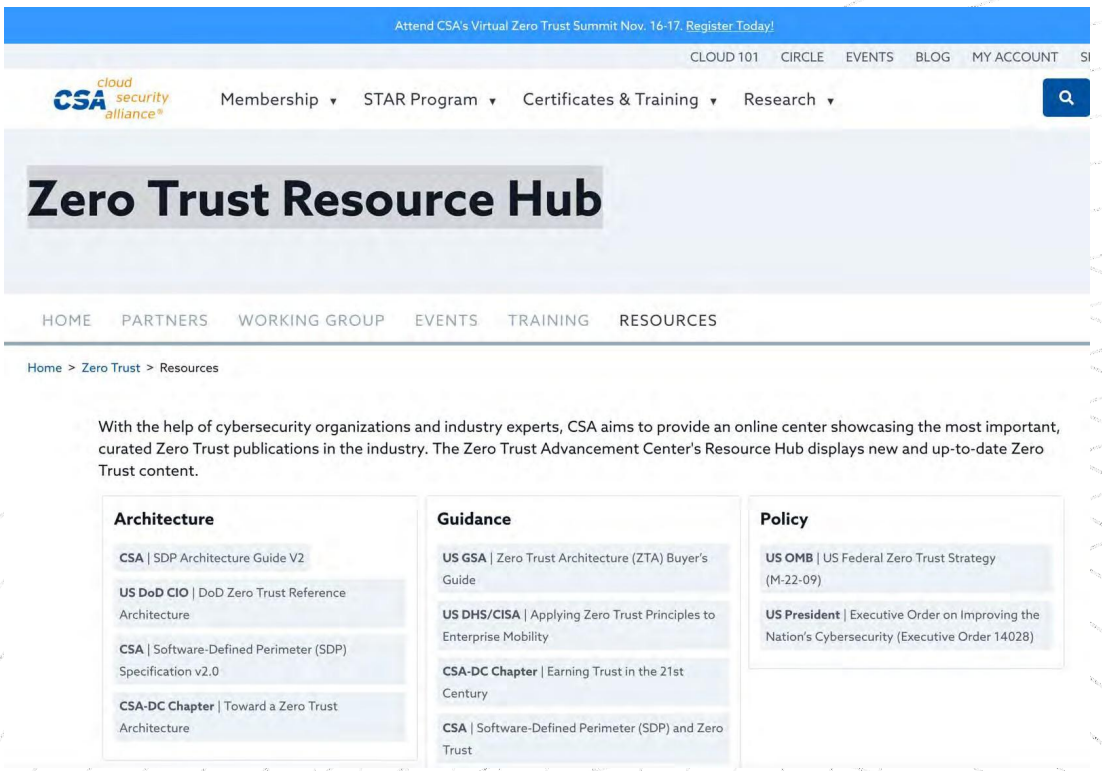
CISA's Zero Trust Maturity Model Version 2.0
https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

Zero Trust Guiding Principles
https://cloudsecurityalliance.org/artifacts/zero-trust-guiding-principles/

Communicating the Business Value of Zero Trust
https://cloudsecurityalliance.org/artifacts/communicating-the-business-value-of-zero-trust/

Copyright Sharpe 42

https://cloudsecurityalliance
. org/zt/resources/



Zero Trust Items

CISA Applying Zero Trust Principles to Enterprise Mobility

https://www.cisa.gov/sites/default/files/2023-01/Zero_Trust_Principles_Enterprise_Mobility_For_Public_Comment_508C.pdf

NSA Embracing a Zero Trust Security Model

https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/-/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.pdf

Advancing Zero Trust Maturity Throughout the User Pillar

https://media.defense.gov/2023/Mar/14/2003178390/-1/-1/0/CSI_Zero_Trust_User_Pillar_v1.1.PDF

Advancing Zero Trust Maturity Throughout the Device Pillar

https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3562460/nsa-shares-recommendations-to-advance-device-security-within-a-zero-trust-frame/

Copyright Sharpe 42

Resources

https://www.grf.org/

https://krebsonsecurity.com/

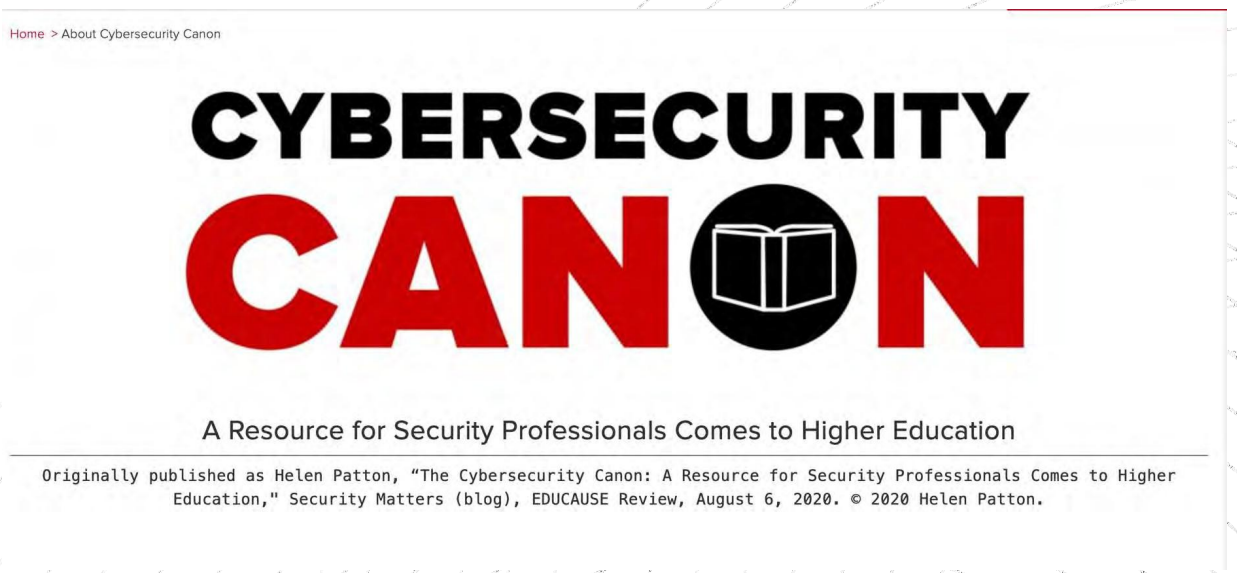
https://www.cisa.gov/

https://www.isaca.org/

https://cloudsecurityalliance.org/

The Ohio State University

Book Reviews
https://icdt.osu.edu/cybercanon/bookre views



Resources

”Embracing a Zero Trust Security Model”, National Security Agency (NSA), Cybersecurity Information,
Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov

“CISA Zero Trust Maturity Model”
https://www.cisa.gov/zero-trust-maturity-model

“CSA Zero Trust Advancement Center”,
https://cloudsecurityalliance.org/zt/?_ga=2.244227201.587457479.1665333778-1649108214.1663679673

“SP 800-207, Zero Trust Architecture”, NIST
https://csrc.nist.gov/publications/detail/sp/800-207/final

“Executive Order on Improving the Nation’s Cybersecurity”, EO 14028,
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the- nations-cybersecurity/

“NSTAC Report tp the President, Zero Trust and Trusted Identity Management”
https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on

“Sharpe like a knife” Do not hesitate to call

Looking for thought to leaders to progress the state of the art through the working groups.





Alex Sharpe

alex@Sharpe42.com
www.linkedin.com/in/alex-sharpe-3rd/

David Voelker



DON Implement Zero Trust Blueprint

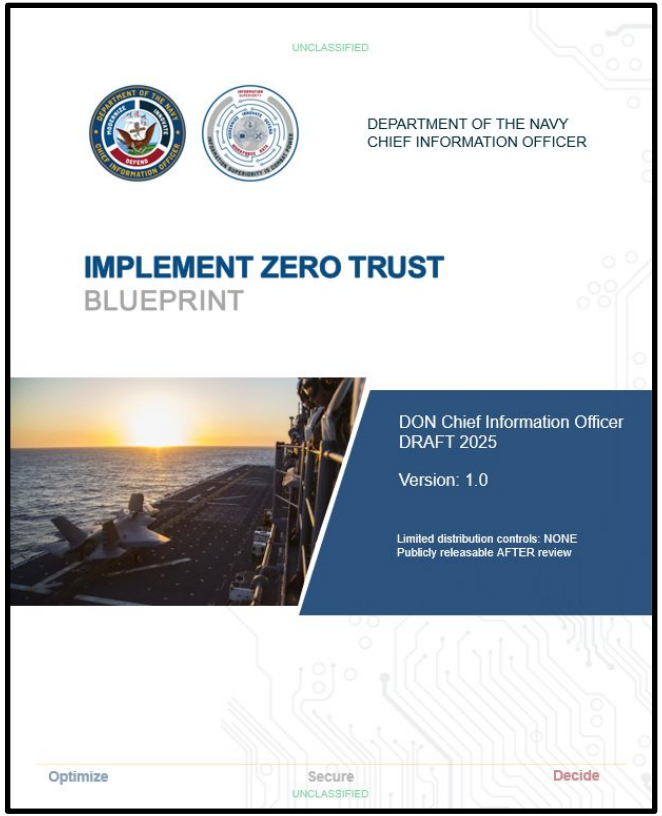
David L. Voelker, DON CIO ZT Implementation Lead

March 2025

Controlled by: Department of the Navy
Controlled by: DON CIO/CTO
CUI Categories: N/A
Distribution/Dissemination Control: DISTRO A
POC: david.l.voelker.civ@us.navy.mil

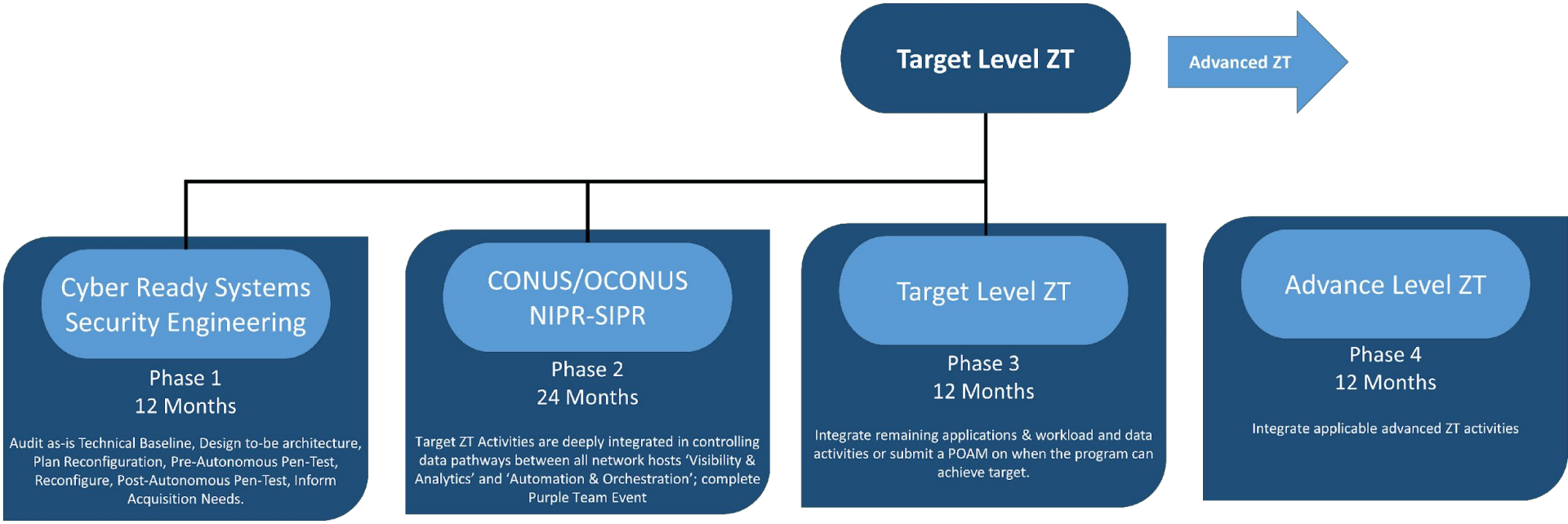
Agenda

- DON ZT Implementation Plan Phases
- Standards Based ZT Architecture
- Continuous Monitoring, Awareness, and Control
- Design Patterns and Approaches
- Resources
- Q&A

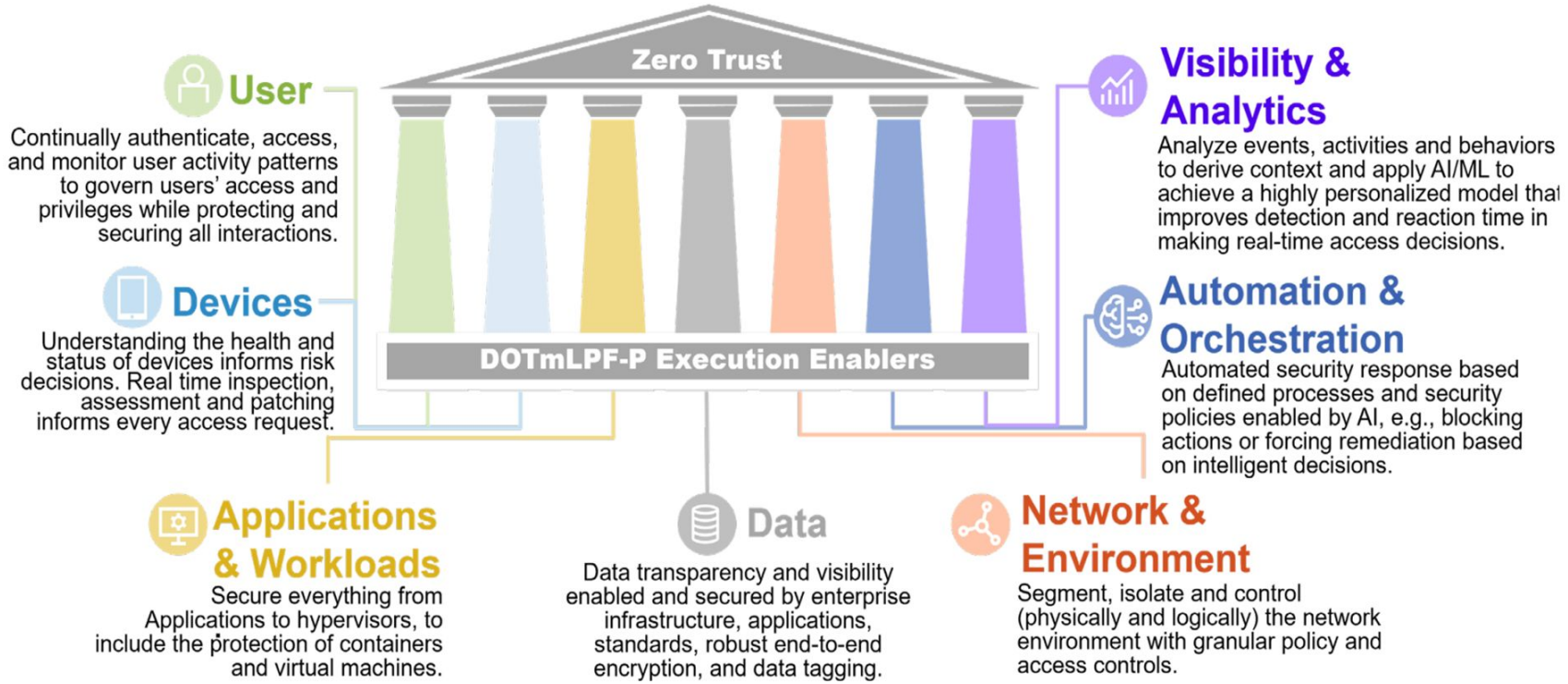


DON ZT Implementation Plan Phases

DON ZT Implementation Plan



DON is a Zero Trust aligned organization at all levels by the end of the decade



Standards Based ZT Architecture

Standards Based ZT Architecture

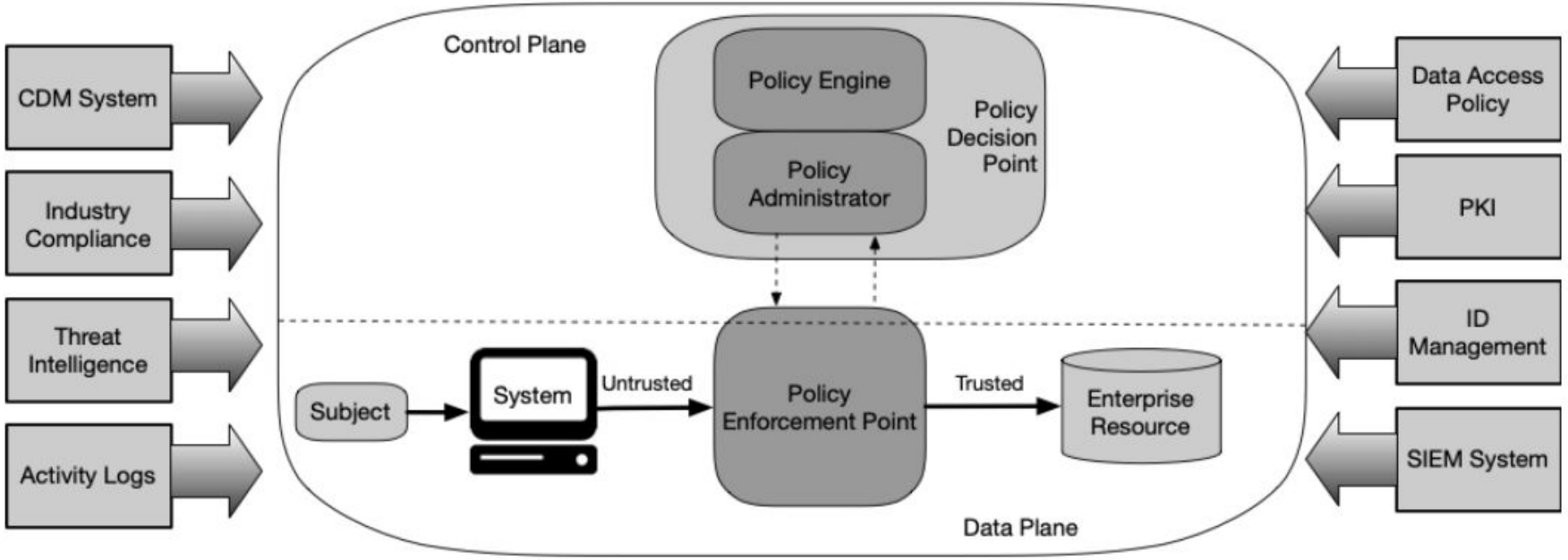
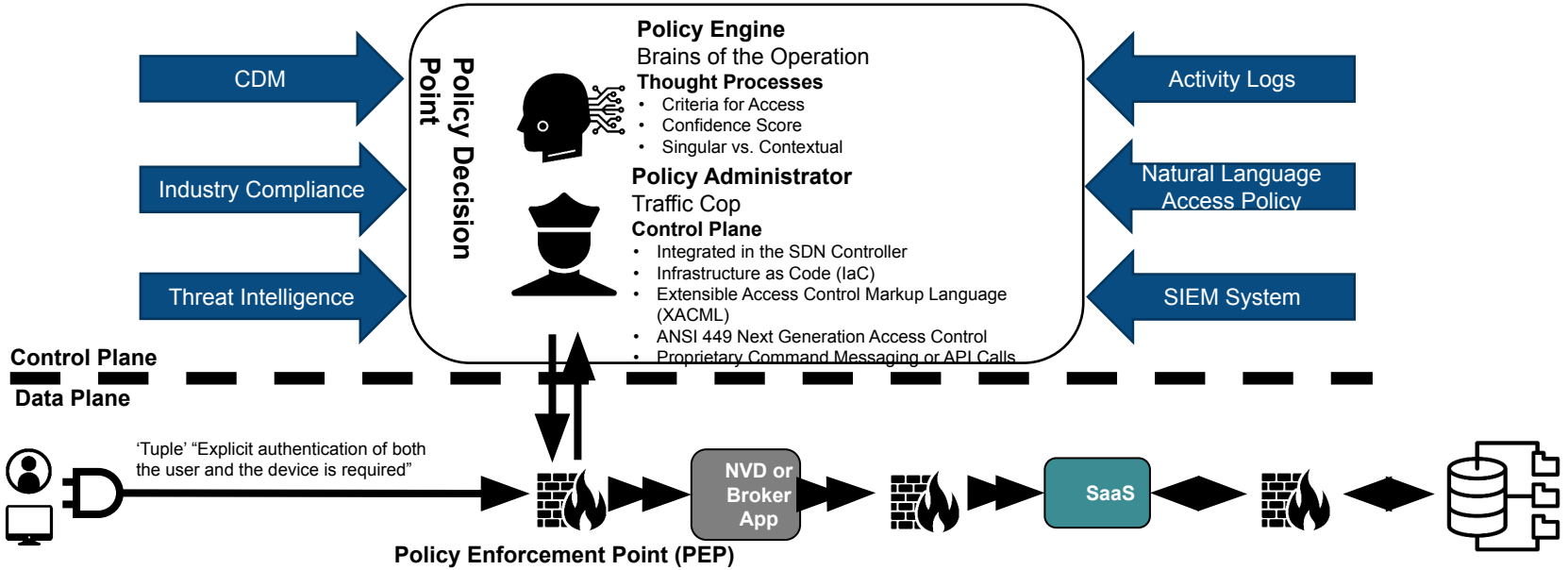


Figure 2: Core Zero Trust Logical Components

Standards Based ZT Architecture



Continuous Monitoring

Continuous Awareness

Continuous Control

Cyber Chess Match

- Assume the adversary has the same visibility and cyber situational awareness you have, maybe more
- They will use deception and decoys, you should too
- The adversary will cheat



Cyber Chess Match

- You face multiple adversaries
- **Detection** is paramount
- They will control the game, if allowed



Cyber Chess Match

- The adversary will take your turn
- They will change the rules
- They will attempt to deny you control



Design to Win!

- Design the systems to take full advantage of technological strengths
- Deploy Micro-segmentation to limit and eliminate adversary surveillance
- Implement AI/ML UEBA, deny the adversary's ability to move
- Exercise continuous Monitoring, Awareness, Command and Control



Design Patterns and Approaches

Collaboration and Strategic Partnerships

- Seek focused expertise from the Enterprise ICAM Service, System Security Engineering Team (SSET) and CSSPs, inherit the best in breed solutions:
  - ❑ Authentication and Authorization
    - Outcome hardened ICAM solution
  - ❑ Visibility & Analytics
    - Outcome Continuous **Detection**
  - ❑ Automation & Orchestration
    - Outcome Continuous **Control**

- Program expertise:
  - ❑ Deeply integrate Macro / Micro-Segmentation
    - Outcome **Detection and Control** (Permit/Deny) Points are Identified, Defined and Operational
  - ❑ Prioritize all remaining applicable ZT activities
    - Outcome Target Level ZT Achieved; Warfighting Capabilities can operate in a contested cyber domain, deny the adversary, and win every time



Audit the Technical Baseline

- Identify HW/SW Reconfiguration or Replacement Options and Requirements
  - Schedule Autonomous Penetration testing before and after reconfigurations
- Types of Users and Locations
  - Onsite / Offsite
  - CONUS/OCONUS
- Devices
  - Networking Equipment
  - End Points
- Data Pathways
- Applications
- Data Stores



Identify applicable ZT activities; create an initial mapping of ZT requirements to functions in the technical baseline

Prioritize ZT implementation based on Target Network, Devices, User, Visibility and Analytics, Automation and Orchestration requirements

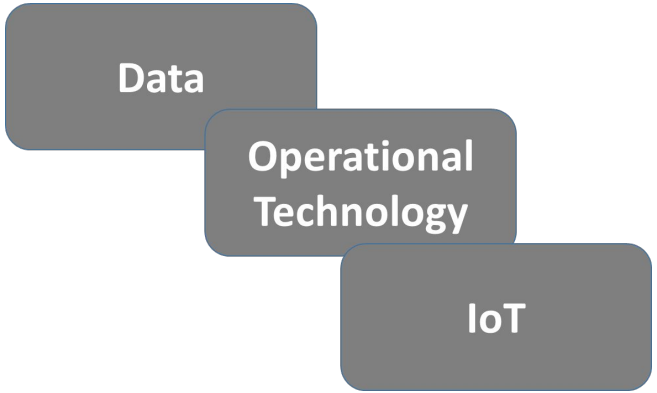
Followed by remaining Target Level ZT activities, ensuring full alignment with ZT requirements and security controls up the OSI and Cloud Hosting Stack

Apply applicable advanced ZT activities

Identify what you want to protect

- The next step in designing a ZTA is identifying the critical assets that need protection
- This includes data, applications, systems, and network resources
- Understanding what needs to be protected helps prioritize security efforts and allocate resources effectively





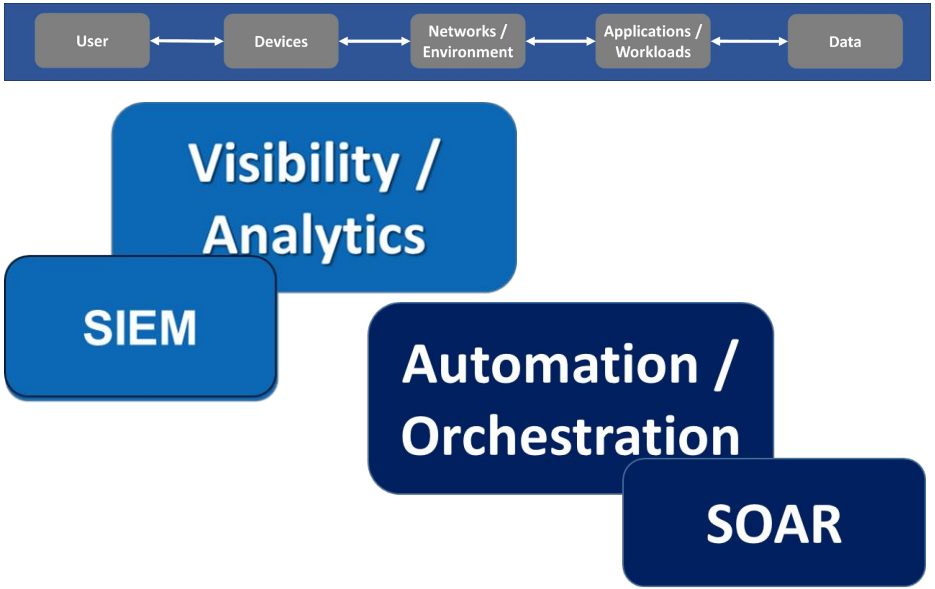
Define Mission Outcomes

- Define mission outcomes that account for continuous operation and resilience in the face of potential breaches
- Assume that adversaries are already inside the network
- This mindset ensures that security measures are proactive rather than reactive

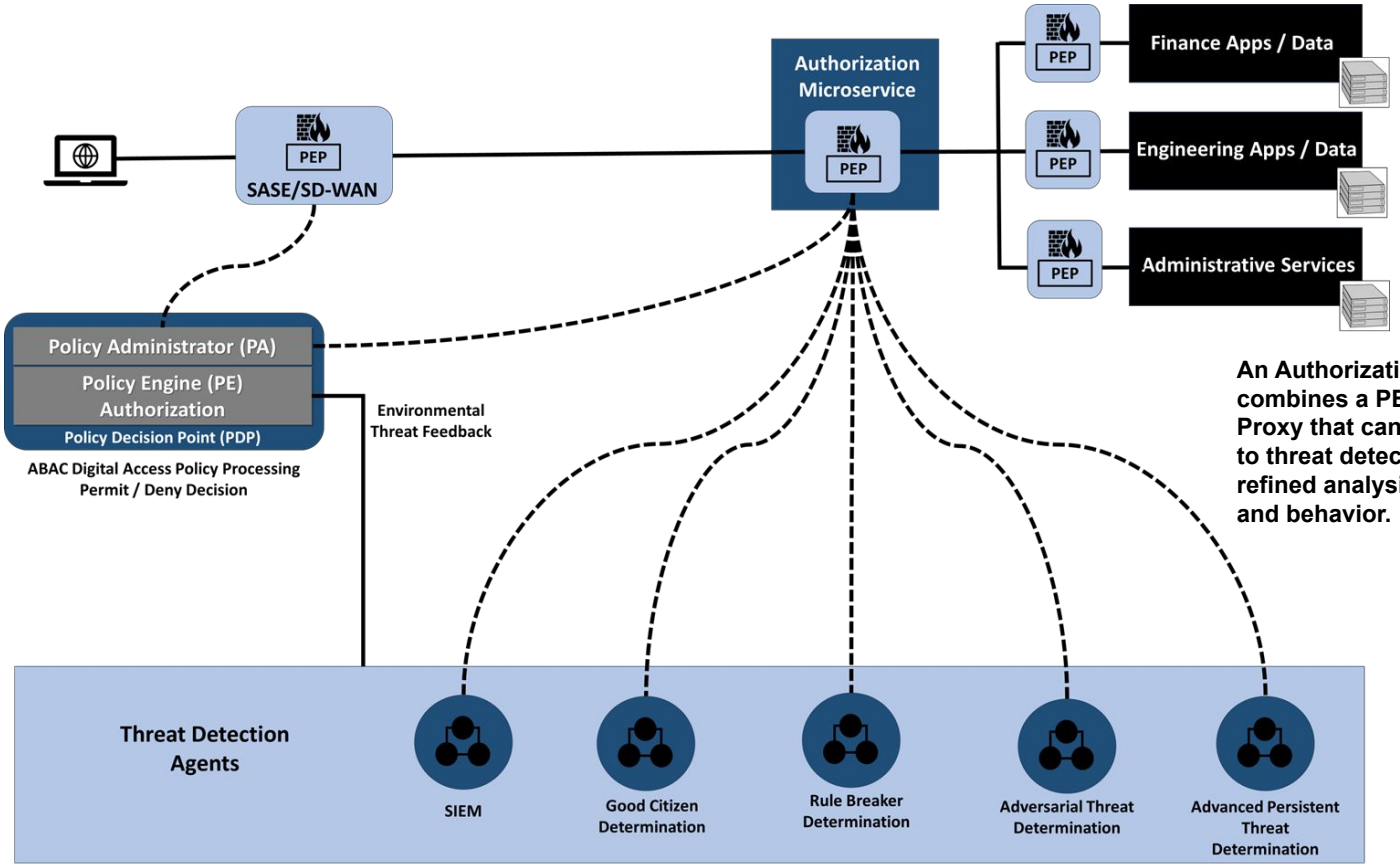


Map Transaction Flows

- Understand how data and processes flow within the network is essential
- Identify data pathways between users, applications, and systems
- Analyze the interactions and dependencies among network components
- Recognize potential points of vulnerability and interception
- Ensure that all transaction flows are secured and monitored

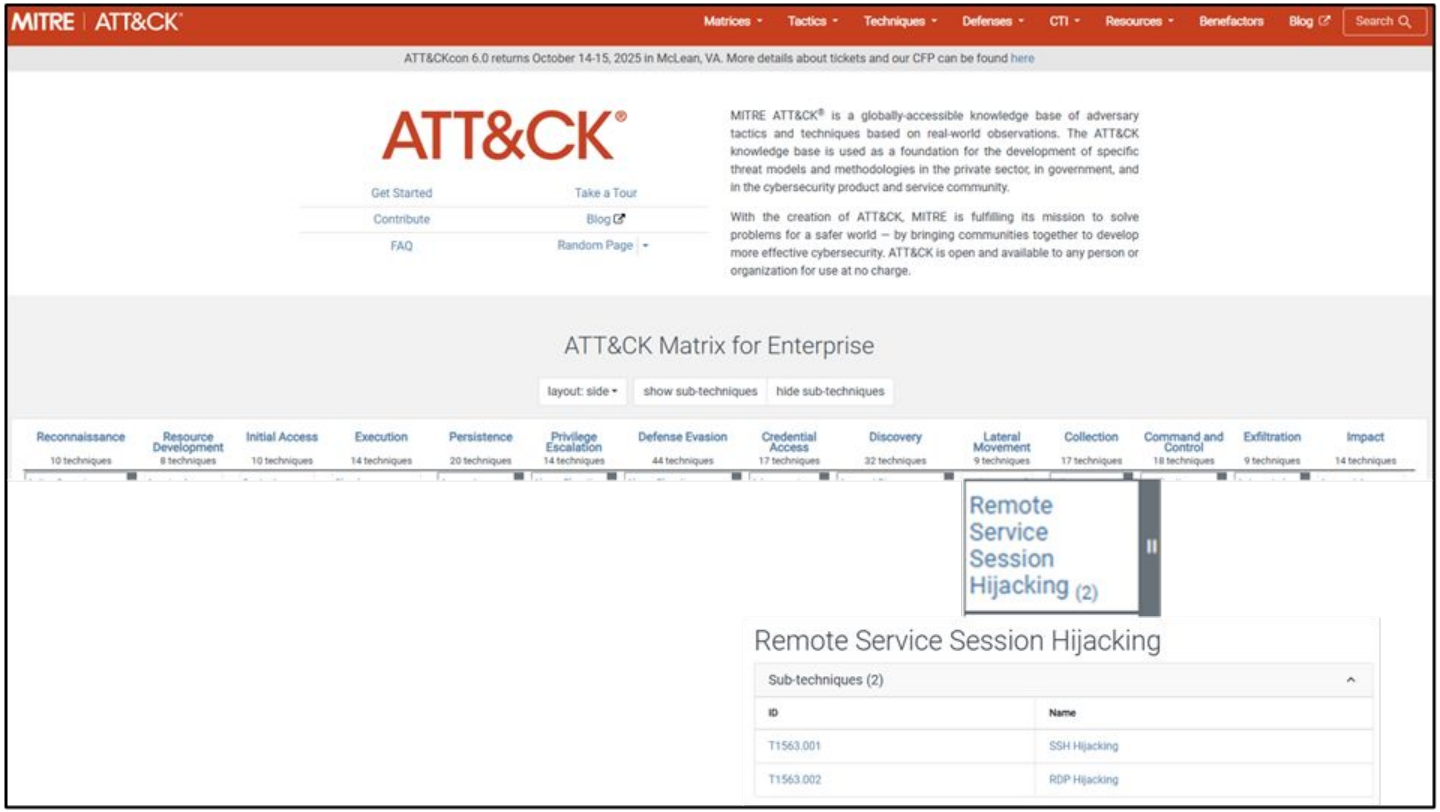


Agentic Threat Detection Framework



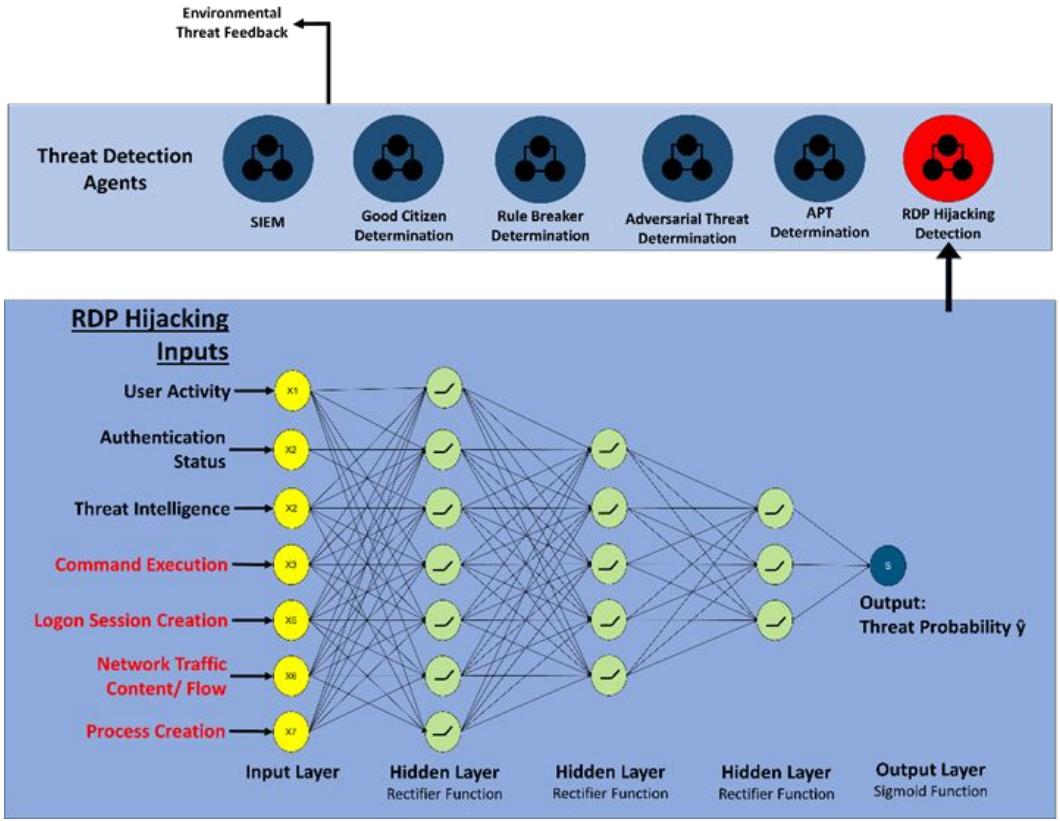
An Authorization Microservice combines a PEP with a TLS v1.3 Proxy that can copy network traffic to threat detection agents for deep refined analysis of user activities and behavior.

MITRE ATT&CK: Remote Service Session Hijacking



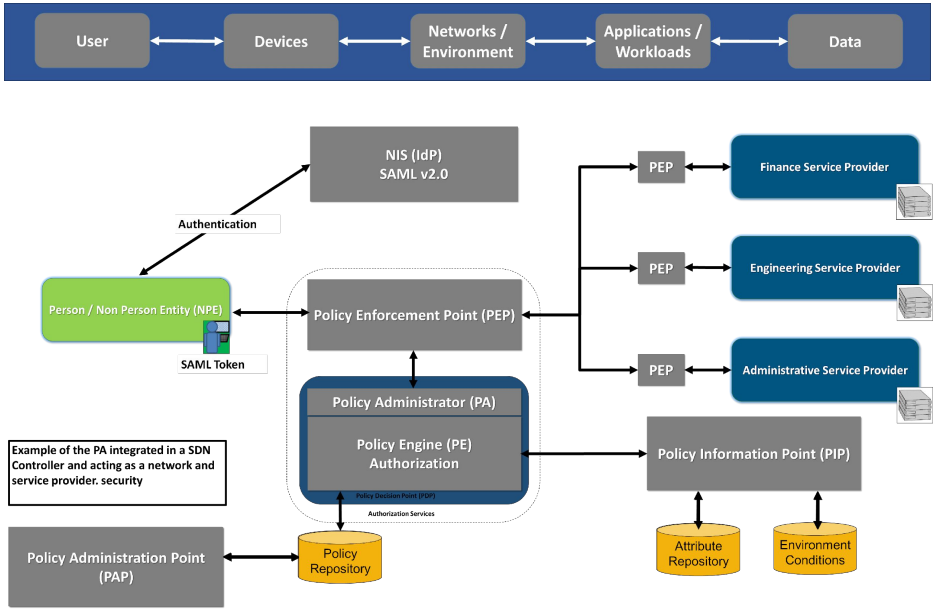
RDP Hijacking Detection Agent

- Detection recommendations
  - Command Execution
  - Logon Session Creation
  - Network Traffic Content / Flow
  - Process Creation



Determine Means of User, Device, and Network Access

- Access control is a cornerstone of ZT
- Apply network segmentation to isolate sensitive data and systems



Zero Trust Architecture NIST SP 800-207 / Attribute Based Access Control (ABAC) NIST SP 800-162 Composite Diagram

Design the Architecture

- Start by securing core data and systems; implement micro segmentation using PEPs to the Macro Boundary
- Determine Access Criteria
- Develop Access Policies
- Design Thinking Activities
  - Tabletop Mission Cyber Risk Assessments (TMCRAs)
- Implement a Metamorphic Cyber Landscape to confuse adversary surveillance techniques
  - Deploy active and changing cyber safeguards, deception and decoy strategies and technologies

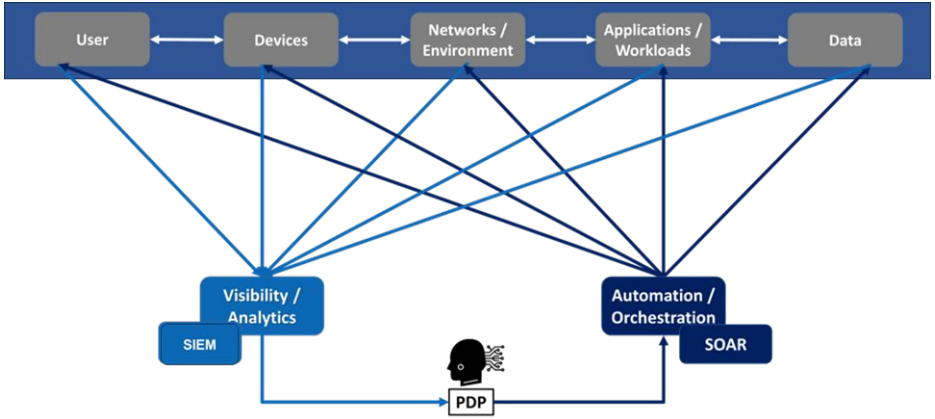


User and Entity Behavioral Analytics (UEBA) "Enhances security by analyzing the behavior of users and entities to identify anomalies that could indicate potential threats" **UEBA is the ZT Lynch Pin!**

Consult **Naval Network Warfare Command (NAVNETWARCOM)** on technical baseline design options that enhance current technology detection strengths

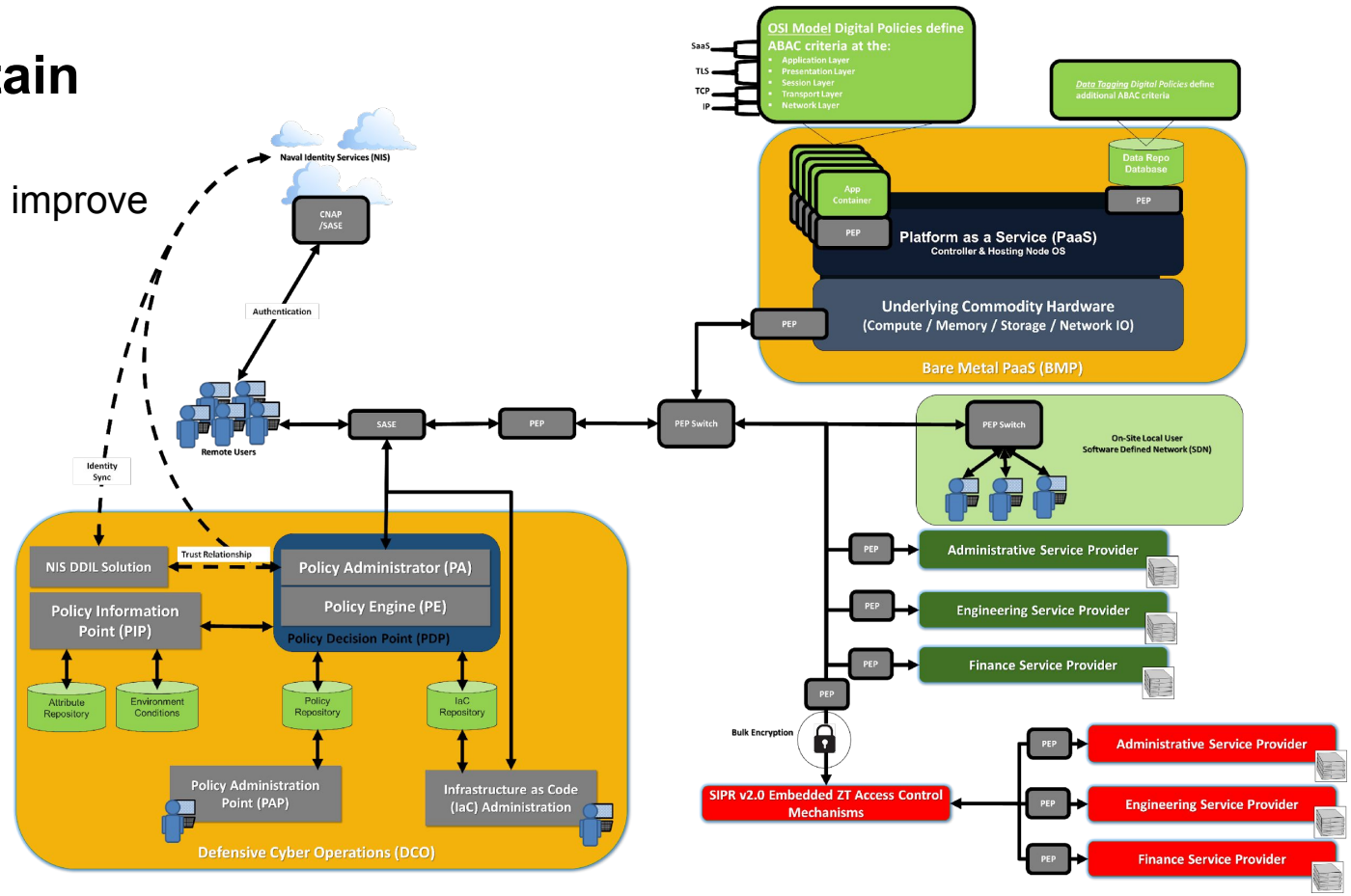
Prototype and Test

- **Verify** that all ZT **requirements** have been implemented
- **Validate** each ZT activity can demonstrate the desired outcome reaching the specified **success criteria**
- Determine how much Visibility is required to detect threat
- Determine how much Command and Control is required to enforce permit / deny access decisions
- Ensure the **ZT** implementation enables an **Active Cyber Defense**
- Simplify the design as much as possible



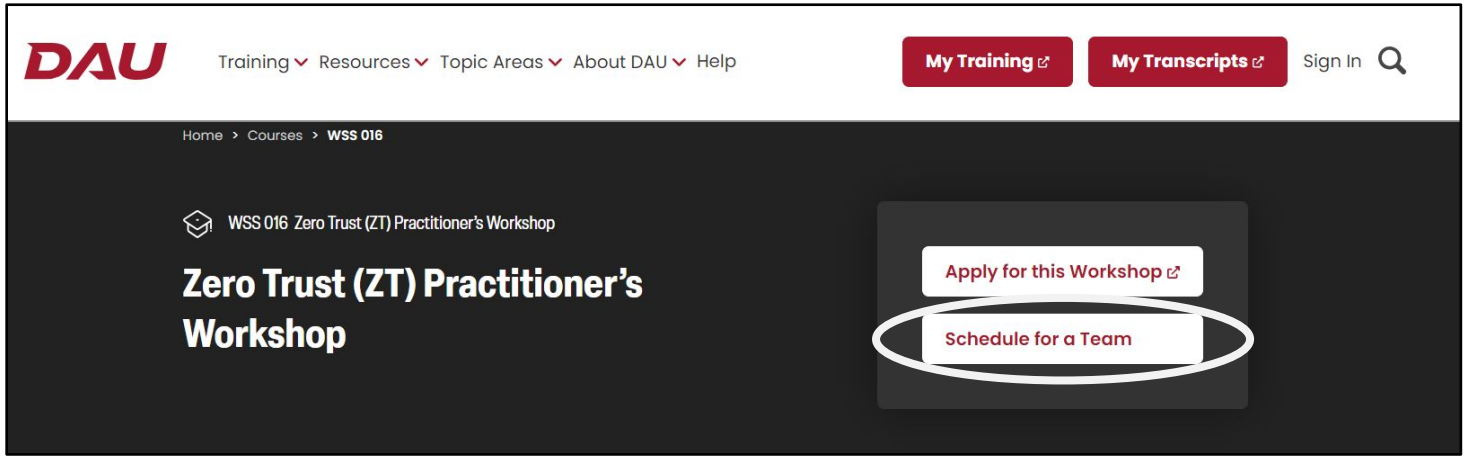
Monitor and Maintain

- Look for opportunities to improve the design



Resources

Zero Trust (ZT) Practitioner's Workshop



- https://www.dau.edu/courses/wss-016
  - The purpose of the workshop is to provide clarity on the Department of Defense (DoD)'s Zero Trust implementation requirements. This strategy supports DoD's overarching efforts toward Digital Modernization. In this workshop, we will review DoD's information technology strategic initiatives, cybersecurity reference architectures, relevant laws, regulations, policies, and standards related to ZT. Participants will exercise their knowledge, skills, and abilities (KSAs) on project management principles, system design analysis, and assessment and reporting methodologies. Participants will assess cybersecurity ZT trade-space and tradeoffs based on the People, Processes, and Technology relating to having adequate security controls, Doctrine, Organization, Training, materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTmLPF-P) and risk management framework (RMF) principles.

Q & A

Zero Trust Securing Naval Warfighting Power



Resources

- International Standards
  - IEEE/ISO/IEC 15288-2023, Systems and software engineering--System life cycle processes
- NIST Standards and Guidebooks
  - NIST 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations
  - NIST 800-137, Information Security Continuous Monitoring
  - NIST 800-162, ABAC
  - NIST 800-207, ZTA
  - NIST 1800-35, Implementing a ZTA
  - NIST Risk Management Framework
- DoD Guidance
  - DoD Manual 8530.01, Cybersecurity Activities Support Procedures
  - DoD Information Security Continuous Monitoring Strategy
  - JFHQ-DODIN Vulnerability Management Branch CONOPS
- DoD CIO Library
  - DoD Zero Trust Strategy
  - DoD Zero Trust Reference Architecture
  - Zero Trust Capabilities and Activities
  - Zero Trust Capability Execution Roadmap
  - Zero Trust Overlays
- DON CIO ZT Program
  - DON ZT Implementation Plan v2.0 (CAC Required)
  - DON ZT Major Design Concept
  - Draft DON ZT Blueprint (CAC Required / Planned release April-2025)

DAY TWO

THURSDAY, APRIL 3RD

John Kindervag

illumio

Integrating Zero Trust Maturity Models

John Kindervag

Chief Evangelist

April 3, 2025



No More Chewy Centers

illumio

For Security & Risk Professionals



September 14, 2010 | Updated: September 17, 2010

No More Chewy Centers: Introducing The Zero Trust Model Of Information Security

by John Kindervag
with Stephanie Balaouras and Lindsey Coit

EXECUTIVE SUMMARY

There's an old saying in information security: "We want our network to be like an M&M, with a hard crunchy outside and a soft chewy center." For a generation of information security professionals, this was the motto we grew up with. It was a motto based on trust and the assumption that malicious individuals wouldn't get past the "hard crunchy outside." In today's new threat landscape, this is no longer an effective way of enforcing security. Once an attacker gets past the shell, he has access to all the resources in our network. We've built strong perimeters, but well-organized cybercriminals have recruited insiders and developed new attack methods that easily pierce our current security protections. To confront these new threats, information security professionals must eliminate the soft chewy center by making security ubiquitous throughout the network, not just at the perimeter. To help security professionals do this effectively, Forrester has developed a new model for information security, called Zero Trust. This report, the first in a series, will introduce the necessity and key concepts of the Zero Trust Model.

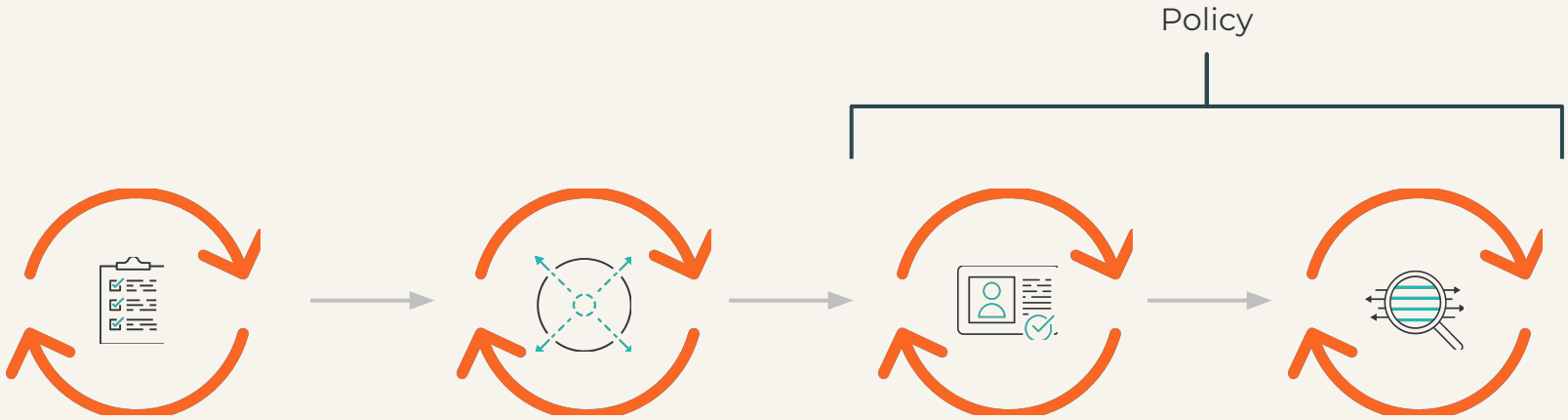
https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf

ZERO TRUST

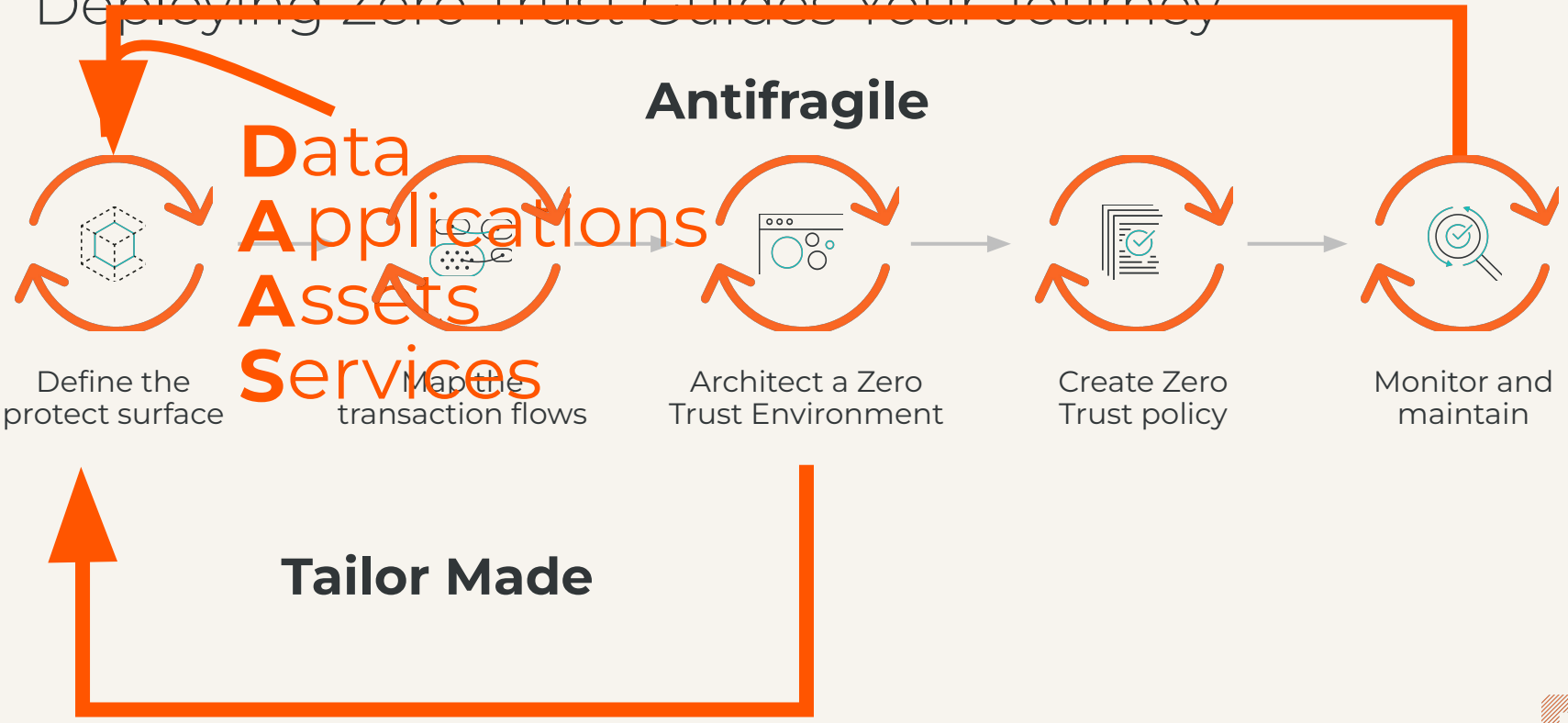


A strategy designed to stop data breaches and prevent other cyber-attacks from being successful by eliminating trust from digital systems.

Zero Trust Design Concepts

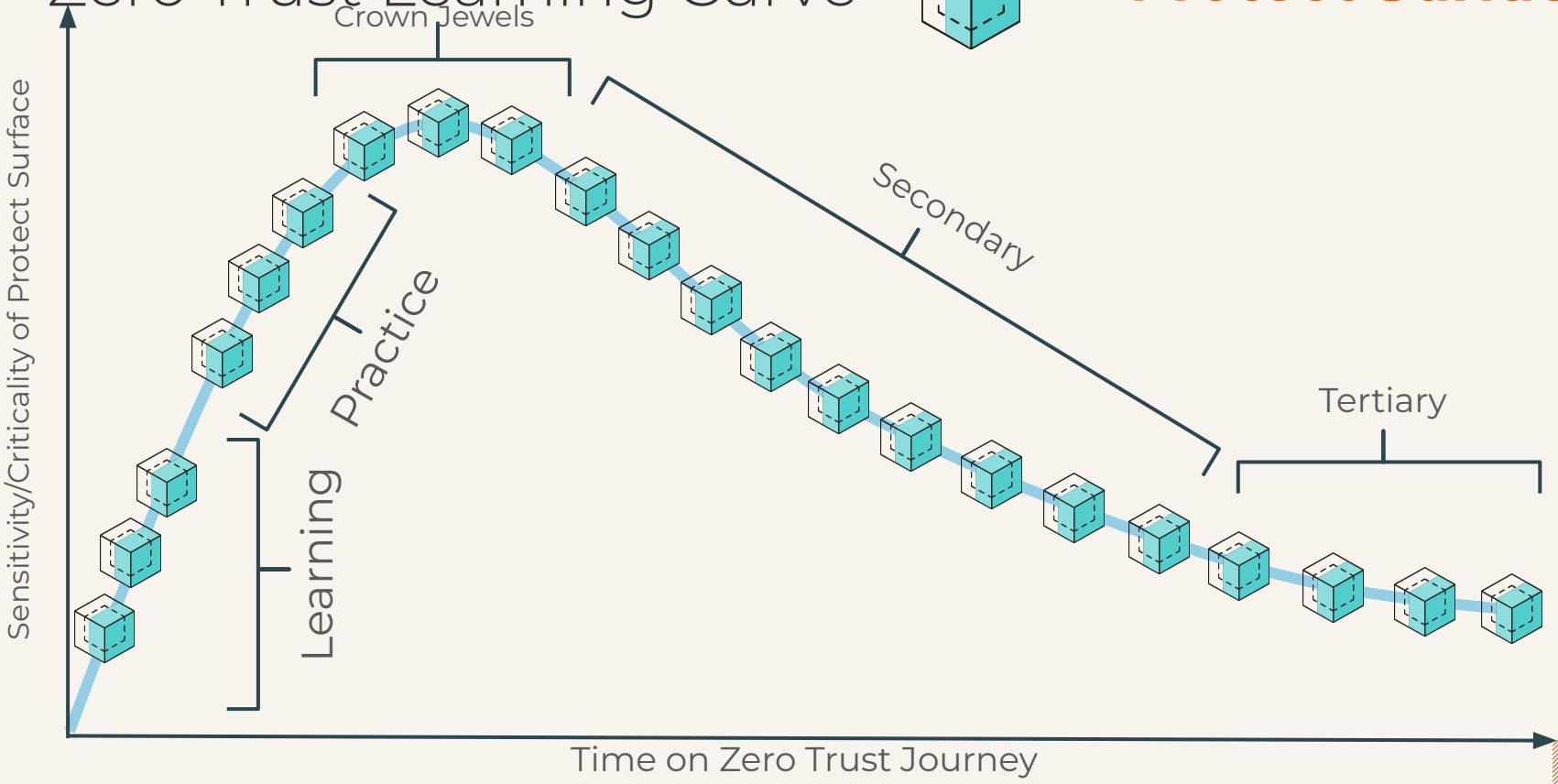


The 5-Step Methodology for Deploying Zero Trust Guides Your Journey

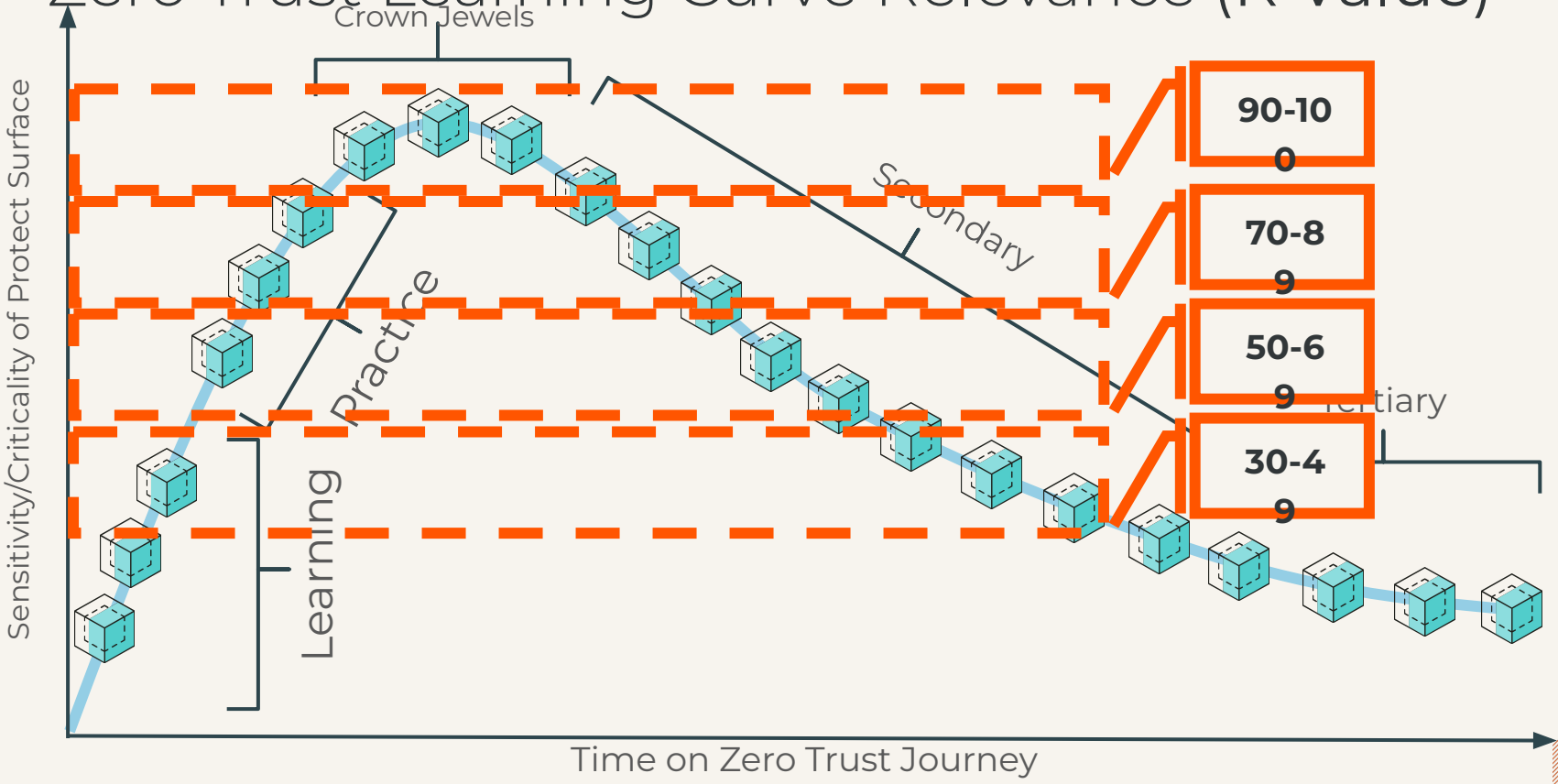


Zero Trust Learning Curve

= **Protect Surface**



Zero Trust Learning Curve Relevance (R Value)



illumio

Zero Trust Maturity Model History



FORRESTER®

FOR SECURITY & RISK PROFESSIONALS

Assess Your Network Security Architecture With Forrester's Zero Trust Maturity Model

Assessment: The Security Architecture And Operations Playbook

by Stephanie Balaouras, Peter Cerrato, and John Kindervag

March 8, 2017

Why Read This Report

As the number of breached records continues to climb, more than ever, security and risk (S&R) pros need to take steps to overhaul their business' traditional infrastructure and invest in Zero Trust practices and technologies. As threat actors continue to rapidly improve their capabilities in 2017, adherence to outdated security practices will only hurt your business and your customers. This report provides a framework with which to evaluate your network security architecture against the Zero Trust principles that matter most.

Key Takeaways

Use Zero Trust To Prevent Devastating Cyberattacks

In a Zero Trust network model, security teams are never blindsided by malicious insiders or stealth attackers because the model demands continuous monitoring for suspicious activity and guarding the firm's most sensitive data in highly secure microperimeters.

Measure Your Zero Trust Maturity In Five Steps

Forrester has defined five steps common to achieving Zero Trust in every network. Thus, our Zero Trust Maturity Model aligns with these steps. The goal of Zero Trust is to greatly enhance security effectiveness without adding unnecessary complexity, and we designed our model the same way. It's simple to both follow and understand.

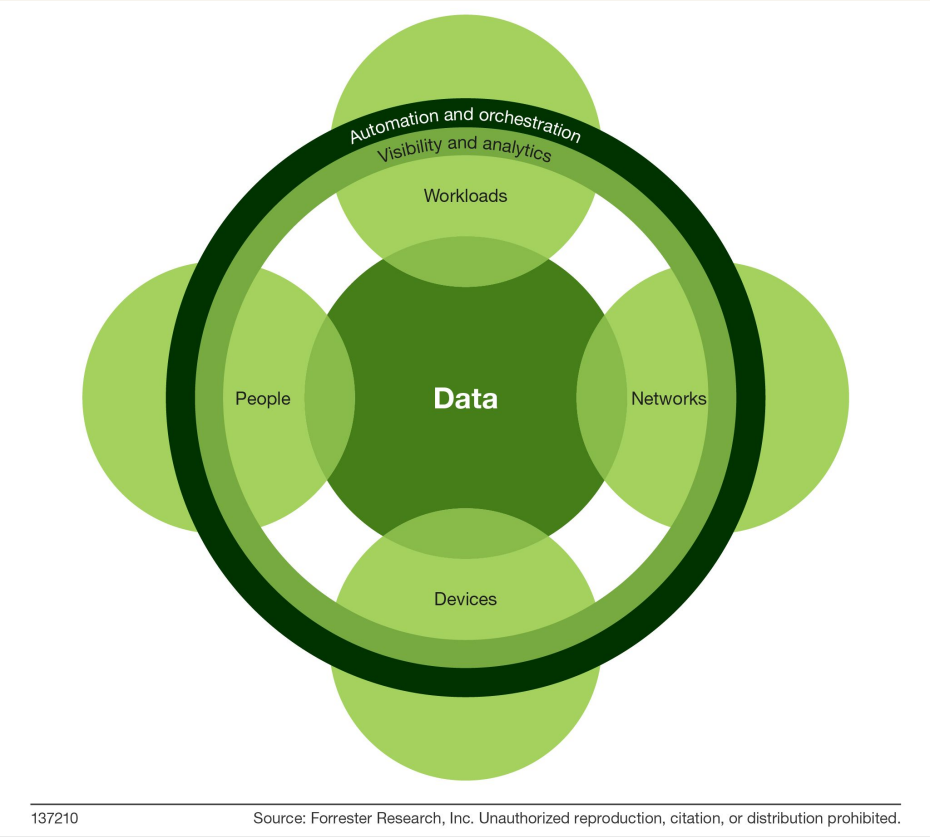
illumio

Zero Trust Maturity Model

DAAS Element Protect Surface	Initial	Repeatable	Defined	Managed	Optimized
 1. Define your Protect Surface	1	2	3	4	5
 2. Map the Transaction Flows	1	2	3	4	5
 3. Architect a Zero Trust Environment	1	2	3	4	5
 4. Create Zero Trust Policy	1	2	3	4	5
 5. Monitor and Maintain the Network	1	2	3	4	5

Total Score

Forrester's ZTX Framework



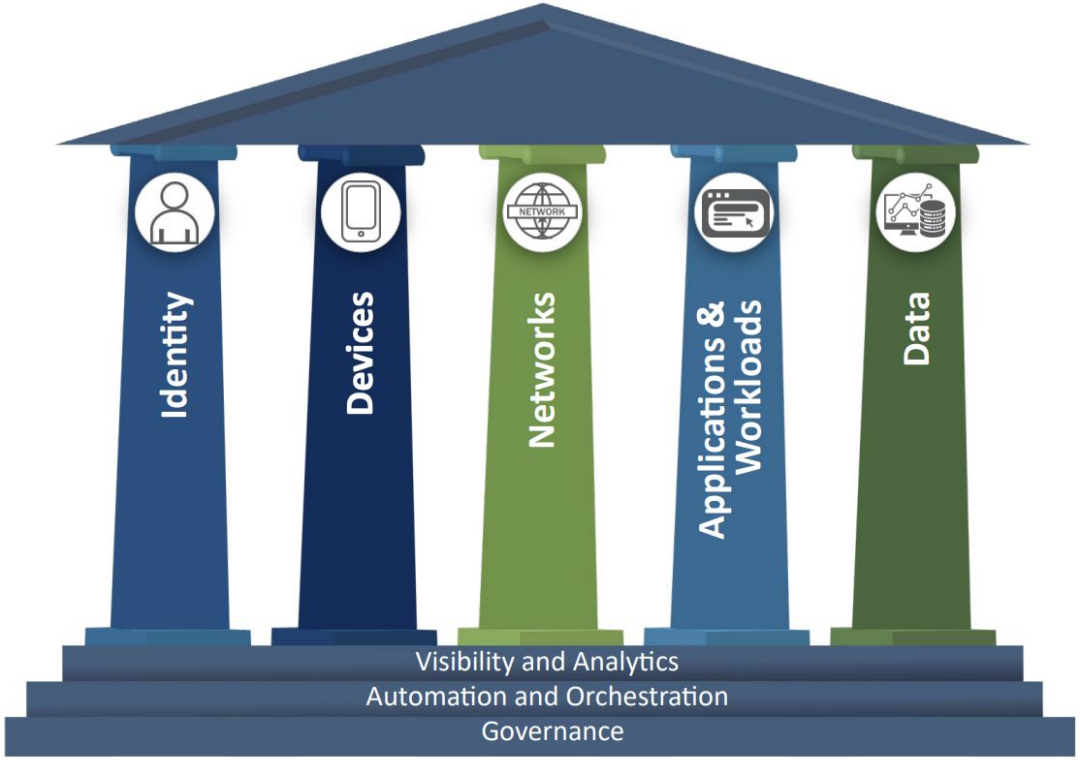
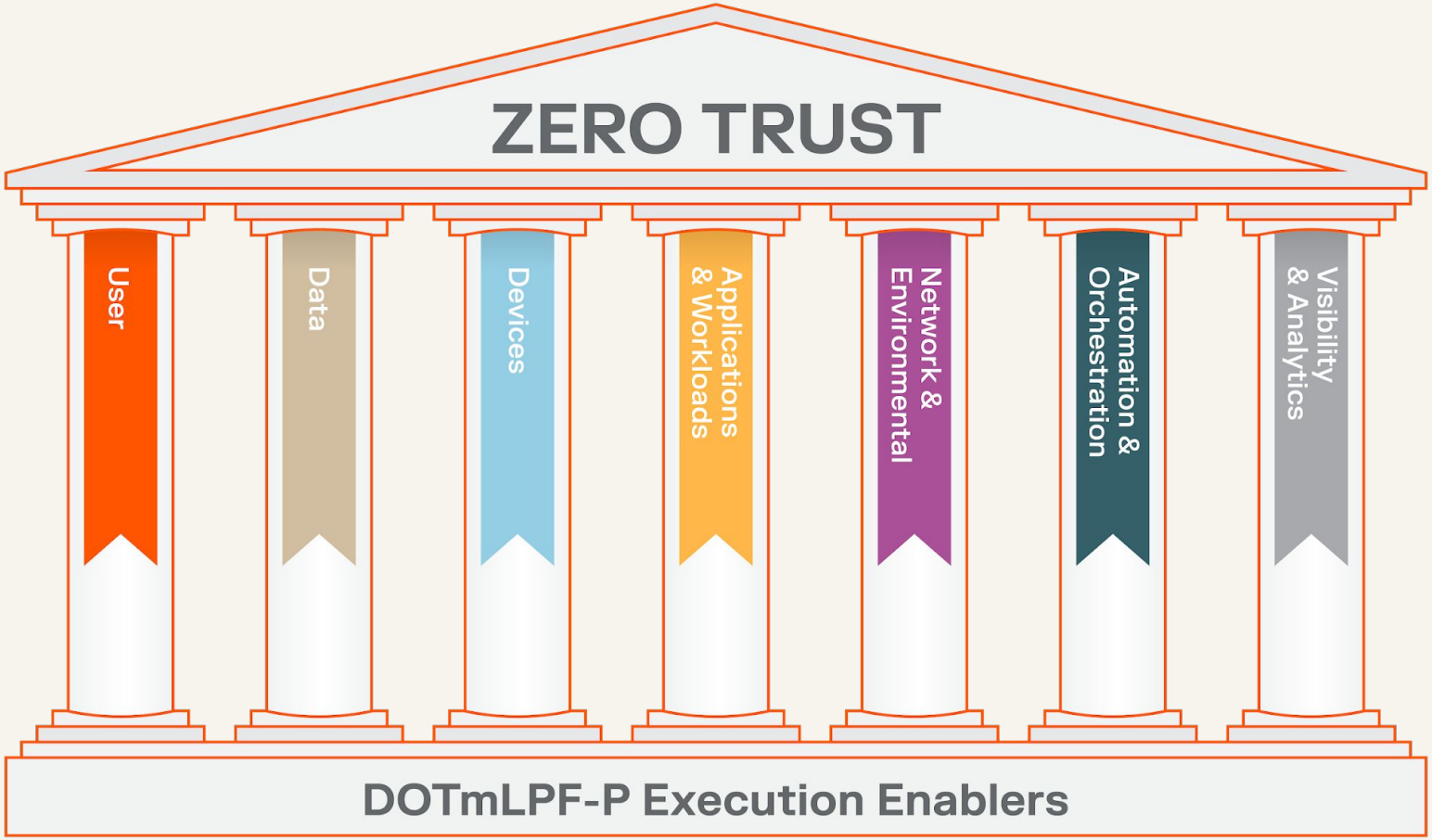


Figure 1: Zero Trust Maturity Model Pillars[8]

CISA's ZTMM is one of many paths to support the transition to zero trust.


ZERO TRUST
User
Data
Devices
Applications & Workloads
Network & Environmental
Automation & Orchestration
Visibility & Analytics
DOTmLPF-P Execution Enablers

Looking Through Different Lenses

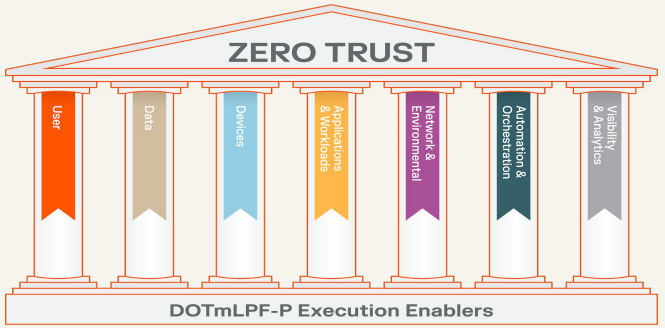
Protect Surface Focused

Zero Trust Maturity Model

DAAS Element / Protect Surface	Initial	Repeatable	Defined	Managed	Optimized
1. Define your Protect Surface	1	2	3	4	5
2. Map the Transaction Flows	1	2	3	4	5
3. Architect a Zero Trust Environment	1	2	3	4	5
4. Create Zero Trust Policy	1	2	3	4	5
5. Monitor and Maintain the Network	1	2	3	4	5
Total Score					

VS

Product Focused



Zero Trust Maturity Model

DAAS Element Protect Surface	Initial	Repeatable	Defined	Managed	Optimized
 1. Define your Protect Surface	1	2	3	4	5
 2. Map the Transaction Flows	1	2	3	4	5
 3. Architect a Zero Trust Environment	1	2	3	4	5
 4. Create Zero Trust Policy	1	2	3	4	5
 5. Monitor and Maintain the Network	1	2	3	4	5

Total Score

The 5-Steps: Step 1 – Define The Protect Surface

Step	Activities	Quantifiable Progress Metric	Scale
1. Define the Protect Surface	Identify DAAS elements to protect (i.e., the protect surface).	Organizational inventory of total DAAS elements (protect surfaces) on the organizational roadmap for future Zero Trust deployments	5 = Complete across all devices, locations, and hosting models 3 = Spotty; we have inventories and classified DAAS in some locations 1 = We are planning a DAAS discovery and inventory project. 0 = None or don't know

Adapted from "The NSTAC Report to the President: Zero Trust and Trusted Identity Management February 23, 2022.

Zero Trust Maturity Model

DAAS Element Protect Surface	Initial	Repeatable	Defined	Managed	Optimized
 1. Define your Protect Surface	1	2	3	4	5
 2. Map the Transaction Flows	1	2	3	4	5
 3. Architect a Zero Trust Environment	1	2	3	4	5
 4. Create Zero Trust Policy	1	2	3	4	5
 5. Monitor and Maintain the Network	1	2	3	4	5

PCI CDE

LUHN FORMULA

Total Score

The 5-Steps: Step 2 – Map the Transaction Flows

Step	Activities	Quantifiable Progress Metric	Scale
2. Map the Transaction Flows	Understand how the networks work by mapping the transaction flows to and from the protect surface, including how various DAAS components interact with other resources on the network. These transaction flows directly inform where to place proper controls.	Percentage of instrumented and validated traffic flows (as a function of total traffic flows)	5 = We continuously map all of our transaction flows using an automated tool 3 = Spotty; We have mapped many of our transaction flows, whether manually or via a tool 1 = We have manually mapped some of our transaction flows 0 = We do not have our transaction flows mapped

Adapted from “The NSTAC Report to the President: Zero Trust and Trusted Identity Management February 23, 2022.

Zero Trust Maturity Model

DAAS Element Protect Surface	Initial	Repeatable	Defined	Managed	Optimized
1. Define your Protect Surface	1	2	3	4	5
2. Map the Transaction Flows	1	2	3	4	5
3. Architect a Zero Trust Environment	1	2	3	4	5
4. Create Zero Trust Policy	1	2	3	4	5
5. Monitor and Maintain the Network	1	2	3	4	5

PCI CDE

LUHN FORMULA

Total Score

The 5-Steps: Step 3 – Architect a Zero Trust

Step	Activities	Quantifiable Progress Metric	Scale
3. Architect a Zero Trust Environment	Design your Zero fTrust architecture, tailored to the Protect Surface(s) determined in steps 1 and 2. The way traffic moves across the network specific to the data in the Protect Surface should determine the design. The architectural elements cannot be predetermined, though a good rule of thumb is to place the controls as close as possible to the Protect Surface.	Percentage of DAAS elements (as a function of the total) that an enforcement point protects	5 = We have a Zero Trust environment with embedded security that segments DAAS elements and controls access appropriately 3 = We have some network segmentation, mainly drive by PCI or some other compliance objective 1 = We plan to refresh our controls as new projects such as cloud deployemnts require; we are considering segmentation. 0 = We have a legacy, hierarchical network. There is no segmentation at Layer 3 or above.

Adapted from “The NSTAC Report to the President: Zero Trust and Trusted Identity Management February 23, 2022.

Zero Trust Maturity Model

DAAS Element Protect Surface	Initial	Repeatable	Defined	Managed	Optimized
1. Define your Protect Surface	1	2	3	4	5
2. Map the Transaction Flows	1	2	3	4	5
3. Architect a Zero Trust Environment	1	2	3	4	5
4. Create Zero Trust Policy	1	2	3	4	5
5. Monitor and Maintain the Network	1	2	3	4	5

PCI CDE

LUHN FORMULA

Total Score

The 5-Steps: Step 4 – Create a Zero Trust Policy

Step	Activities	Quantifiable Progress Metric	Scale
4. Create a Zero Trust policy	Instantiate Zero Trust using the Kipling Method of Zero Trust policy writing to determine who or what can access your Protect Surface. Consider both person and non-person entities.	Percentage of DAAS elements (as a function of the total) that a defined zero trust policy protects	= We have implemented Kipling Method policies across all Protect Surfaces to protect our DAAS elements appropriately 3 = We have implemented Kipling Method policies for some Protect Surfaces, mainly driven by PCI or some other compliance objective 1 = We use traditional firewall rules to control access to our legacy perimeter-based network. 0 = We have a trusted internal network where domain users have access to most network resources

Adapted from “The NSTAC Report to the President: Zero Trust and Trusted Identity Management February 23, 2022.

Zero Trust Maturity Model

DAAS Element
Protect Surface

PCI CDE

	Initial	Repeatable	Defined	Managed	Optimized
1. Define your Protect Surface **LUHN FORMULA**	1	2	3	4	5
2. Map the Transaction Flows	1	2	3	4	5
3. Architect a Zero Trust Environment	1	2	3	4	5
4. Create Zero Trust Policy **Req. 1.1.7 FW Auditing**	1	2	3	4	5
5. Monitor and Maintain the Network	1	2	3	4	5

Total Score

The 5-Steps: Step 5 – Monitor and Maintain

Step	Activities	Quantifiable Progress Metric	Scale
5. Monitor and Maintain the Environment	Inspect and log all traffic. The telemetry from this process helps prevent significant cybersecurity events and provides valuable security improvement insights over the longterm. As a result, each subsequent protect surface can become more robust and better protected over time	Month-over-month true and false positive percentages for security incidents for zero trust deployments (to quantify efficacy and provide a closed feedback loop for zero trust technology and policy refinement)	5 = We have flow validation and Security analytics across all Protect Surfaces. 3 = We have some flow validation and Security Analytics, but they are limited and do not encompass all Protect Surfaces 1 = We have basic logging capabilities but lack full-flow validation or advanced Security Analytics. 0 = None or don't know

Adapted from "The NSTAC Report to the President: Zero Trust and Trusted Identity Management February 23, 2022.

Zero Trust Maturity Model

DAAS Element Protect Surface	Initial	Repeatable	Defined	Managed	Optimized
1. Define your Protect Surface	1	2	3	4	5
2. Map the Transaction Flows	1	2	3	4	5
3. Architect a Zero Trust Environment	1	2	3	4	5
4. Create Zero Trust Policy	1	2	3	4	5
5. Monitor and Maintain the Network	1	2	3	4	5
Total Score					12 / 20 > 180

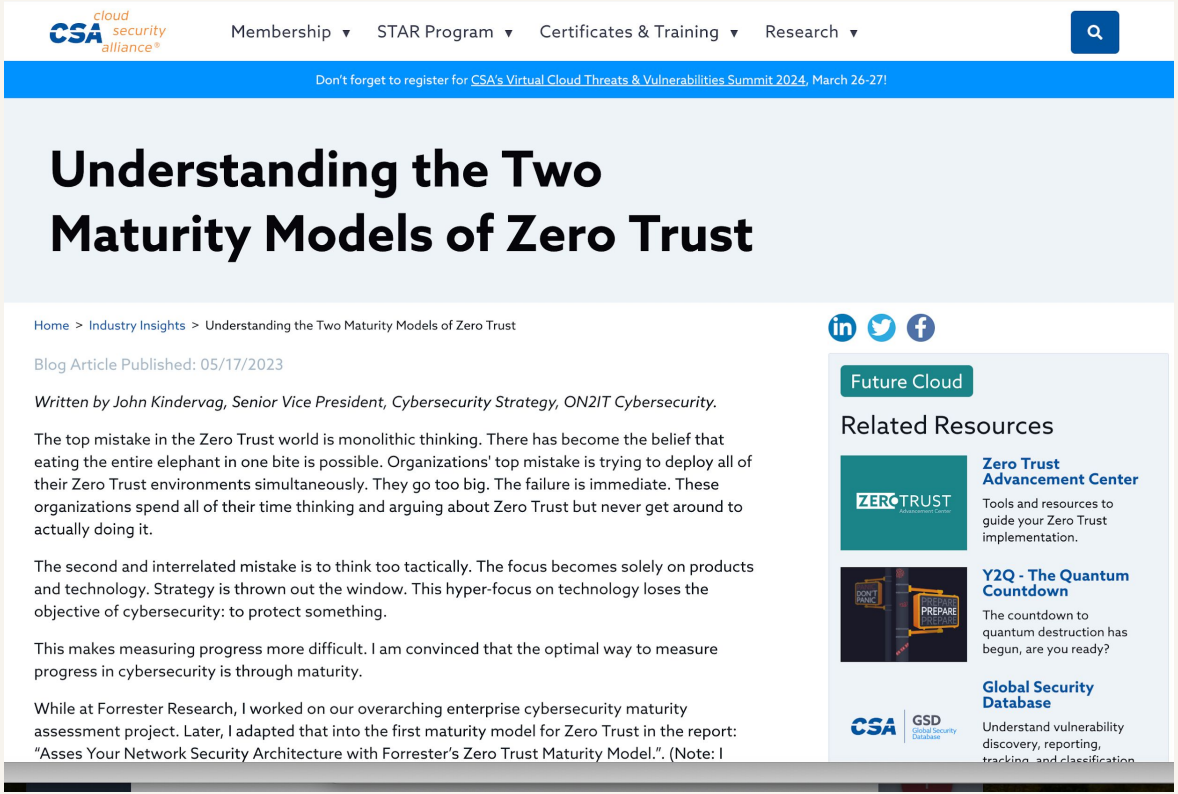
PCI CDE

LUHN FORMULA

Req. 1.1.7 FW Auditing

Req. 10 Logging

CSA Article



cloud security alliance®

Membership ▾ STAR Program ▾ Certificates & Training ▾ Research ▾

Don't forget to register for CSA's Virtual Cloud Threats & Vulnerabilities Summit 2024, March 26-27!

Understanding the Two Maturity Models of Zero Trust

Home > Industry Insights > Understanding the Two Maturity Models of Zero Trust

Blog Article Published: 05/17/2023

Written by John Kindervag, Senior Vice President, Cybersecurity Strategy, ON2IT Cybersecurity.

The top mistake in the Zero Trust world is monolithic thinking. There has become the belief that eating the entire elephant in one bite is possible. Organizations' top mistake is trying to deploy all of their Zero Trust environments simultaneously. They go too big. The failure is immediate. These organizations spend all of their time thinking and arguing about Zero Trust but never get around to actually doing it.

The second and interrelated mistake is to think too tactically. The focus becomes solely on products and technology. Strategy is thrown out the window. This hyper-focus on technology loses the objective of cybersecurity: to protect something.

This makes measuring progress more difficult. I am convinced that the optimal way to measure progress in cybersecurity is through maturity.

While at Forrester Research, I worked on our overarching enterprise cybersecurity maturity assessment project. Later, I adapted that into the first maturity model for Zero Trust in the report: "Asses Your Network Security Architecture with Forrester's Zero Trust Maturity Model.". (Note: I

Future Cloud

Related Resources

ZERO TRUST Advancement Center

Zero Trust Advancement Center

Tools and resources to guide your Zero Trust implementation.

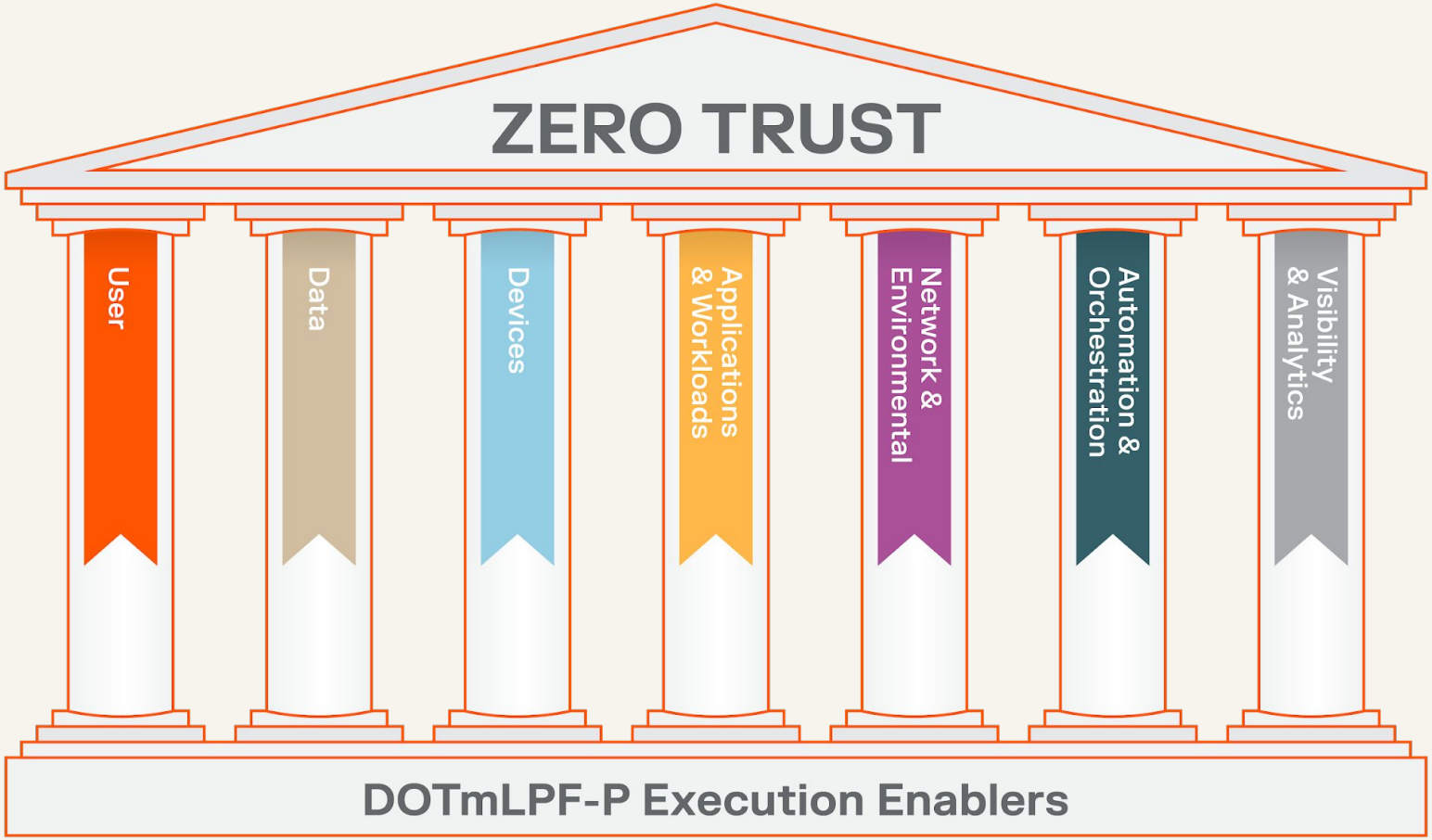
Y2Q - The Quantum Countdown

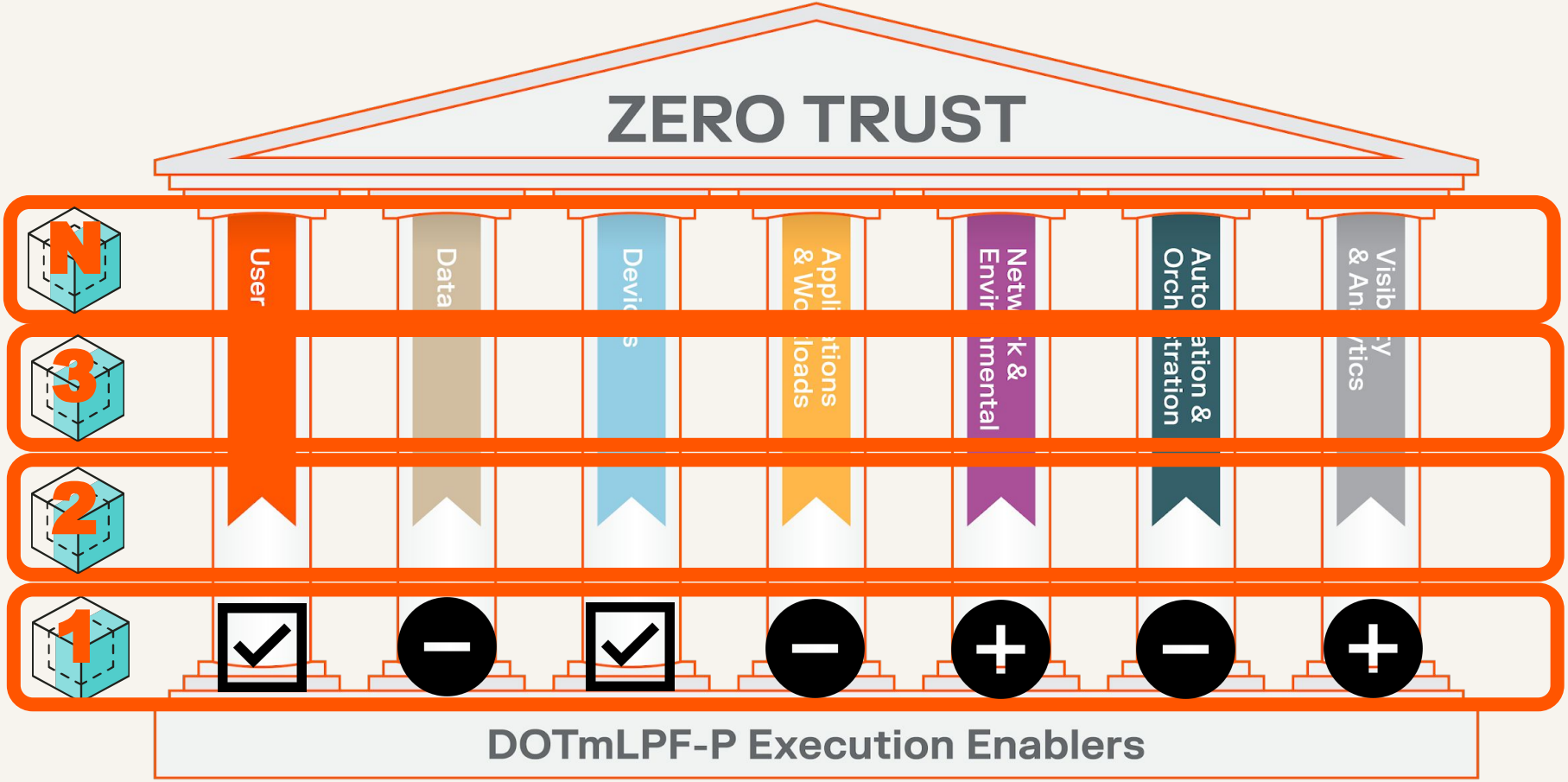
The countdown to quantum destruction has begun, are you ready?

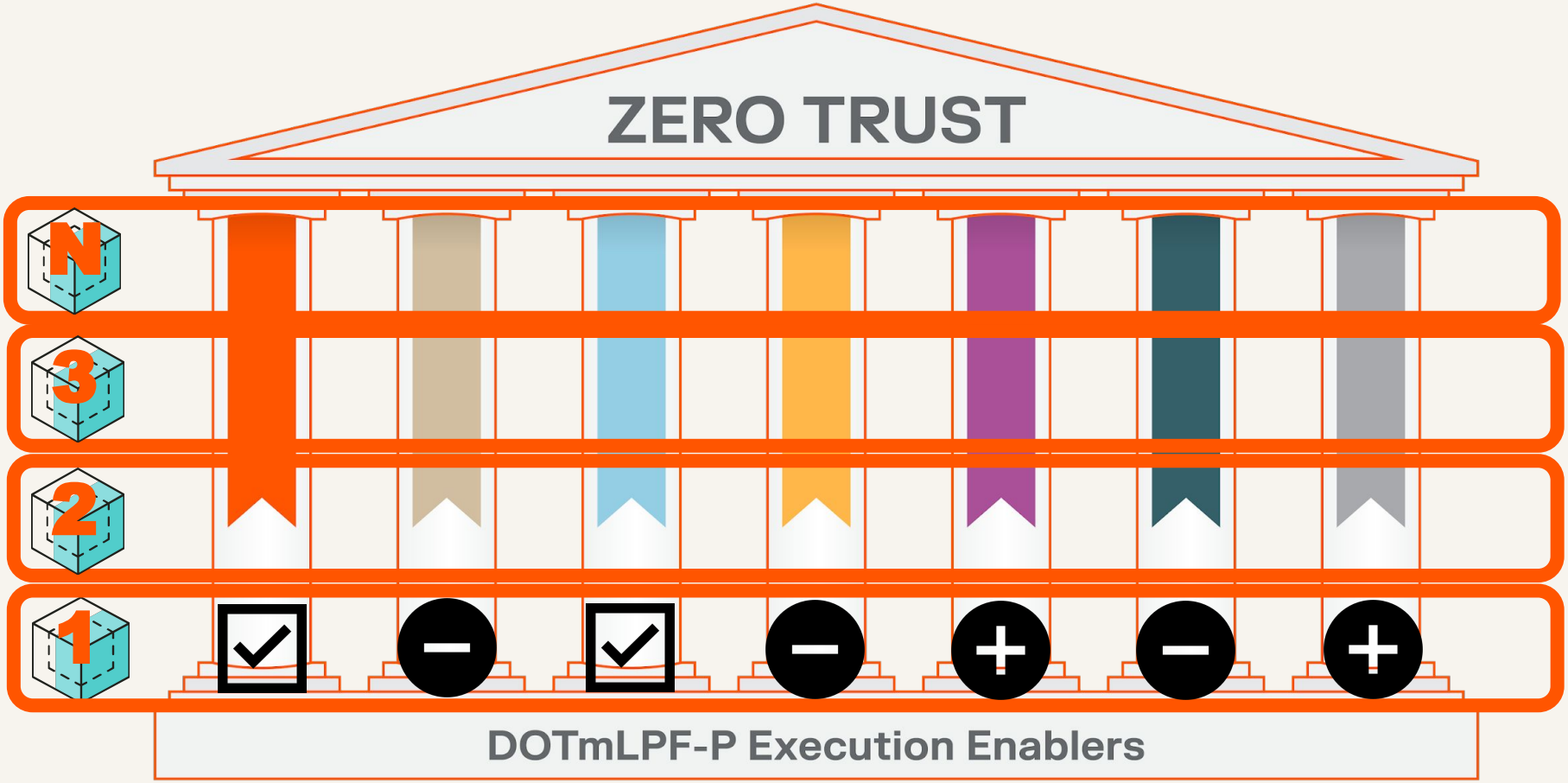
CSA GSD Global Security Database

Global Security Database

Understand vulnerability discovery, reporting, tracking, and classification


ZERO TRUST
User
Data
Devices
Applications & Workloads
Network & Environmental
Automation & Orchestration
Visibility & Analytics
DOTmLPF-P Execution Enablers


ZERO TRUST
N
3
2
1
User
Data
Devi s
Appli tions & Wo loads
Netw k & Envir mental
Auto ation & Orch tration
Visib y & An tics
DOTmLPF-P Execution Enablers


ZERO TRUST
N
3
2
1
DOTmLPF-P Execution Enablers

illumio

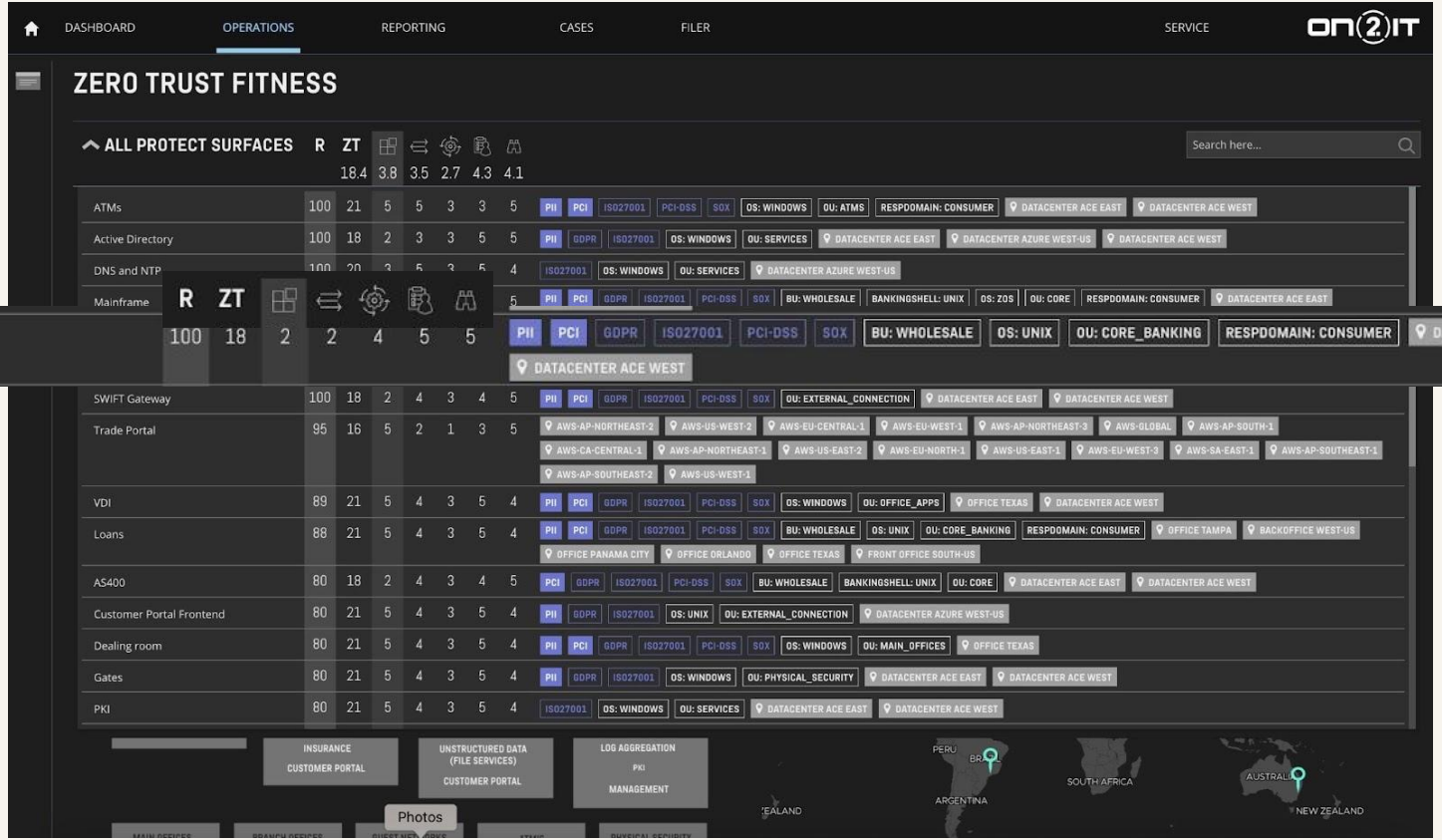
Maturity Models in Action



Aggregate Scoring



Per Protect Surface Scoring



Implementation Drill Down



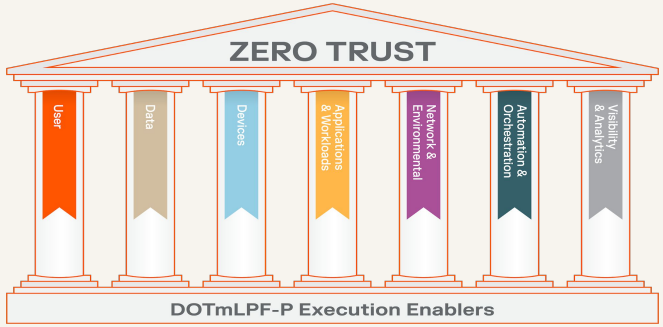
Use Multiple POVs

Protect Surface Focused

Zero Trust Maturity Model

DAAS Element / Protect Surface	Initial	Repeatable	Defined	Managed	Optimized
1. Define your Protect Surface	1	2	3	4	5
2. Map the Transaction Flows	1	2	3	4	5
3. Architect a Zero Trust Environment	1	2	3	4	5
4. Create Zero Trust Policy	1	2	3	4	5
5. Monitor and Maintain the Network	1	2	3	4	5
Total Score					

Product Focused





Thank You

John Kindervag

Chief Evangelist

Sean Connelly

Zero Trust Maturity across Governments

Sean Connelly

2025 Zscaler, Inc. All rights reserved

Sean Connelly's Background

- 11 years at CISA (and former NPPD) / 20+ years in federal IT
- 15 years helping lead OMB's TIC Initiative
- Co-led CISA's participation in the Five-Eyes Emerging Tech Working Group
- Co-author of:
  - NIST SP 800-207 - Zero Trust Architecture
  - CISA's Zero Trust Maturity Model
  - Many other federal IT guidance documents



The Basics: Zero Trust

- **Definition**: An evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. (NIST SP 800-207 on ZTA)

in other words…

Zero Trust is not about building higher walls – it's about designing smarter defenses

Traditional Network Security

- Perimeter focused
- Independent & siloed controls

Zero Trust Security

- Data-centric focus
- Layered & integrated controls

Sean Connelly

2025 Zscaler, Inc. All rights reserved

Federal Zero Trust Efforts



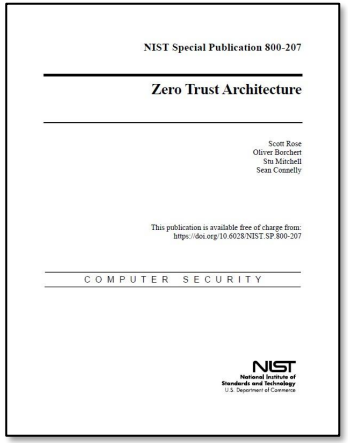
Zero Trust Documents across USG:

- NIST SP 800-207
- Cyber Executive Order 14028
- DOD Zero Trust Strategy
- GSA Zero Trust Buyer's Guide
- CISA Zero Trust Maturity Model
- NSA Embracing Zero Trust
- GSA EIS ZT Architecture
- NIST Planning for ZTA
- NIST SP 1800-35 Implementing ZTA
- *Many* agency specific ZTA documents

Sean Connelly

2025 Zscaler, Inc. All rights reserved

Federal Civilian Zero Trust Landscape


NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

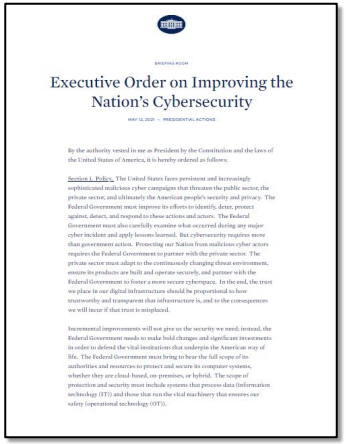
This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

The Principles

[NIST SP 800-207 Zero Trust Architecture]


Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

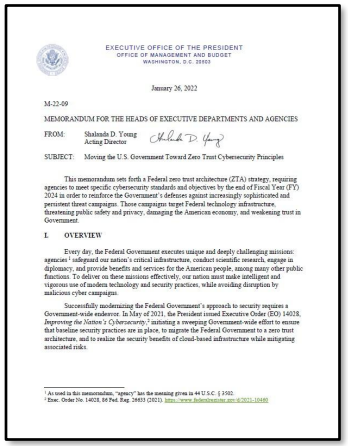
By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life. The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid. The scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)).

The Imperative

[EO 14028 Improving the Nation's Cybersecurity]


EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

January 26, 2022

M-22-09

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director

SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

This memorandum sets forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns. These campaigns target Federal technology infrastructure, threatening public safety and privacy, damaging the American economy, and weakening trust in Government.

I. OVERVIEW

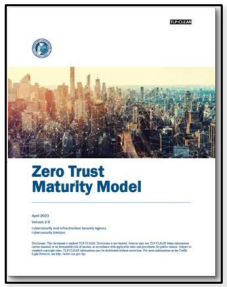
Every day, the Federal Government executes unique and deeply challenging missions: agencies[1] safeguard our nation's critical infrastructure, conduct scientific research, engage in diplomacy, and provide benefits and services for the American people, among many other public functions. To deliver on these missions effectively, our nation must make intelligent and vigorous use of modern technology and security practices, while avoiding disruption by malicious cyber campaigns.

Successfully modernizing the Federal Government's approach to security requires a Government-wide endeavor. In May of 2021, the President issued Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*,[2] initiating a sweeping Government-wide effort to ensure that baseline security practices are in place, to migrate the Federal Government to a zero trust architecture, and to realize the security benefits of cloud-based infrastructure while mitigating associated risks.

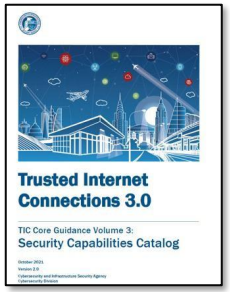
[1] As used in this memorandum, "agency" has the meaning given in 44 U.S.C. § 3502.
[2] Exec. Order No. 14028, 86 Fed. Reg. 26633 (2021). https://www.federalregister.gov/d/2021-10460

The Strategy

[OMB M-22-09 Zero Trust Strategy]


Zero Trust Maturity Model

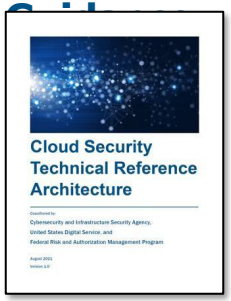
[CISA Zero Trust Maturity Model]


Trusted Internet Connections 3.0

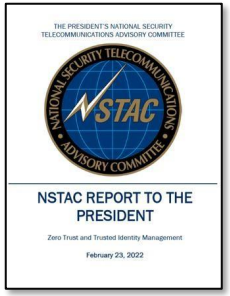
TIC Core Guidance Volume 3:
Security Capabilities Catalog

[TIC Catalog]

The Operational


Cloud Security Technical Reference Architecture

[Federal Cloud Security TRA]


THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

NSTAC REPORT TO THE PRESIDENT

Zero Trust and Trusted Identity Management

February 23, 2022

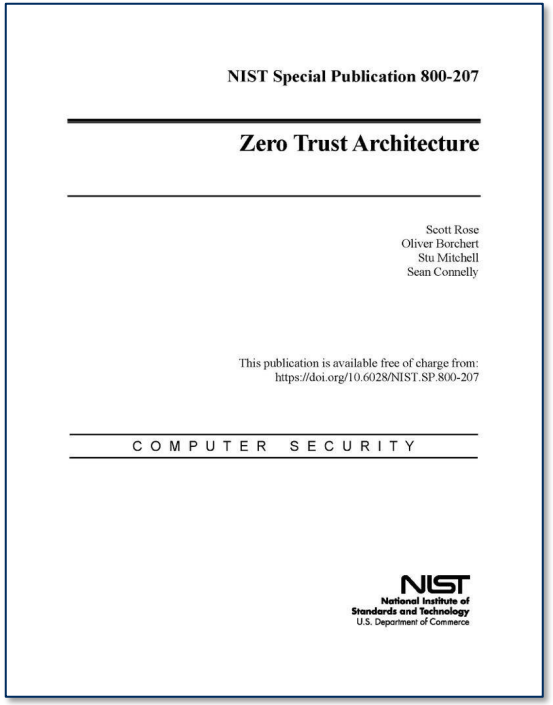
[NSTAC Report]

NIST SP 800-207 Zero Trust Architecture

Seven Tenets of Zero Trust

1) All data sources & computing services are considered resources.
2) All communication is secured regardless of network location.
3) Access to individual enterprise resources is granted on a per-session basis.
4) Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
5) The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6) All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7) The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

- "Zero Trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised."
- "Zero Trust Architecture is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning,


NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

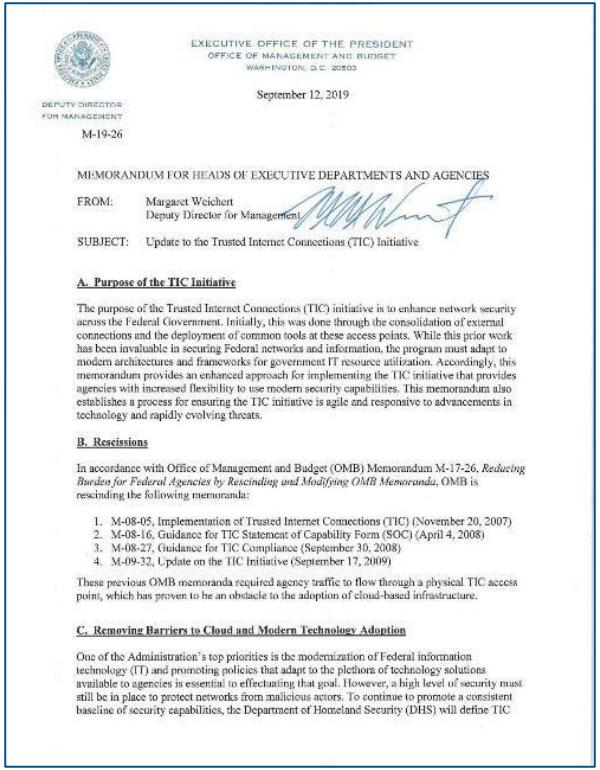
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Sean Connelly

2025 Zscaler, Inc. All rights reserved

OMB Memorandum M-19-26 – TIC 3

- Trusted Internet Connections (TIC) – first initiative started in 2008
- Latest updates began in September 2019
- Tasks CISA with modernizing the Federal agencies connect to the Internet
- Multiple Uses Cases released (latest in 2023)
- Same agencies & teams that led Zero Trust
- Focus is towards:
  - New Network Strategies
  - Flexible Architecture
  - Better Visibility



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

DEPUTY DIRECTOR FOR MANAGEMENT

September 12, 2019

M-19-26

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Margaret Weichert
Deputy Director for Management

SUBJECT: Update to the Trusted Internet Connections (TIC) Initiative

A. Purpose of the TIC Initiative

The purpose of the Trusted Internet Connections (TIC) initiative is to enhance network security across the Federal Government. Initially, this was done through the consolidation of external connections and the deployment of common tools at these access points. While this prior work has been invaluable in securing Federal networks and information, the program must adapt to modern architectures and frameworks for government IT resource utilization. Accordingly, this memorandum provides an enhanced approach for implementing the TIC initiative that provides agencies with increased flexibility to use modern security capabilities. This memorandum also establishes a process for ensuring the TIC initiative is agile and responsive to advancements in technology and rapidly evolving threats.

B. Rescissions

In accordance with Office of Management and Budget (OMB) Memorandum M-17-26, *Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda*, OMB is rescinding the following memoranda:

1. M-08-05, Implementation of Trusted Internet Connections (TIC) (November 20, 2007)
2. M-08-16, Guidance for TIC Statement of Capability Form (SOC) (April 4, 2008)
3. M-08-27, Guidance for TIC Compliance (September 30, 2008)
4. M-09-32, Update on the TIC Initiative (September 17, 2009)

These previous OMB memoranda required agency traffic to flow through a physical TIC access point, which has proven to be an obstacle to the adoption of cloud-based infrastructure.

C. Removing Barriers to Cloud and Modern Technology Adoption

One of the Administration's top priorities is the modernization of Federal information technology (IT) and promoting policies that adapt to the plethora of technology solutions available to agencies is essential to effectuating that goal. However, a high level of security must still be in place to protect networks from malicious actors. To continue to promote a consistent baseline of security capabilities, the Department of Homeland Security (DHS) will define TIC

2025 Zscaler, Inc. All rights reserved

Three Prong Approach to Foster Zero Trust Adoption Across USG

Policy

- Cyber Executive Order 14028
- OMB M-22-09
- NSTAC Report to the President on Zero Trust Technical
- NIST 800-207 on Zero Trust Architecture
- DOD Zero Trust Strategy
- CISA Zero Trust Maturity Model
- Trusted Internet Connections Initiative Funding
- Budgetary deep-dives on a per-agency basis
- Technology Modernization Fund
- GSA Zero Trust Buyer's Guide
- Various lab/demo environments

These examples are only **some** of the ways to foster Zero Trust adoption

Sean Connelly

2025 Zscaler, Inc. All rights reserved

Maturation of Zero Trust Architectures

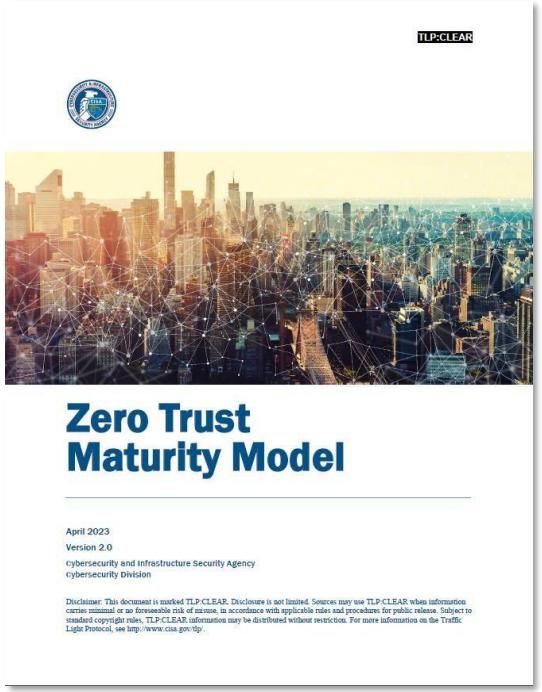
At Federal Civilian agencies

Sean Connelly

2025 Zscaler, Inc. All rights reserved

CISA's Zero Trust Maturity Model

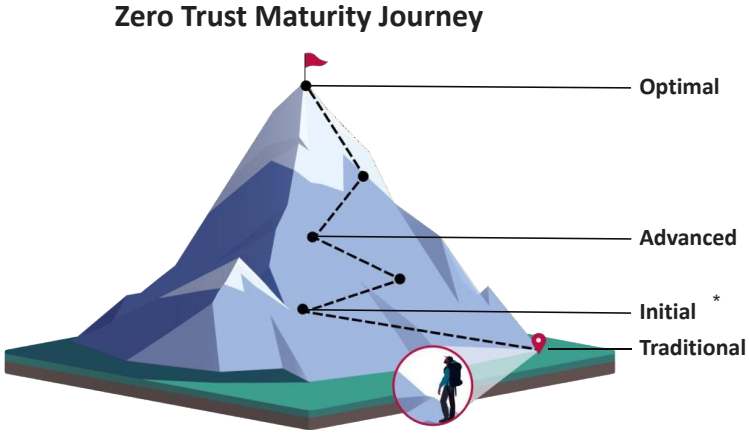
- Civilian agencies align their Zero Trust maturation with CISA's Zero Trust Maturity Model
- Version 2.0 was released in April 2023
- **Intent:** Help agencies as they develop plans to implement Zero Trust Architectures (ZTA) in response to EO14028 Sec 3,b,ii (May 2021)
- **OMB's M-22-09** (January 2022) requires agencies to achieve specific zero trust security goals that are organized using the ZTMM



2025 Zscaler, Inc. All rights reserved

Zero Trust Maturity Journey

- Each stage on the Zero Trust Maturity Journey requires greater levels of protection, detail, and complexity for adoption, with exponential growth in efforts and benefits.
  - **Traditional:** Manual configuration, response, and mitigation; static and siloed policies and solutions
  - **Initial*:** Starting automation; initial cross-pillar solutions; some responsive changes to least privilege; aggregated visibility for internal systems
  - **Advanced:** Automated controls where applicable; cross-pillar policy enforcement; least-privilege changes based on risk/posture; response to pre-defined mitigations
  - **Optimal:** Fully automated, just-in-time, self-reporting; dynamic least privilege access; cross-pillar interoperability with continuous monitoring,



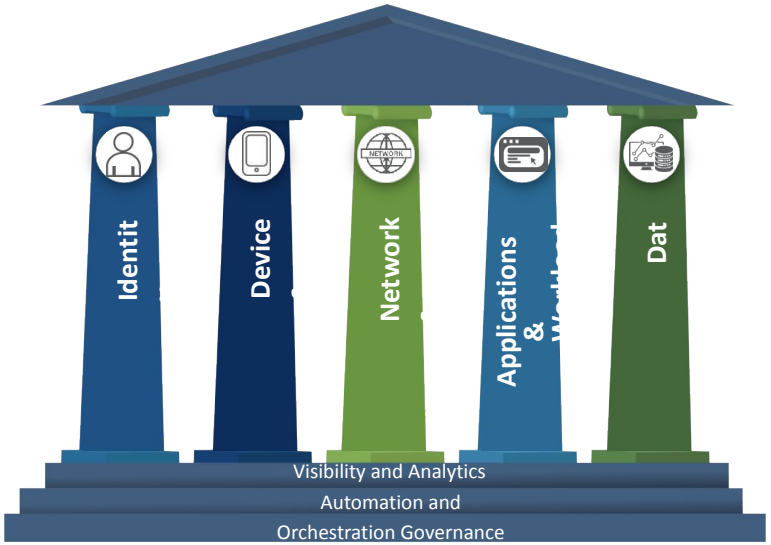
*New with ZTMM V2

Sean Connelly

2025 Zscaler, Inc. All rights reserved

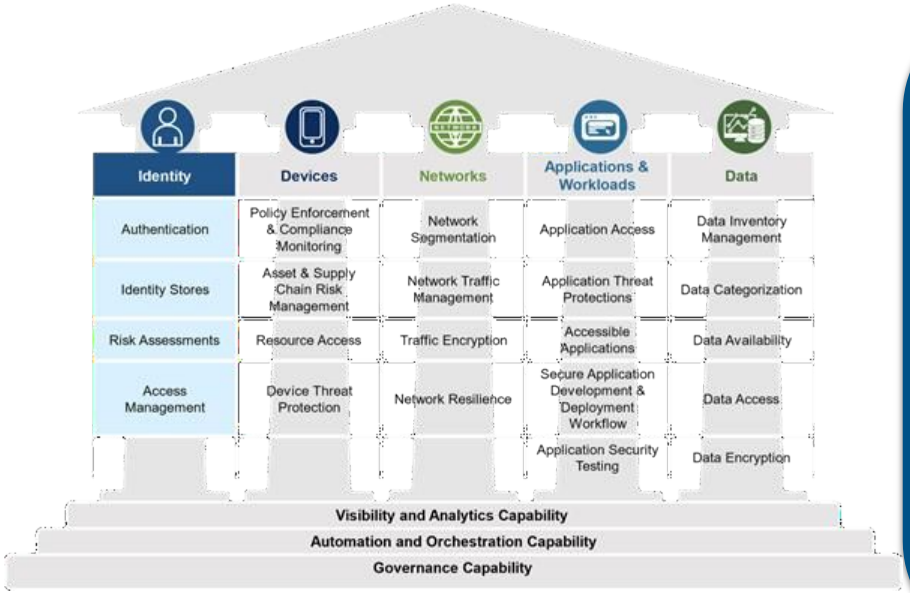
Zero Trust Maturity Model Overview

- The ZTMM represents a gradient of implementation across five distinct pillars and three cross-cutting capabilities
  - Each of the five pillars is a functional domain where Zero Trust principles are implemented
  - Three cross-cutting capabilities that span across all five pillars
- Heavily influenced by NIST, DOD, and NSA's zero trust publications
- This is a general model and is intended to provide direction for agencies



2025 Zscaler, Inc. All rights reserved

Identity Pillar Success Stories & Trends



Why (Problem/Need):

- Compromised credentials remain leading attack vector
- Legacy Authentication Methods
- Distributed Identity Platforms

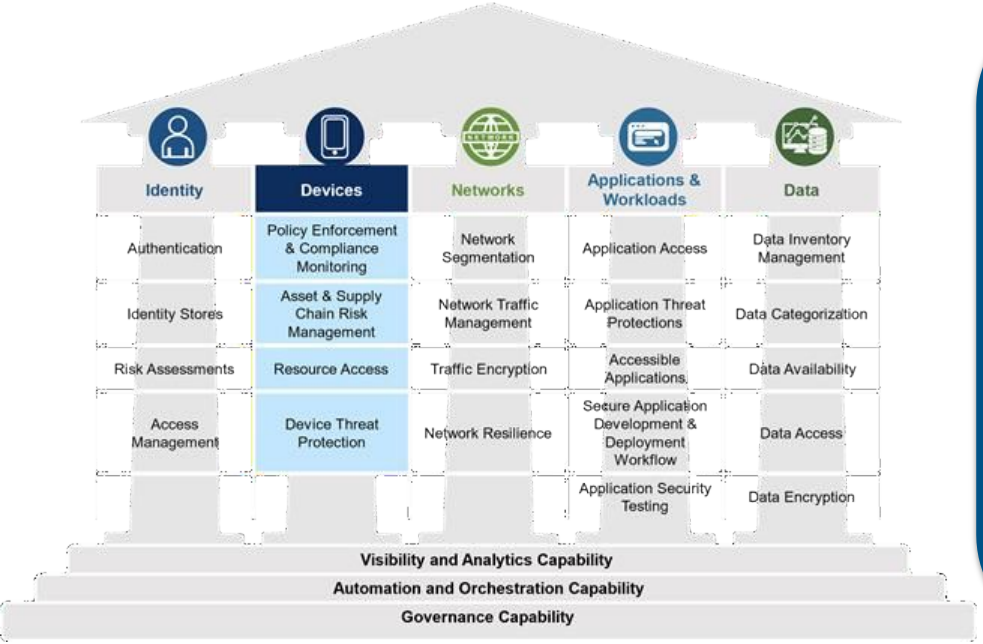
What/How to improve:

- Implement PR-MFA (move from PIV)
- Stronger user and roles inventories
- Use contextual signals to strengthen authentication and authorization
- Consolidate identity platforms

Sean Connelly

2025 Zscaler, Inc. All rights reserved

Device Pillar Success Stories & Trends



Why (Problem/Need):

- Lack comprehensive device inventory
- Exploitation of edge devices rising
- Lack of real-time threat detection

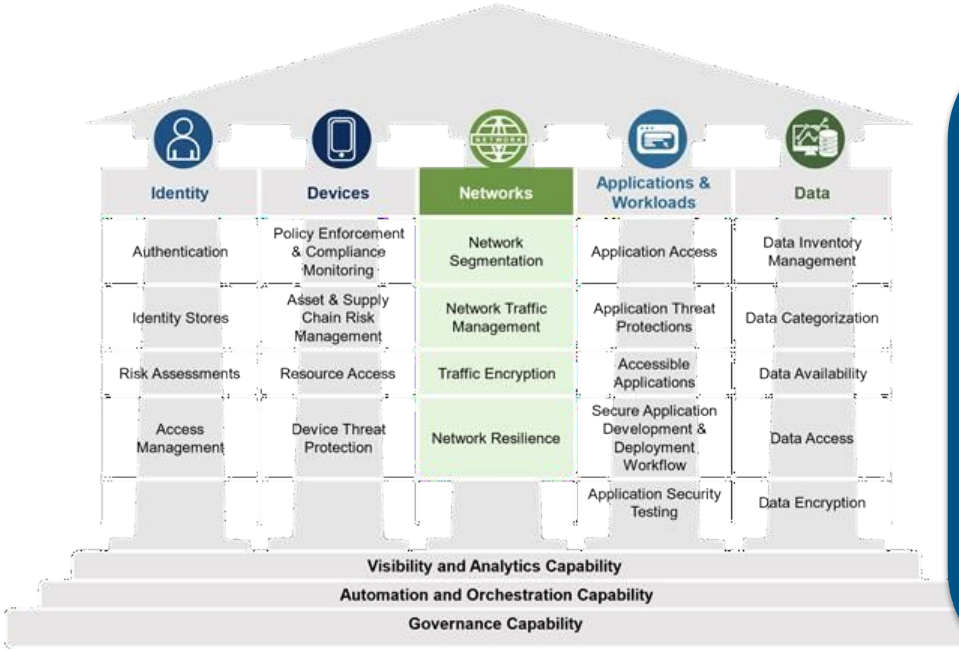
What/How to improve:

- Deploy EDR tools that meet CISA's technical standards
- Define logging and incident response metrics

Sean Connelly

2025 Zscaler, Inc. All rights reserved

Networks Pillar Success Stories & Trends



Why (Problem/Need):

- Implicit trust embedded in networks
- DNS is a target for manipulation
- Increase % of encrypted traffic

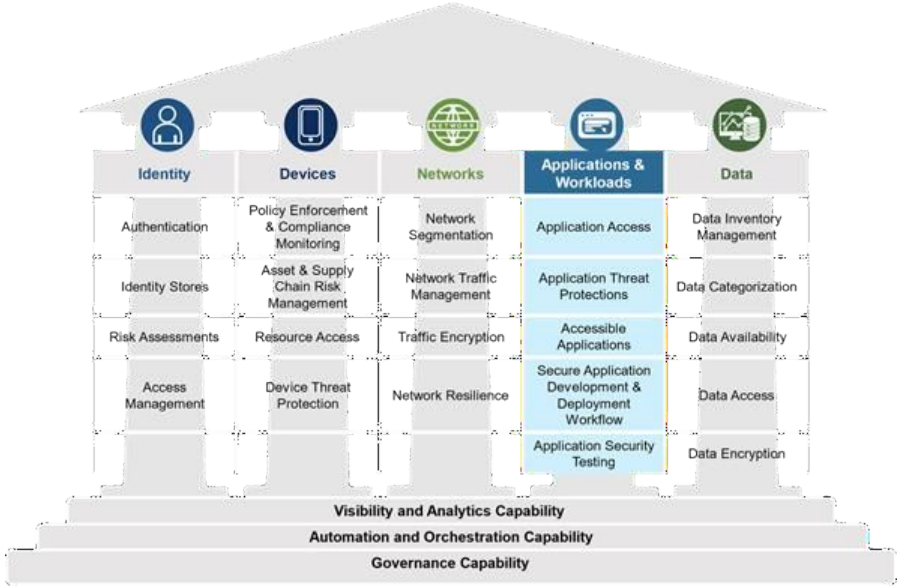
What/How to improve:

- Segment networks into isolated zones
- Foster SASE adoption, move off of legacy perimeter models
- Implement centralized DNS platform
- Enforce HTTPS and encrypted DNS

Sean Connelly

2025 Zscaler, Inc. All rights reserved

Applications & Workloads Pillar Success Stories & Trends



Why (Problem/Need):

- Web apps are a primary attack vector
- Application vulnerabilities are not always being addressed properly
- Cloud-based app require new ways to to consider risk

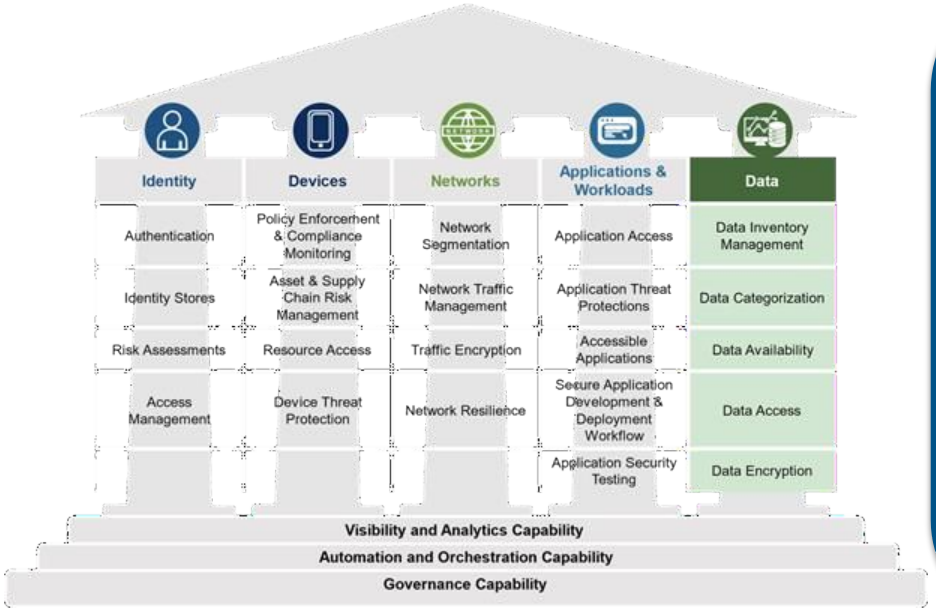
What/How to improve:

- Deploy rigorous app security testing
- Require public-facing systems to have a Vulnerability Disclosure Program
- Migrate a FISMA MOD system to be internet accessible

Sean Connelly

2025 Zscaler, Inc. All rights reserved

Data Pillar Success Stories & Trends



Why (Problem/Need):

- Unstructured data is a security risk
- Lack of proper data inventories
- Weak ability to audit data access

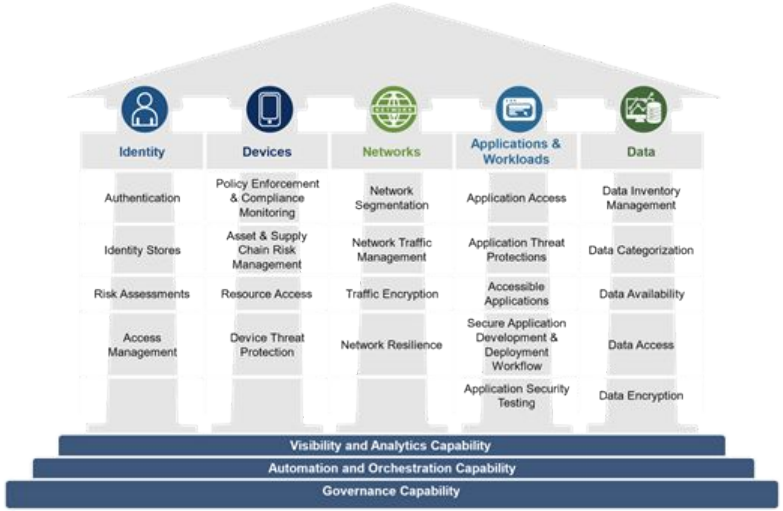
What/How to improve:

- Automate data classification & tagging
- Audit encryption key management
- Leverage cloud-based security analytics to access data access in near real-time

Sean Connelly

2025 Zscaler, Inc. All rights reserved

Cross Cutting Capabilities Success Stories & Trends



Why (Problem/Need):

- Security teams need better insights into user/device/network behavior
- Policies must dynamically adapt
- Agencies risk inconsistent ZT adoption

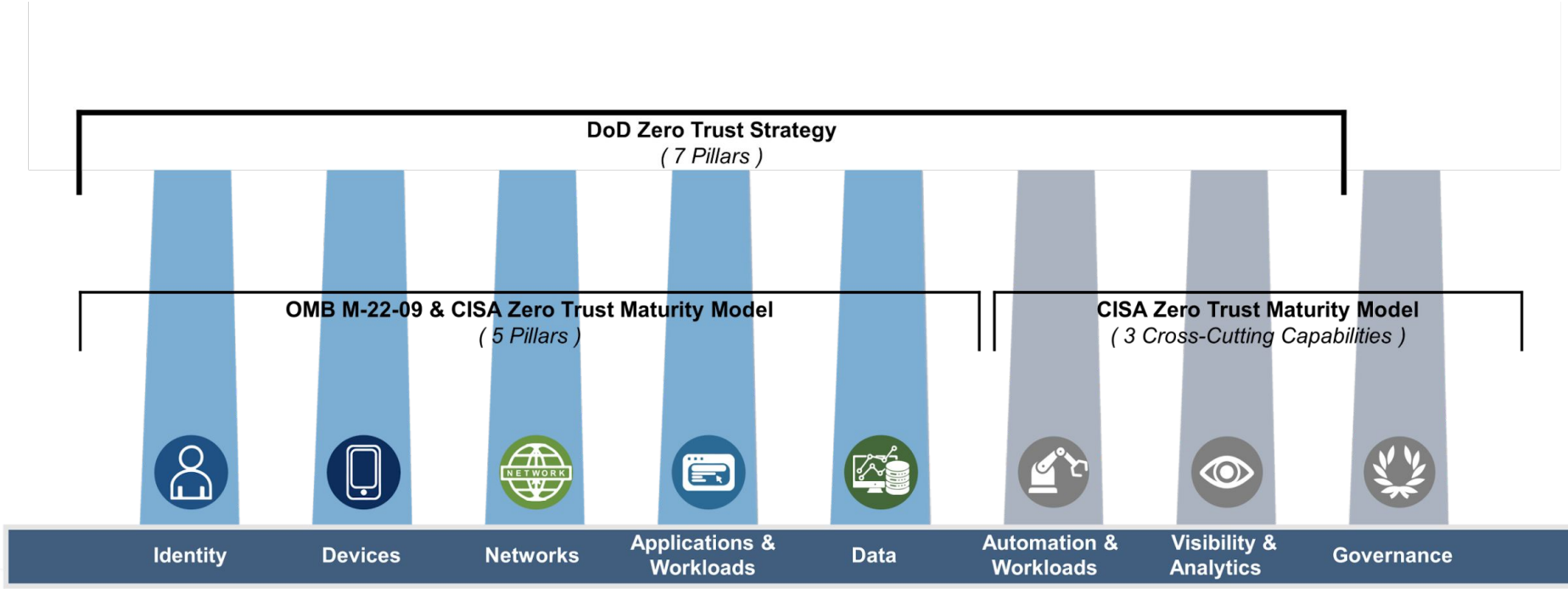
What/How to improve:

- Implement centralized logging and behavioral analytics
- Automate security responses to isolate, investigate and contain threats faster
- Develop governance frameworks

Sean Connelly

2025 Zscaler, Inc. All rights reserved

CISA & DoD Zero Trust Alignment



Sean Connelly

2025 Zscaler, Inc. All rights reserved

Top Challenges with Zero Trust

Security Gaps	• A piecemeal approach to zero trust can create gaps. Unwinding a legacy solution can create unexpected security lapses.
Long-term Commitment	• Zero trust requires commitment through ongoing administration. People move into new roles and change locations.
Zero Trust vs. Productivity	• Introducing a new security architecture cannot slow down the business or the mission.
Visibilit y	• Zero trust requires significant visibility that many agencies do not currently have access to.
Measuring/Validating Zero Trust Architecture	• Still in early stages, determining how zero trust architecture can best be measured and validated against standards.

Sean Connelly

2025 Zscaler, Inc. All rights reserved

Zero Trust Adoption By International Governments

Sean Connelly

2025 Zscaler, Inc. All rights reserved

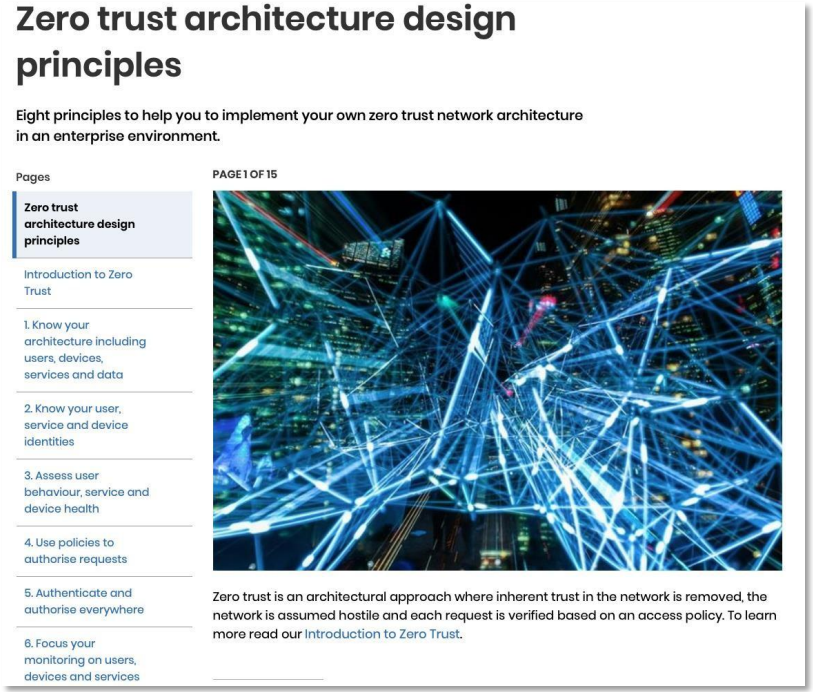
United Kingdom Zero Trust Efforts

UK's National Cyber Security Centre NCSC published "Zero Trust Architecture Design & Principles" in Feb 2023.

Eight Principles to implement a Zero Trust Architecture

1. Know your users, devices, services and data
2. Know your user, service and device identities
3. Assess user behavior, service and device health
4. Use polices to authorize requests
5. Authenticate and authorize everywhere
6. Focus your monitoring on users, devices and services
7. Don't' trust any network, including your own
8. Choose services which have been designed for Zero Trust

Includes blog posts and supplementary guidance



Zero trust architecture design principles

Eight principles to help you to implement your own zero trust network architecture in an enterprise environment.

Pages

- **Zero trust architecture design principles**
- Introduction to Zero Trust
- 1. Know your architecture including users, devices, services and data
- 2. Know your user, service and device identities
- 3. Assess user behaviour, service and device health
- 4. Use policies to authorise requests
- 5. Authenticate and authorise everywhere
- 6. Focus your monitoring on users, devices and services

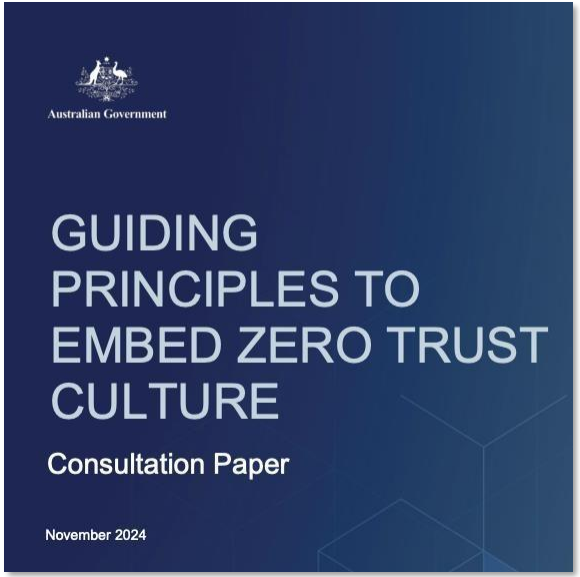
PAGE 1 OF 15

Zero trust is an architectural approach where inherent trust in the network is removed, the network is assumed hostile and each request is verified based on an access policy. To learn more read our Introduction to Zero Trust.

2025 Zscaler, Inc. All rights reserved

Australian Zero Trust Efforts

- Department of Home Affairs just closed an RFC on their "**Guiding Principles to Embed Zero Trust Culture**" Consultation Paper.
- The five guiding principles provide direction on the policy uplift activities required to embed a Zero Trust culture across the Commonwealth
  1. Identify & manage cyber security risk at an enterprise level
  2. Understand accountabilities and responsibilities at all levels
  3. Know and understand your most critical assets
  4. Maintain resiliency through a comprehensive cyber strategy
  5. Go beyond incident planning
- Aligns with the **2023-2030 Australian Cyber Security Strategy**, highlights the importance of uplifting Commonwealth Government cyber security.



2025 Zscaler, Inc. All rights reserved

Australian Zero Trust Efforts

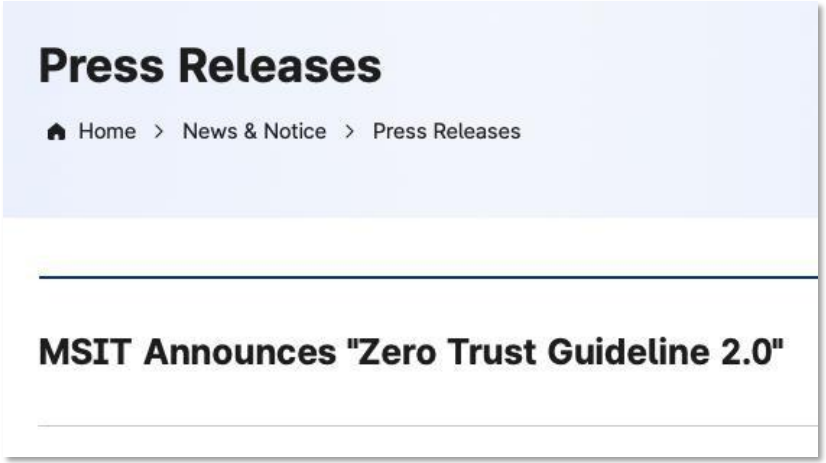
- Published in Feb 2025, the Australian Signals Directorate's (ASD's) "Foundations for Modern Defensible Architecture" provides a baseline of secure design and architecture activities.
- Ten Foundational aspects to build, maintain, update and enhance systems
  1. Centrally managed enterprise identities
  2. High assurance authentication
  3. Contextual authorization
  4. Reliable asset inventory
  5. Secure endpoints
  6. Reduced attack surface
  7. Resilient networks
  8. Secure-by-design software
  9. Comprehensive assurance and governance
  10. Continuous and actionable monitoring
- Aligns closely with NIST, CISA and NSA ZT guidance



2025 Zscaler, Inc. All rights reserved

South Korea Zero Trust Efforts

- The Ministry of Science and ICT (MSIT), in collaboration with the Korea Internet & Security Agency (KISA), released their Zero Trust Guideline in December 2024.
- Developed with input from industry, academia, and research experts, the guideline incorporates analyses of domestic and international trends and implementation cases.
- The guideline defines a maturity model, which has been expanded from three stages to four stages.
- Enables organizations to diagnose and analyze their current security posture, set goals, and verify progress when adopting the Zero Trust model.

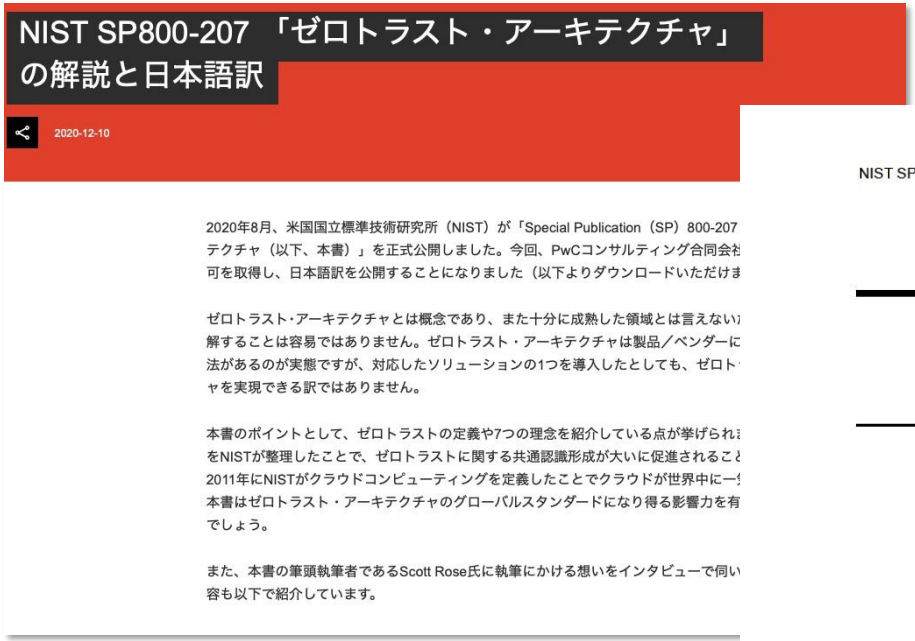


*

2025 Zscaler, Inc. All rights reserved

NIST 800-207 in other languages

Unofficial translations of 800-207 are available in Spanish and Japanese





*

Sean Connelly

2025 Zscaler, Inc. All rights reserved

Technology Modernization Fund

TMF

Sean Connelly

2025 Zscaler, Inc. All rights reserved

Technology Modernization Fund

- Federal Agencies submit proposals that are vetted by a Board of federal technology executives.
- Over $1.05 billion invested in 69 projects across 34 federal agencies.
- Only the highest impact projects with measurable return on investment and high likelihood of success are funded.
- To best steward taxpayer dollars, agencies receive incremental funding, unlocking transfers only by successfully completing project milestones.



Sean Connelly

2025 Zscaler, Inc. All rights reserved

Technology Modernization Fund

- While on the TMF Board, we awarded ~$800M awarded across 50+ projects at 25+ agencies

- All TMF awards have Zero Trust principles baked-in, helping agencies modernize their core missions.

- Some proposals were implicit with their Zero Trust efforts (but aligned with the seven ZT tenets).
  - Veterans: making it easier for Veterans to receive service benefits (new Identity services)
  - Farmers: faster labor certifications (new front-end w/ better cybersecurity)
  - Global Trade: more efficient cargo processing (mainframe to cloud migration)

- Some proposals were more explicit towards establishing new Zero Trust architectures:
  - GSA: $30M (Stronger ICAM & SOAR solutions)
  - ED: $20M (new ZT PMO, better SASE & stronger Cloud architectures)

2025 Zscaler, Inc. All rights reserved

Points of Contact

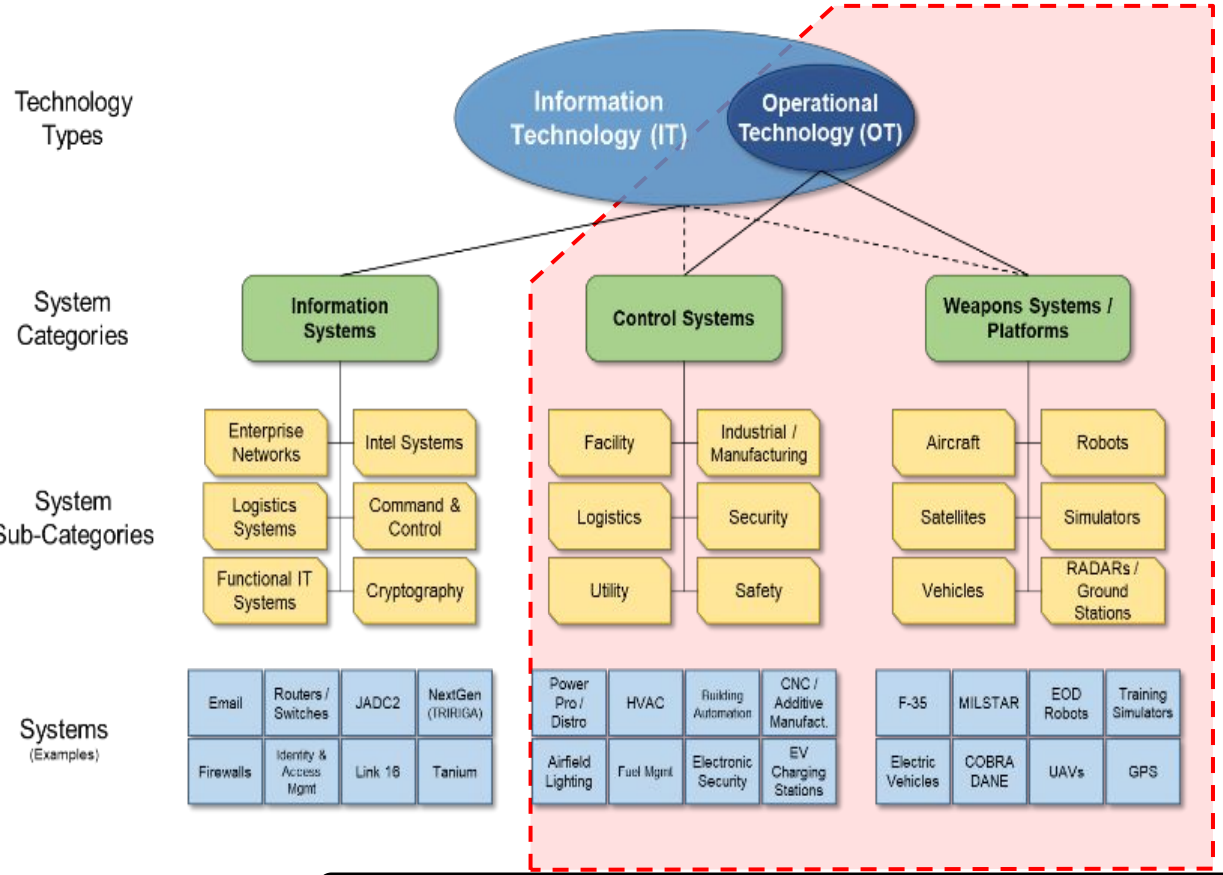
Email: sconnelly@zscaler.com

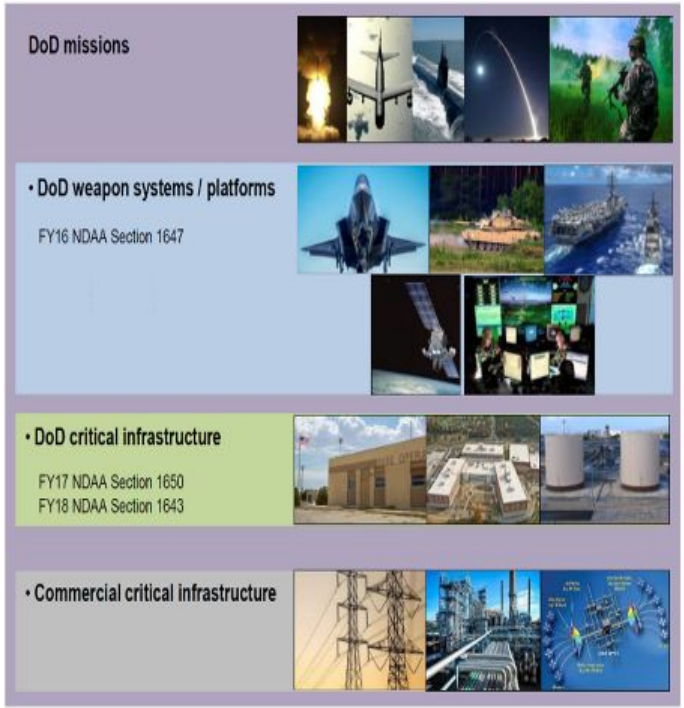
LinkedIn: https://www.linkedin.com/in/seanconnellydc/



Daryl Haegley

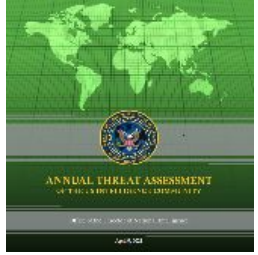
Missions Require IT & OT





100% of missions depend on power, water, or cooling

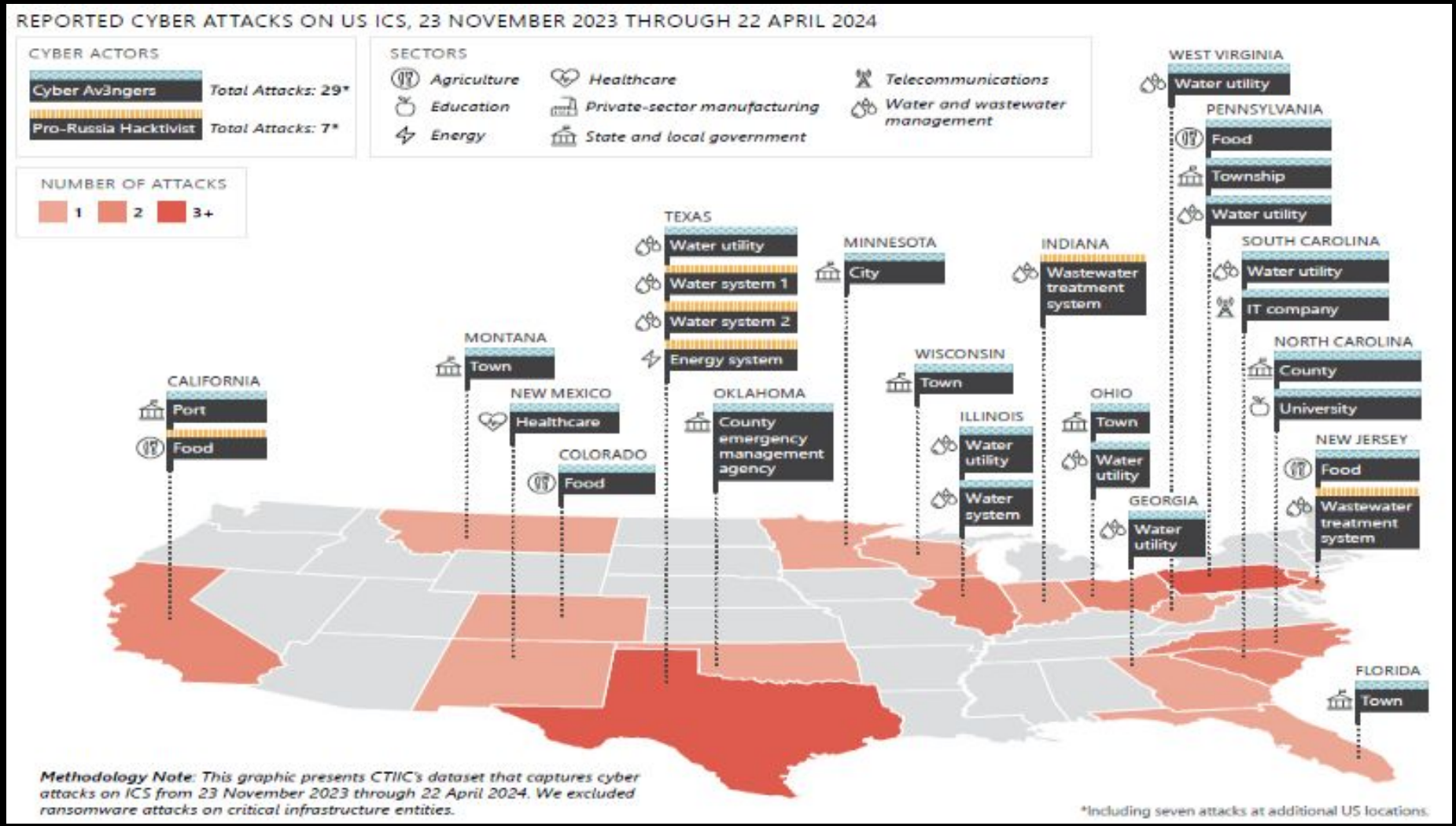
Director of National Intelligence- Annual Threat Assessments



Control systems/critical infrastructure are top "cyber" threats

- **Russia maintains its capability to target critical infrastructure, including underwater cables & industrial control systems, in US /allied / partner countries**
- **PRC operations discovered by U.S. private sector were intended to pre-position cyber attacks against infrastructure in Guam and to enable disrupting communications; it would consider aggressive cyber operations against U.S. critical infrastructure and military assets**
- **Iran has ability to conduct attacks on critical infrastructure, as well as to conduct influence and espionage activities. Iran was responsible for multiple cyber attacks between Apr-Jul'20 against Israeli water facilities that caused unspecified short-term effects (*press reporting*)**
- **Pyongyang's cyber forces have matured and are fully capable of achieving a variety of strategic objectives against diverse targets, including a wider target set in the US and South Korea**

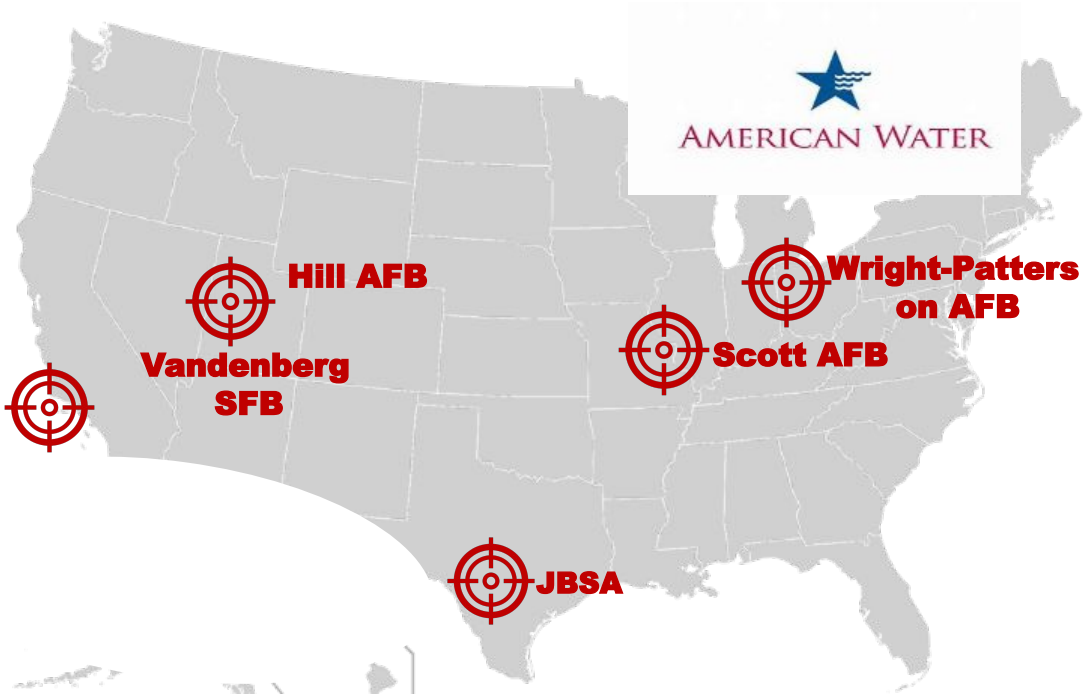
Adversaries Constantly Look for Any Weak Link …Which is Ours?


REPORTED CYBER ATTACKS ON US ICS, 23 NOVEMBER 2023 THROUGH 22 APRIL 2024
CYBER ACTORS
Cyber Av3ngers
Total Attacks: 29*
Pro-Russia Hacktivist
Total Attacks: 7*
SECTORS
Agriculture
Education
Energy
Healthcare
Private-sector manufacturing
State and local government
Telecommunications
Water and wastewater management
NUMBER OF ATTACKS
1
2
3+
CALIFORNIA
Port
Food
MONTANA
Town
NEW MEXICO
Healthcare
COLORADO
Food
TEXAS
Water utility
Water system 1
Water system 2
Energy system
OKLAHOMA
County emergency management agency
MINNESOTA
City
WISCONSIN
Town
ILLINOIS
Water utility
Water system
INDIANA
Wastewater treatment system
OHIO
Town
Water utility
GEORGIA
Water utility
WEST VIRGINIA
Water utility
PENNSYLVANIA
Food
Township
Water utility
SOUTH CAROLINA
Water utility
IT company
NORTH CAROLINA
County
University
NEW JERSEY
Food
Wastewater treatment system
FLORIDA
Town
Methodology Note: This graphic presents CTIIC's dataset that captures cyber attacks on ICS from 23 November 2023 through 22 April 2024. We excluded ransomware attacks on critical infrastructure entities.
*Including seven attacks at additional US locations.

In the News: American Water Cybersecurity Attack (Oct '24)

BLUF: 07 Oct '24 -largest water and wastewater utility company in US, American Water (AW), announced that it was victim of a cyberattack

- **Cyberattack against AW billing systems, halting operations for a week**
- **AW services 18 military sites including five DAF installations**
- **Thankfully, no direct impact to water or wastewater services but attack demonstrates vulnerability in critical infrastructure**



Water and wastewater systems will continue to be vulnerable target for adversaries; Need increased focus / resources on water resiliency

1st DoD Zero Trust Pilot - Spangdahlem AB

- Project BlastWave selected – DoD CIO ZTPfMO
  - Oil & Nat Gas OT experience
- BlastWave's *BlastShield* software-defined perimeter, Dark Trace's AI & Nozomi's Guardian solutions improved security and protection of on-base Supervisory Control and Data Acquisition (SCADA)
- Equipt installed Dec'23; DoD CIO Deputy visit Jan'24
  - ~$500K project solution for installation's 5 water wells and 2 water treatment facilities

Funded w/ Sustainment for 2yrs; Red Team Eval in Nov'24

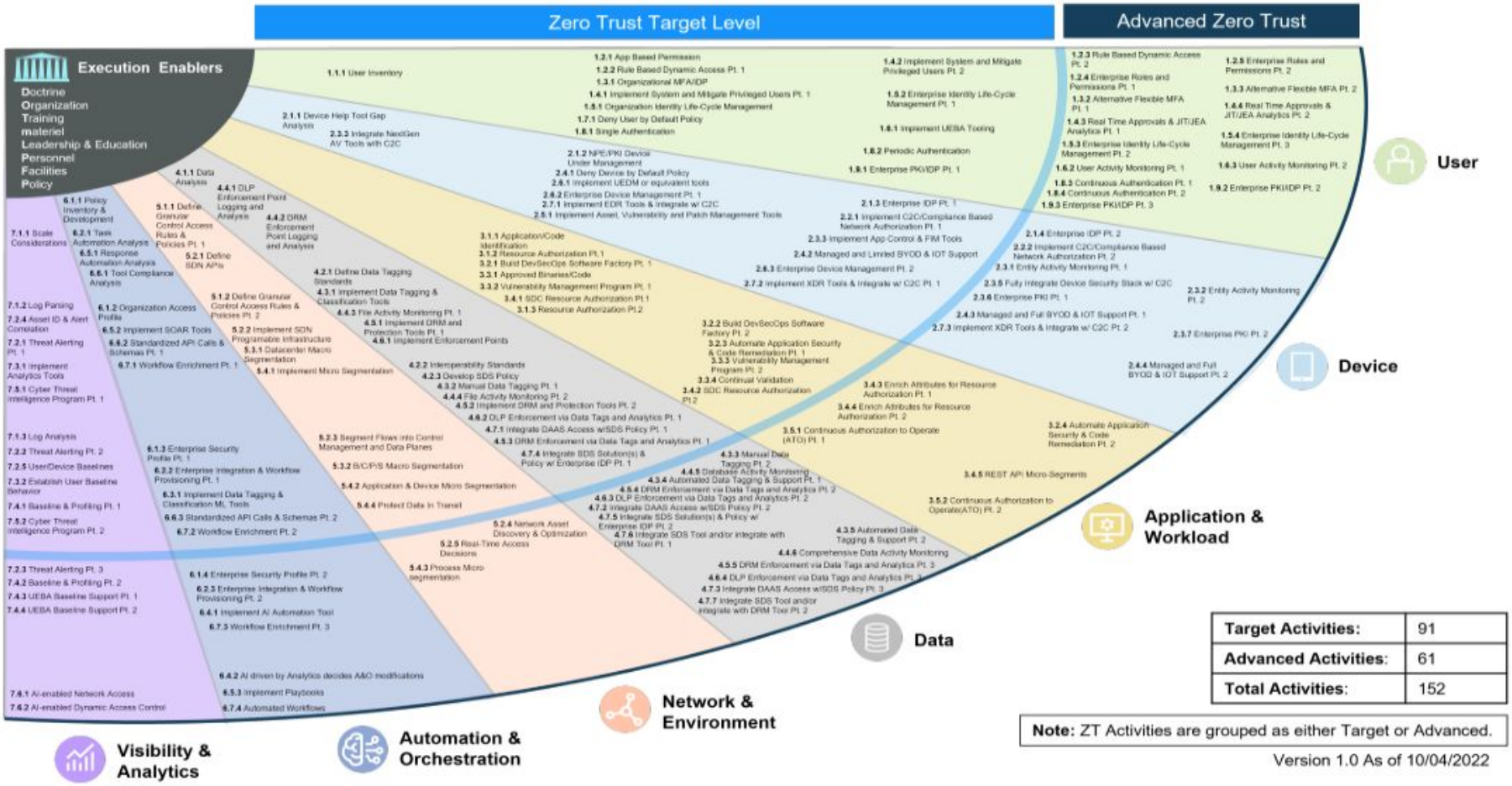
"OT Zero Trust Alliance"

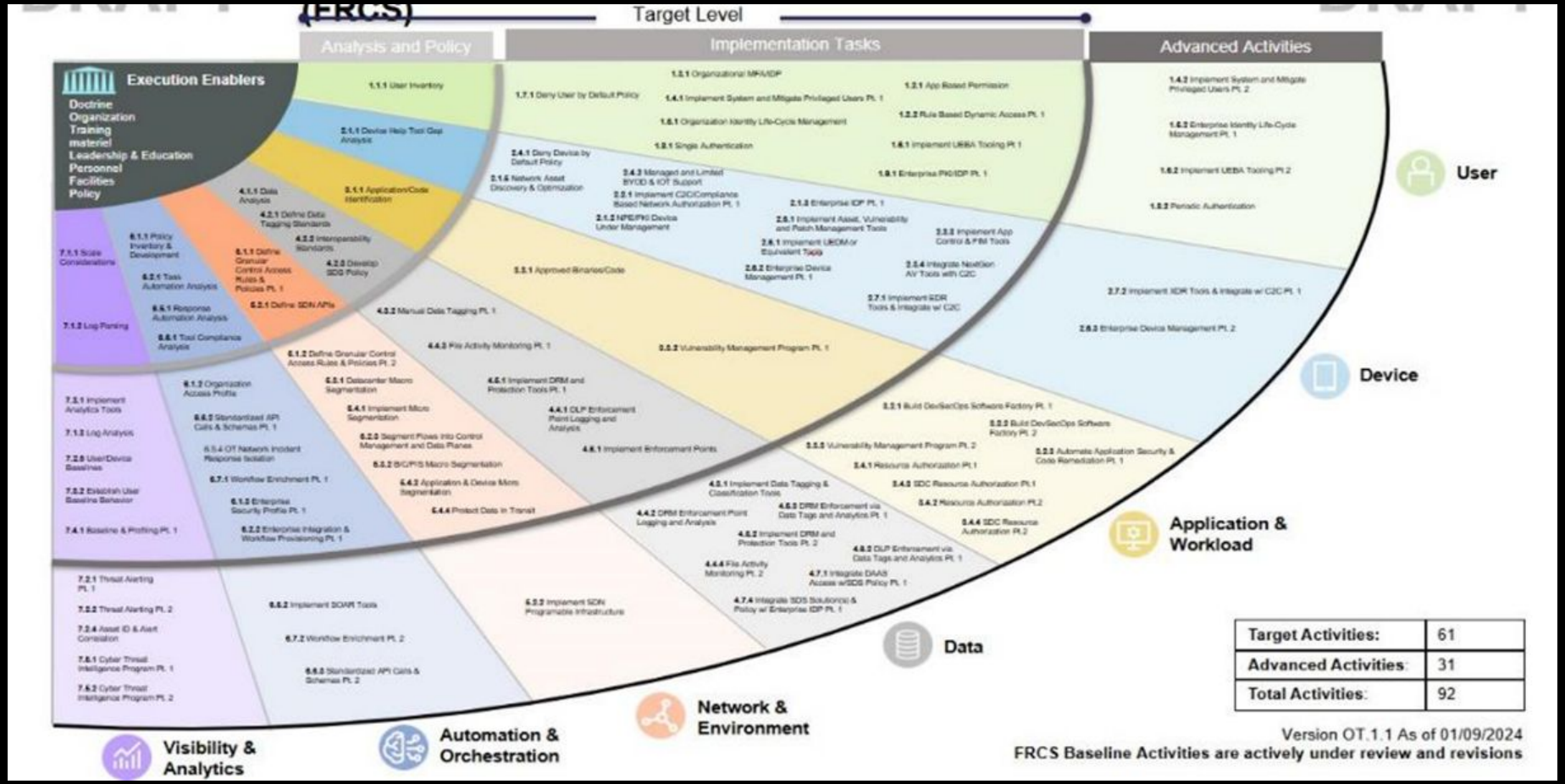
BlastWave
DarkTrace
Nozomi
CloudBees
Boston Consulting Grp





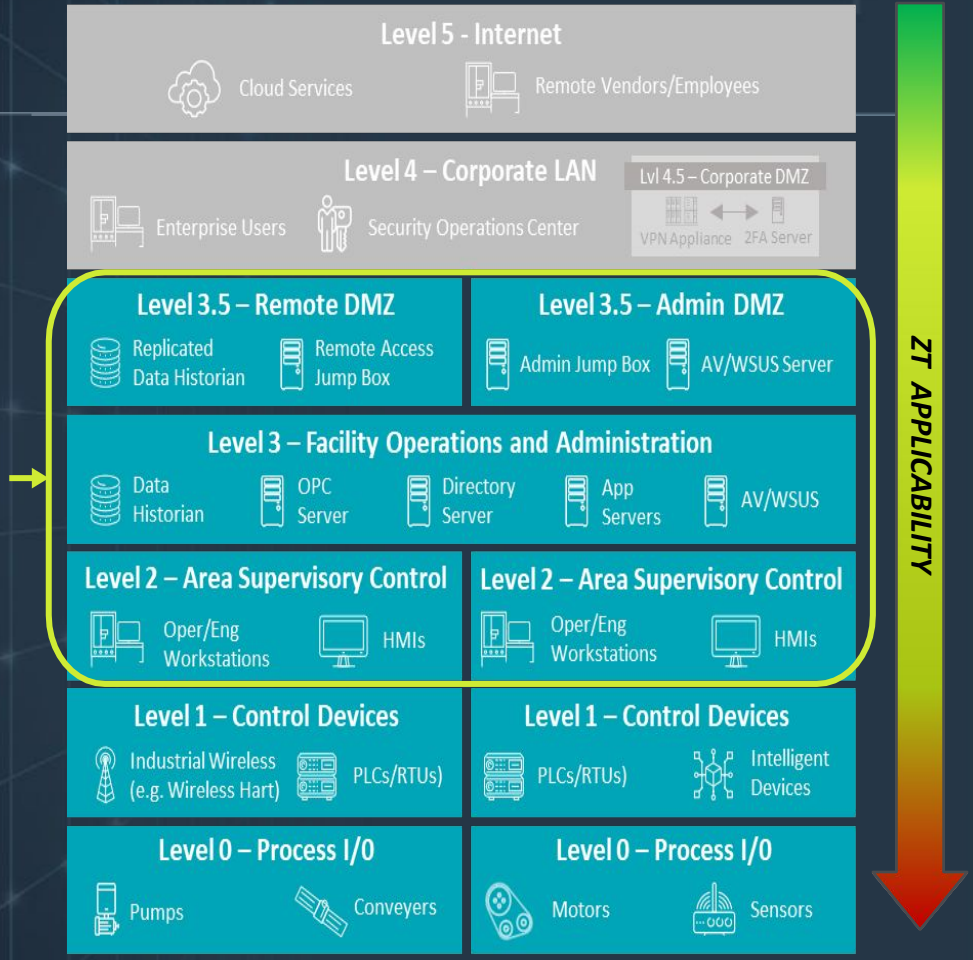
ZT ACTIVITIES APPLY = IT (152)




(FRCS)
Target Level
Analysis and Policy
Implementation Tasks
Advanced Activities
Execution Enablers
Doctrine
Organization
Training
materiel
Leadership & Education
Personnel
Facilities
Policy
User
Device
Application & Workload
Data
Network & Environment
Automation & Orchestration
Visibility & Analytics
Target Activities: 61
Advanced Activities: 31
Total Activities: 92
Version OT.1.1 As of 01/09/2024
FRCS Baseline Activities are actively under review and revisions

DEMYSTIFYING ZERO TRUST FOR OT

- Focus on ***The Funnel of Opportunity*** for ZT implementation (Purdue L3-L1)
- Successful OT cybersecurity programs do the basics well
- ZT & OT Cybersecurity are fundamentally both engineering disciplines
- OT data isn't always sensitive
- Novel solutions don't scale
- Endpoints can't always be hardened, but can always be secured
- Connectivity and bandwidth are often constrained
- Detection/response dwell time directly correlates to risk of impact

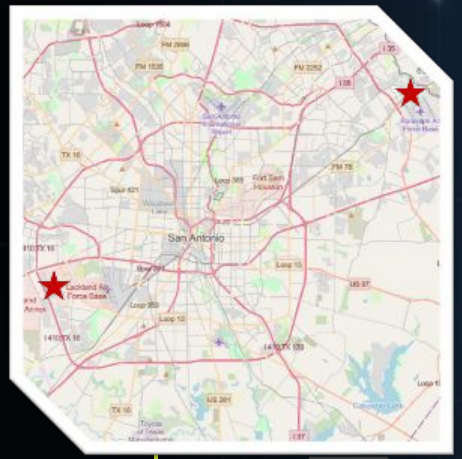


© 2024 Booz Allen Hamilton Inc.

ZERO TRUST OT PILOT – SW REGION AF & USSF NETWORKS

Intent **Proposed: JBSA-Lackland, JBSA-Randolph**

- Align to DoD Mission Assurance Priority Installations
- Pilot installations with control systems on AFCEC COIN
- Combination of large and small-sized installations
- Integrate ZT security across Air Force and Space Force
- Integrate with connected systems and dashboard to 16th AF
- Evaluate power utility systems, HVAC systems,
- Install and assess software-defined perimeter (SDP) security solution
- Integrate with AFCEC COIN
- Integrated dashboard for data visibility and interface with 16th AF
- Leverage existing Nozomi deployments (CE COIN)



2 SITES

SURVEY

INSTALL

EACH SITE

CE COIN Monitoring

OT Network Cloaking (Blastwave)

OT NSM (Nozomi)

INTEGRATE

ENABLE ACTION

16TH AIR FORCE

Tier II CSSP Incident Response

AFIN Network

ELICSAR BDP

ESTABLISH ZT on OT NETWORK

SOFTWARE-DEFINED PERIMETER

BlastWave



NETWORK THREAT DETECTION

NOZOMI NETWORKS



© 2024 Booz Allen Hamilton Inc.

ZT TARGET ACTIVITIES MAPPED TO PURDUE MODEL



6) AUTOMATION & ORCHESTRATION

1. Defined Security Processes — LEVEL-1
2. Task & Workflow Automation — LEVEL-3
3. Data Tagging & ML — LEVEL-2
4. AI Implementation — N/A
5. SOAR Automation & Response — LEVEL-3
6. Tool Compliance Analysis — LEVEL-1
7. Workflow Enrichment — LEVEL-3

7) VISIBILITY AND ANALYTICS

1. Log Parsing & Analysis — LEVEL-1
2. Threat Alerting — LEVEL-1
3. User Behavior Analytics — LEVEL-2
4. Network/User Baseline & Profiling — LEVEL-2
5. Cyber-Threat Intelligence Integration — LEVEL-1
6. AI-Enabled Access Control — LEVEL-3

3) APPLICATIONS & WORKLOADS

1. Application Inventory — LEVEL-2
2. DevSecOps — N/A
3. Application Vulnerability Management — LEVEL-1
4. SDP Resource Authorization — N/A
5. cATO — N/A

5) NETWORK & ENVIRONMENT

1. Define Granular Access — LEVEL-1
2. Software Defined Networking — LEVEL-1
3. Network Macro-Segmentation — LEVEL-3
4. Network Micro-Segmentation — LEVEL-1

4) DATA

1. Data Classification — LEVEL-1
2. Data Tagging & Storage — LEVEL-2
3. Implement Data Tagging & Classification — LEVEL-3
4. Data Loss Prevention (DLP) — LEVEL-2
5. DRM Protection & Enforcement — N/A
6. DLP Enforcement Points — LEVEL-3
7. DaaS/SDS Integration — N/A

1) USER

1. Account Discovery & Inventory — LEVEL-2
2. App-Based Permissions — LEVEL-2
3. Organizational MFA — LEVEL-2
4. Privileged User Management — LEVEL-1
5. Privilege Lifecycle Management — LEVEL-1
6. UEBA — LEVEL-2
7. Deny User by Default — LEVEL-1
8. IdP Authentication — LEVEL-2
9. Enterprise PKI/IdP — LEVEL-2

2) DEVICES

1. Asset Discovery & Inventory — LEVEL-1
2. Comply to Connect — LEVEL-3
3. Implement EUBA — LEVEL-2
4. BYOD & IoT Support — LEVEL-1
5. Patching & Vulnerability Management — LEVEL-1
6. Implement UEDM — LEVEL-2
7. EDR/XDR Integration with C2C — LEVEL-2

LEGEND

- LEVEL-5
- LEVEL-4
- LEVEL-3

© 2024 Booz Allen Hamilton Inc.

Zero Trust Activity Coverage & Validation

Covered by BAH | Covered by BlastWave
Covered by AF Networks | Covered by Nozomi | Activity Not Covered



User

- User Inventory
- Conditional User Access
- Multi-Factor Authentication
- Privileged Access Management
- Identity Federation & User Credentialing
- Behavioral, Contextual ID, & Biometrics
- Least Privileged Access
- Continuous Authentication
- Integrated ICAM Platform



Device

- Device Inventory
- Device Detection & Compliance
- Device Authorization with Real-Time Inspection
- Remote Access
- Partially & Fully Automated Asset, CVE, & Patch Mgmt
- Unified Endpoint Mgmt (UEM) & Mobile Device Mgmt (MDM)
- Endpoint & Extended Detection & Response (EDR & XDR)



Application & Workload

- Application Inventory
- Secure Software Development & Integration
- Software Risk Management
- Resource Authorization & Integration
- Continuous Monitoring & Ongoing Authorizations



Data

- Data Catalog Risk Assessment
- DoD Enterprise Data Governance
- Data Labelling & Tagging
- Data Monitoring & Sensing
- Data Encryption & Rights Management
- Data Loss Prevention (DLP)
- Data Access Control



Network & Environment

- Data Flow Mapping
- Software Define Networking (SDN)
- Macro Segmentation
- Micro Segmentation



Automation & Orchestration

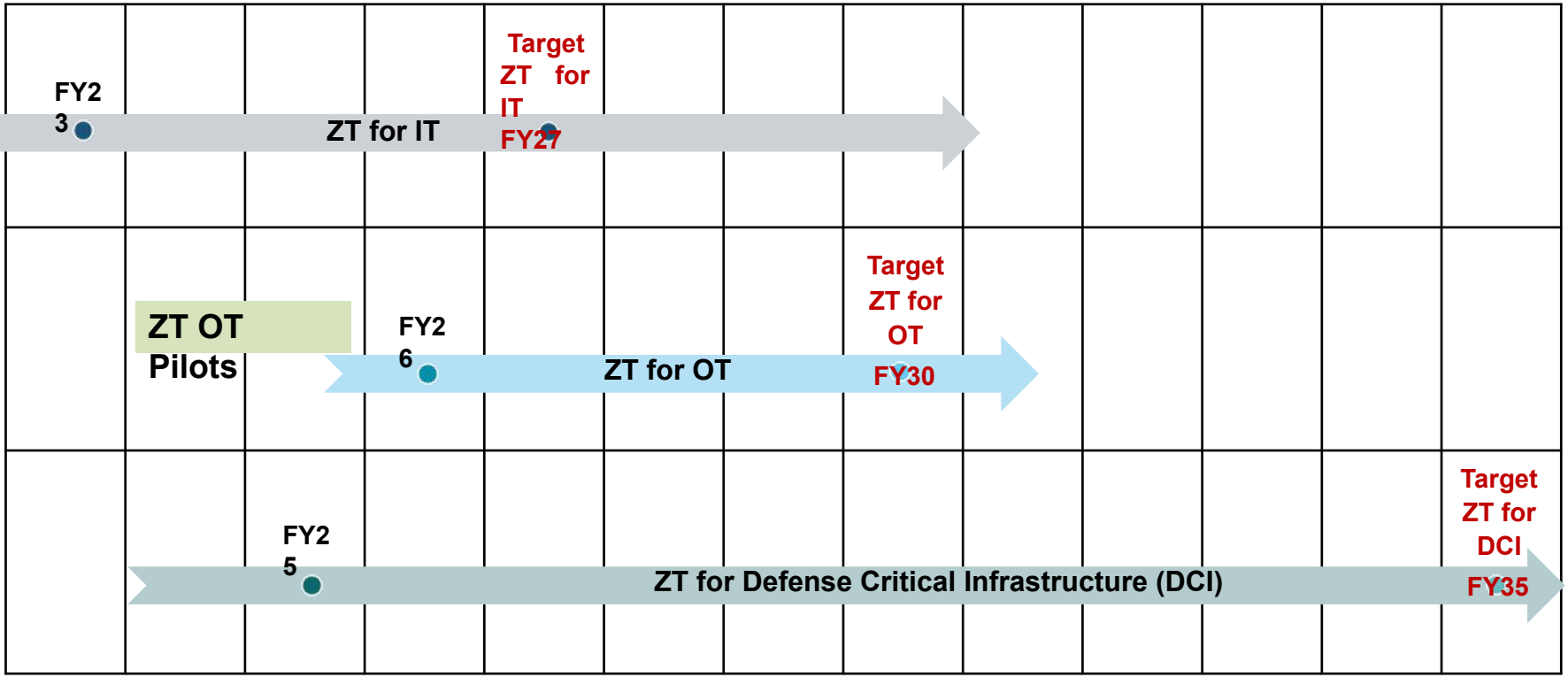
- Policy Decision Point (PDP) & Policy Orchestration
- Critical Process Automation
- Machine Learning
- Artificial Intelligence
- Security Orchestration Automation & Response (SOAR)
- API Standardization
- Security Operations Center (SOC) & Incident Response (IR)



Visibility & Analytics

- Log All Traffic (Network, Data, Apps, Users)
- Security Information & Event Management (SIEM)
- Common Security & Risk Analytics
- User & Entity Behavior Analytics
- Threat Intelligence Integration
- Automated Dynamic Policies

ZT PfMO "Notional" Deadlines for DoD



“The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.” ***Sun Tzu***





The W. Edwards Deming Institute

W. Edwards Deming

A bad system will beat a good person every time.

source: quotes.deming.org/10091

Cyber Resiliency Office for Control Systems

Who:

New office dedicated to coordinating & overseeing cyber defense & resilience of DAF OT/CS

What: **<1 stop shop>**

- **Coordinate Policy among control system owners**
- **Coordinate between system owners and cyber defenders**
- **Oversight of DAF-wide DCI cyber initiatives**
- **Funding advocacy & spend priorities**



Why:

Installations are power projection platforms underpinned by critical control systems that expose critical assets to adversarial threats

Specific Focus on OT long overdue!

Contact

Email: af.crocs@us.af.mil

Web:
https://usaf.dps.mil/teams/DAFCRoCSGroup (CAC-enabled)



CYBER RESILIENCY OFFICE
FOR CONTROL SYSTEMS
CROCS

Jason Garbis

Distribution Statement A.
Approved for public release: distribution is unlimited.

NUMBERLINE SECURITY

It’s About the Forest, Not the Trees

Why Improving Zero Trust Maturity Shouldn’t Be Your Only Goal

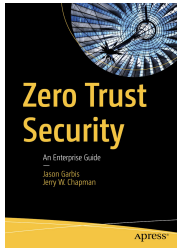
Jason Garbis

Co-Chair, Zero Trust working group, Cloud Security Alliance

Founder and Principal, Numberline Security

IANS Faculty Member

Co-Author: *Zero Trust Security: An Enterprise Guide*



Zero Trust Initiatives Are Not Trees



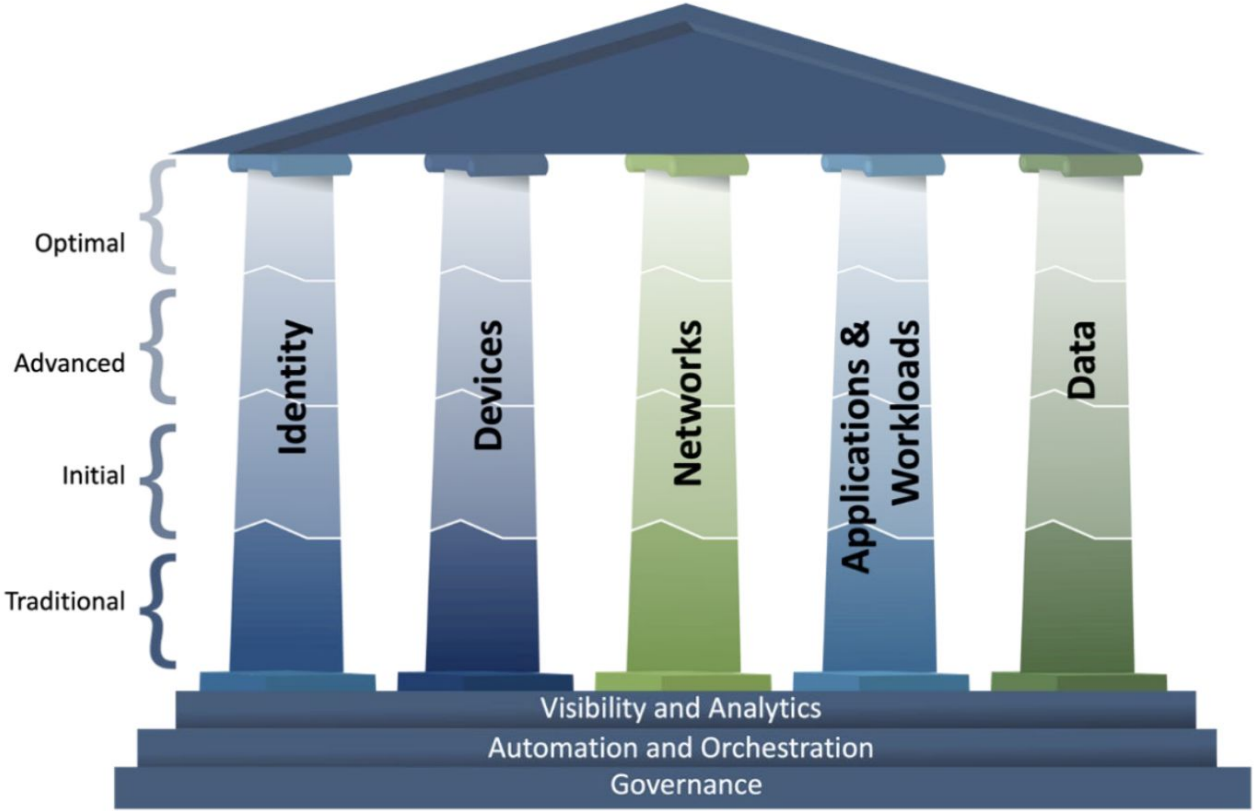


Maturity Models are excellent tools…

…but they can be too one-dimensional

CISA Maturity Model

NUMBERLINE SECURITY



Source: CISA ZTMM v2.0, April 2023

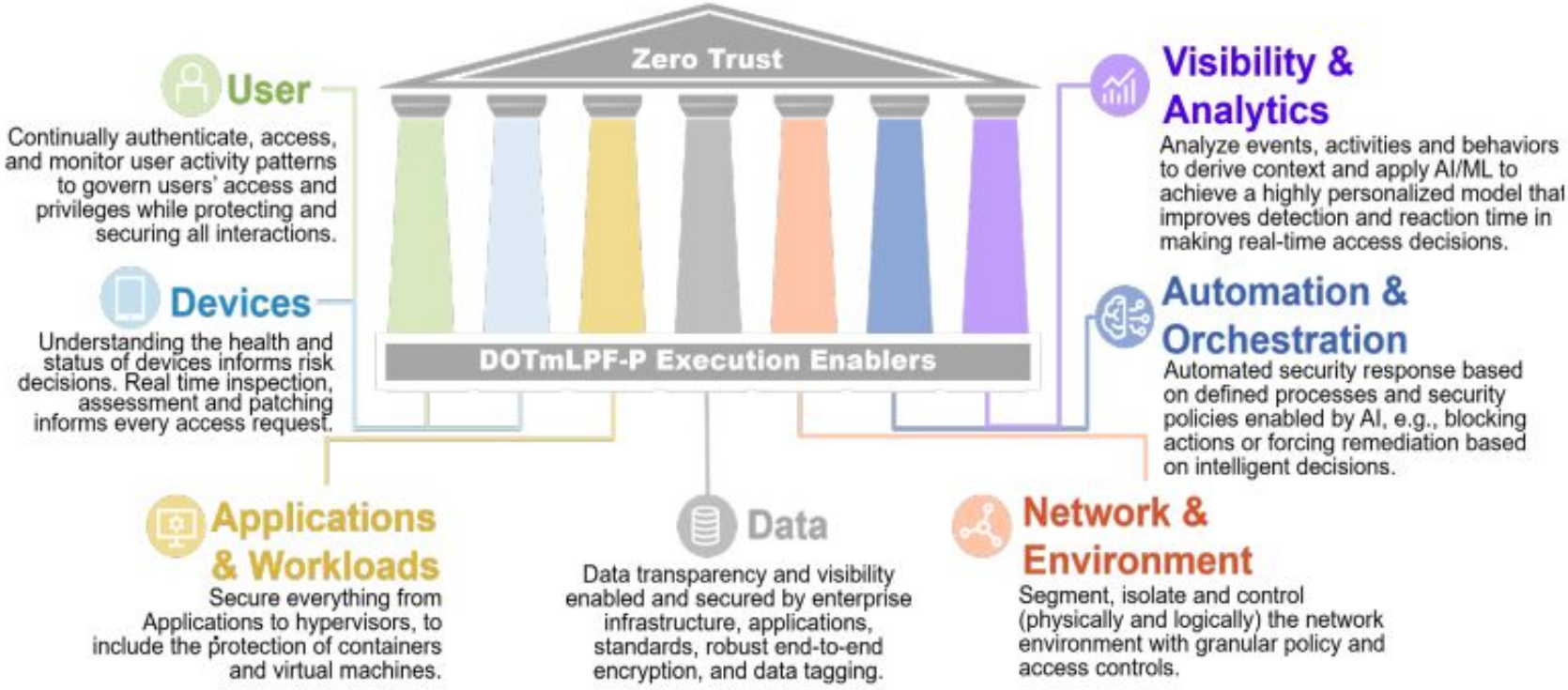
CISA: Function Maturity Pathways

NUMBERLINE SECURITY

Function	Traditional	Initial	Advanced	Optimal
Identity Stores	Agency only uses self-managed, on-premises (i.e., planned, deployed, and maintained by agency) identity stores.	Agency has a combination of self-managed identity stores and hosted identity store(s) (e.g., cloud or other agency) with minimal integration between the store(s) (e.g., Single Sign-on.).	Agency begins to securely consolidate and integrate some self-managed and hosted identity stores.	Agency securely integrates their identity stores across all partners and environments as appropriate.
Risk Assessments	Agency makes limited determinations for identity risk (i.e., likelihood that an identity is compromised).	Agency determines identity risk using manual methods and static rules to support visibility.	Agency determines identity risk with some automated analysis and dynamic rules to inform access decisions and response activities.	Agency determines identity risk in real time based on continuous analysis and dynamic rules to deliver ongoing protection.
Access Management (New Function)	Agency authorizes permanent access with periodic review for both privileged and unprivileged accounts.	Agency authorizes access, including for privileged access requests, that expires with automated review.	Agency authorizes need-based and session-based access, including for privileged access request, that is tailored to actions and resources.	Agency uses automation to authorize just-in-time and just-enough access tailored to individual actions and individual resource needs.

Source: CISA ZTMM v2.0, April 2023

DoD Zero Trust Maturity Model Pillars



Source: DoD Zero Trust Strategy, Oct 2022

DoD Zero Trust Capabilities



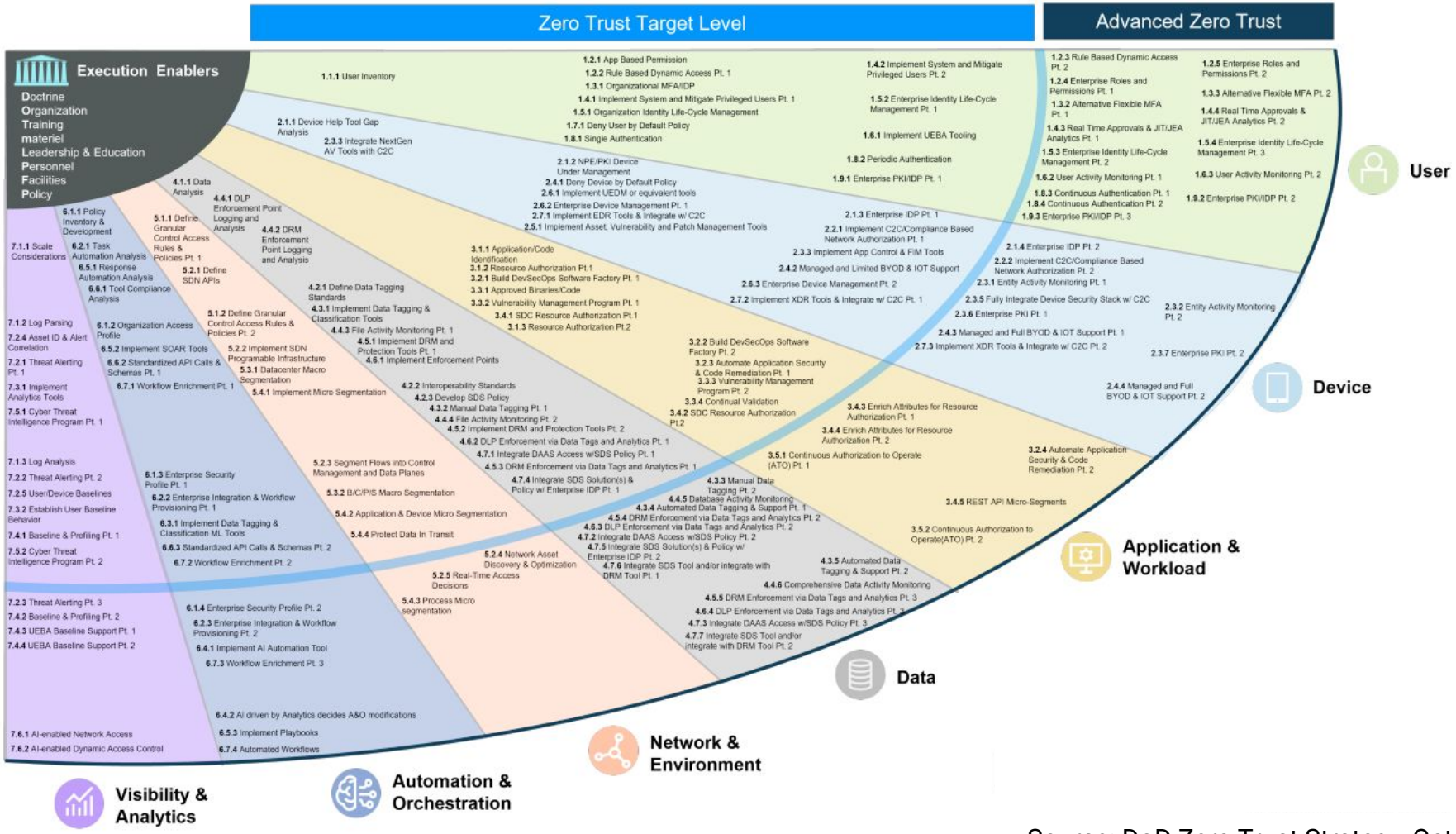
Source: DoD Zero Trust Strategy, Oct 2022

DoD Zero Trust Capabilities (Target & Advanced Levels)

	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

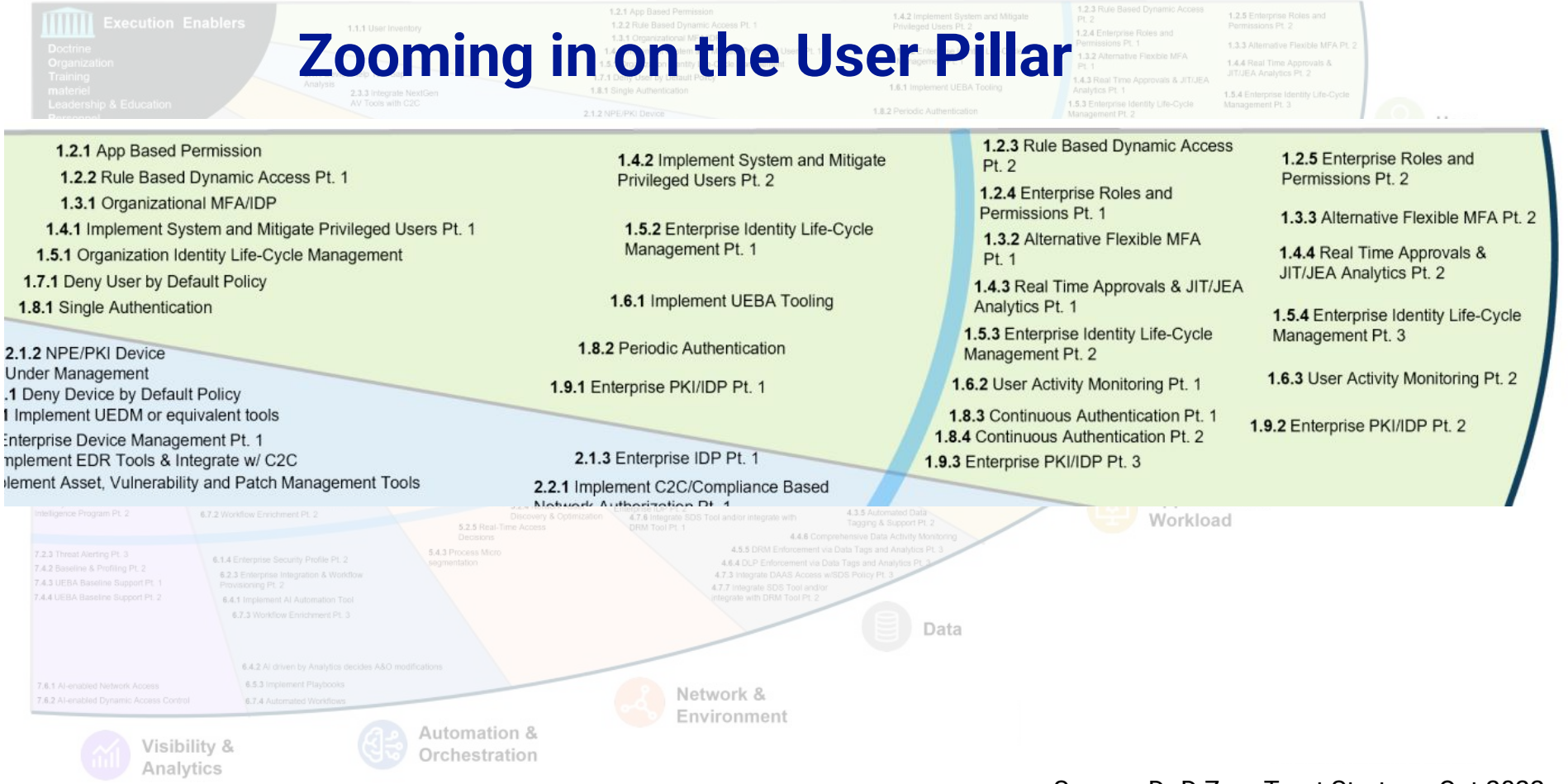
EXECUTION ENABLERS	Doctrine	Organization	Training	materiel	Leadership & Education	Personnel	Facilities	Policy

Source: DoD Zero Trust Strategy, Oct 2022



Source: DoD Zero Trust Strategy, Oct 2022

Zooming in on the User Pillar

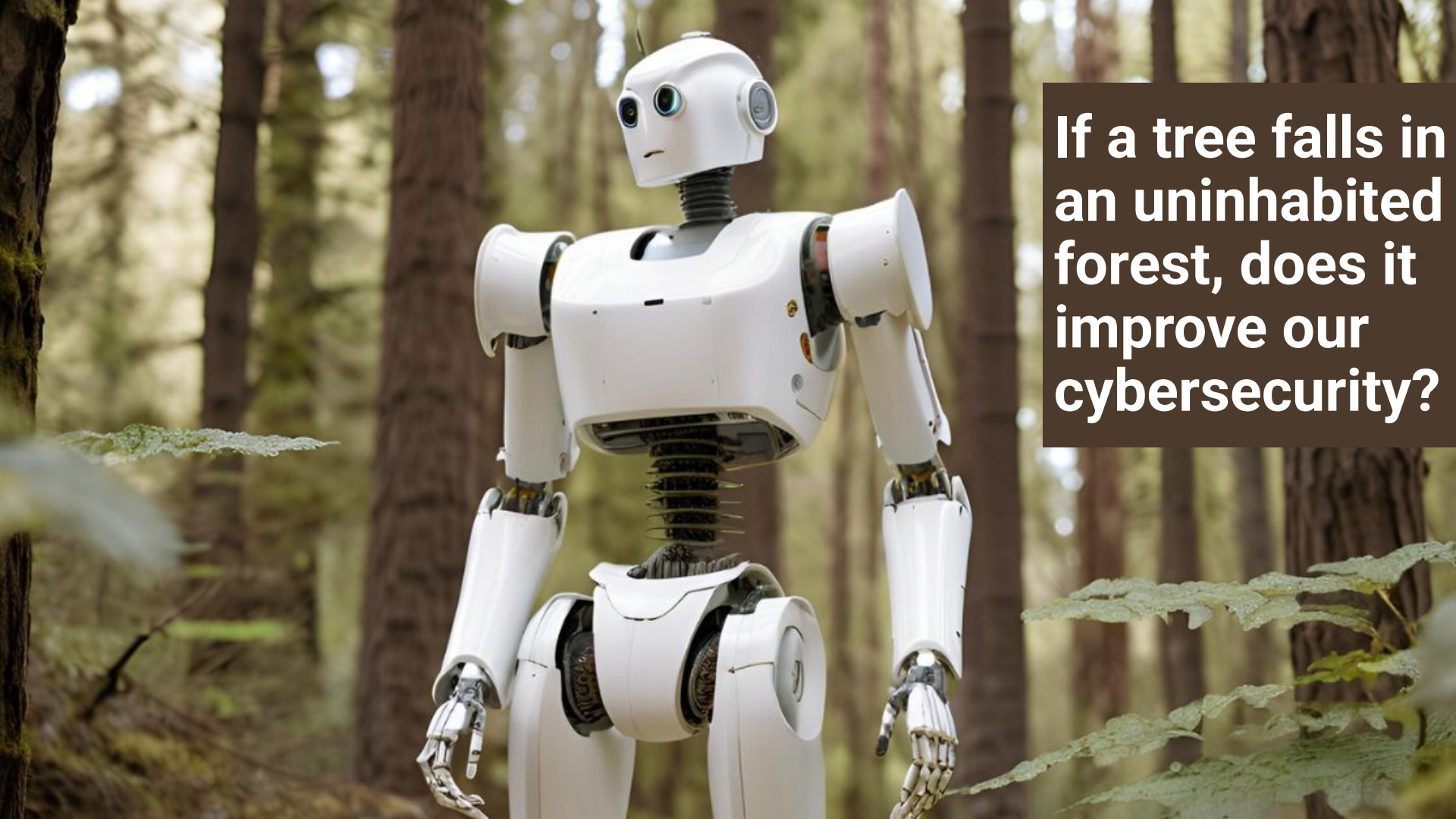


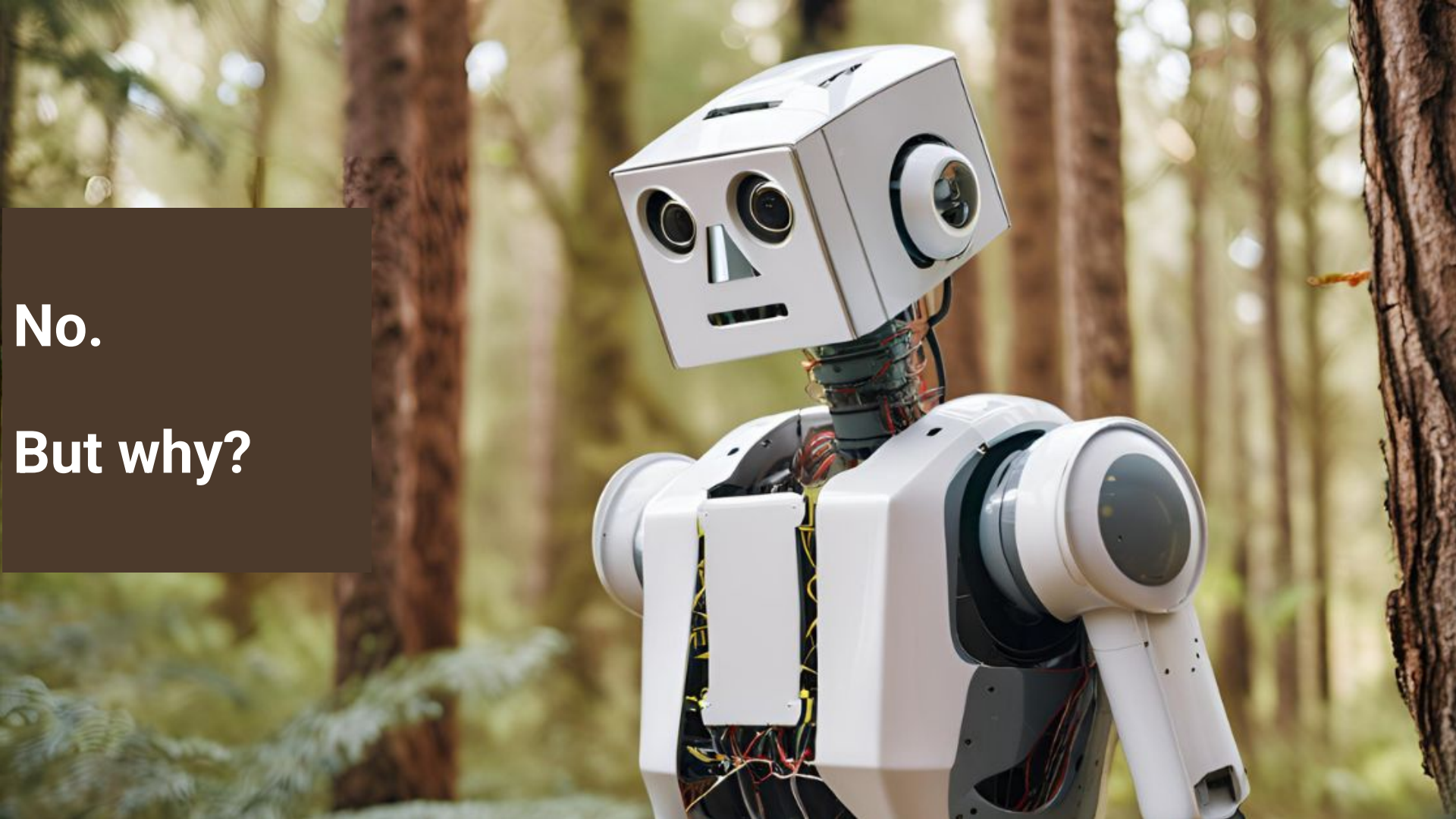
Source: DoD Zero Trust Strategy, Oct 2022

We’re not throwing anything under the bus!




1
1a


If a tree falls in an uninhabited forest, does it improve our cybersecurity?


No.
But why?

We need to move beyond Gantt charts



We’re not throwing anything under the bus!



So, what’s the forest?



What's the hierarchy?



Business or Mission Asset

Protect Surface

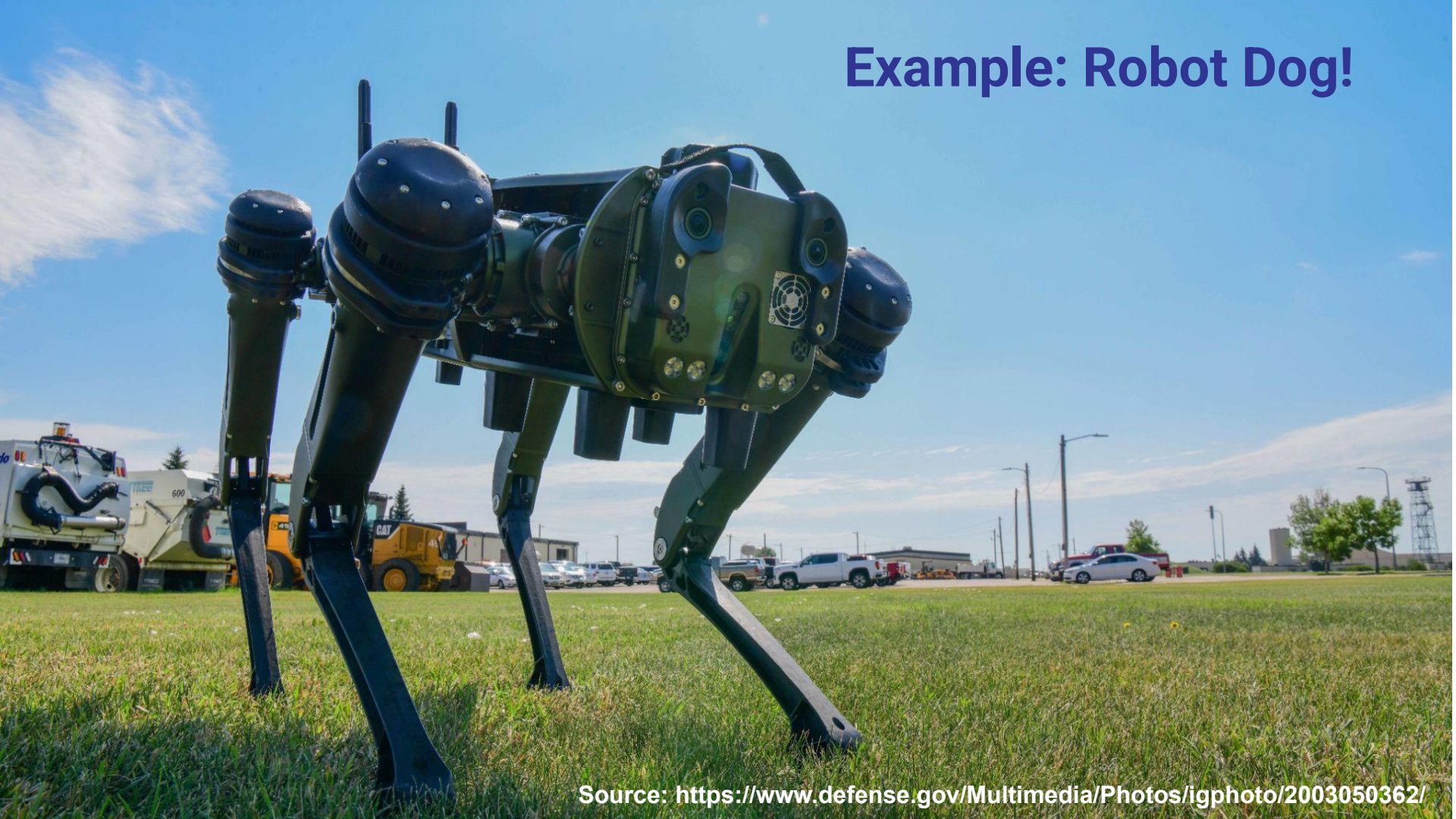
Transaction Flow

Access Policy

Capability

Tool, Technology, Process

Example: Robot Dog!

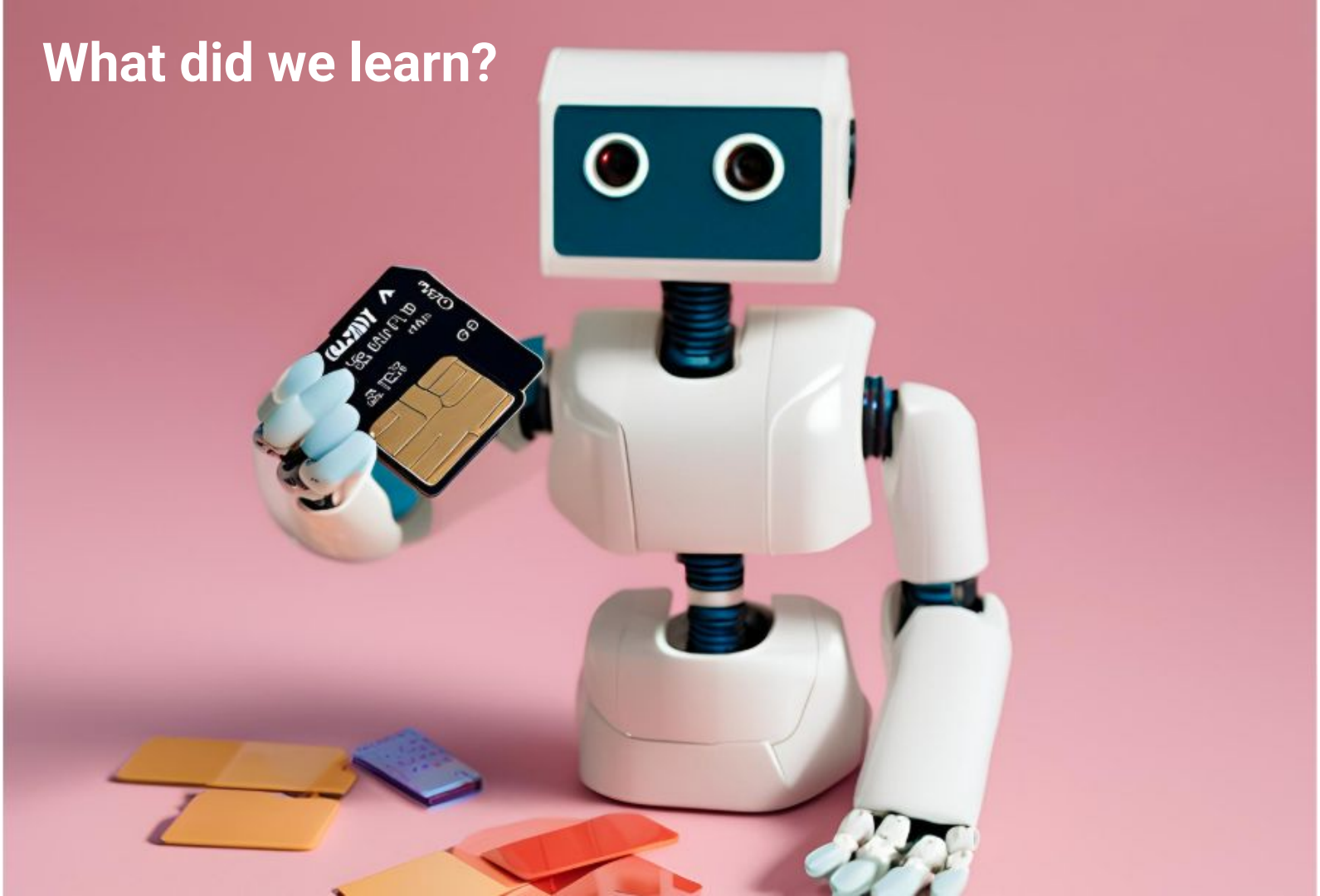


Source: https://www.defense.gov/Multimedia/Photos/igphoto/2003050362/

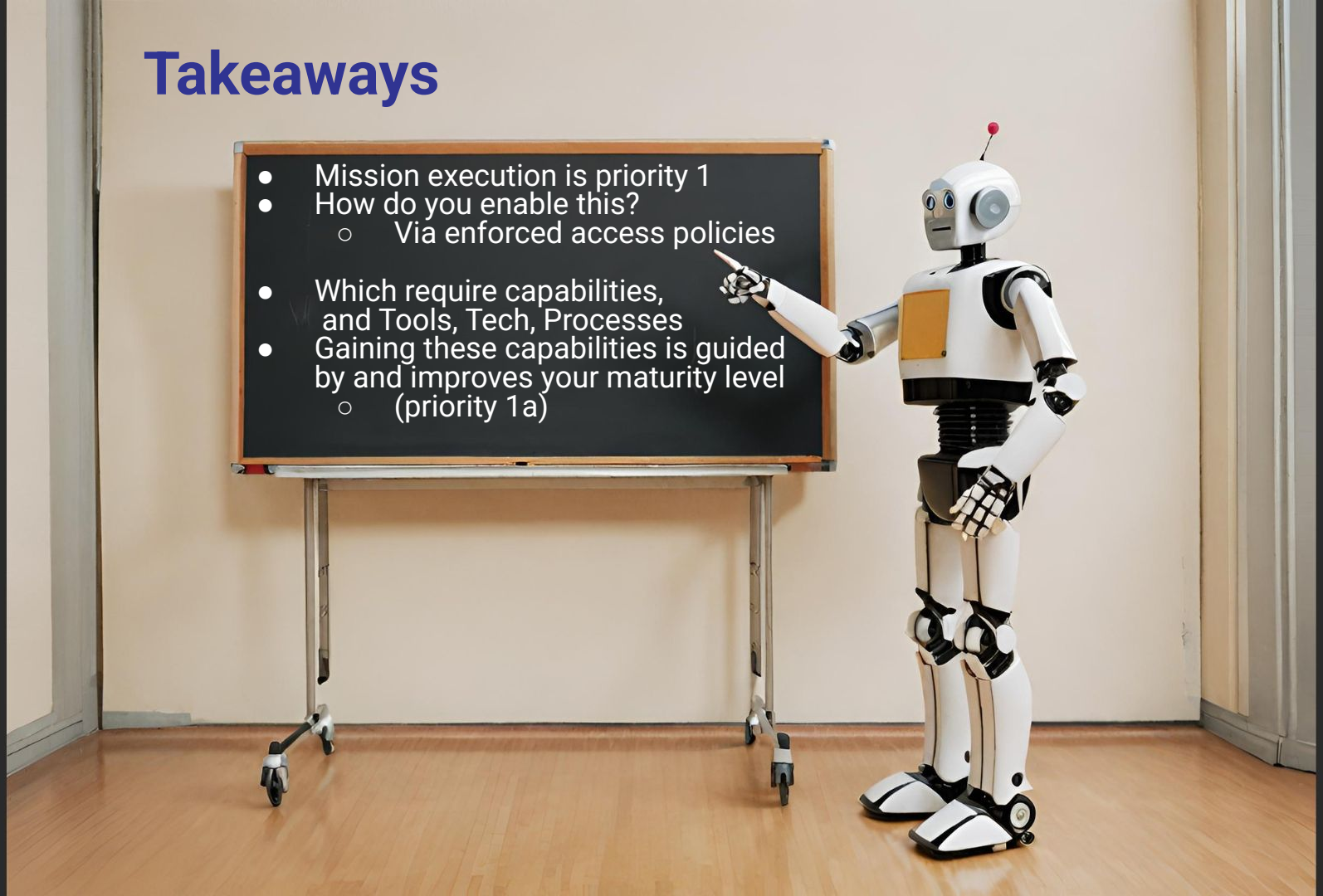
example

<< to be added>>

What did we learn?



Takeaways


Mission execution is priority 1
How do you enable this?
Via enforced access policies
Which require capabilities, and Tools, Tech, Processes
Gaining these capabilities is guided by and improves your maturity level
(priority 1a)

Thank You

Feedback or questions?

 Jason Garbis

 @JasonGarbis@infosec.exchange

www.NumberlineSecurity.com

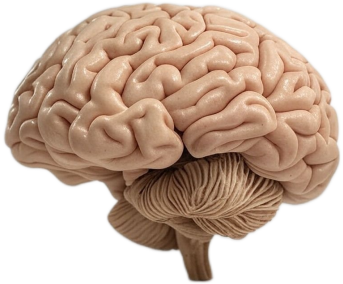
John Caballero


NSA
NSA
CYBER COMMAND
CYBER COMMAND
CYBER COMMAND
DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA
DIA
CYBER COMMAND
DARPA
3rd Annual DoD
ZERO TRUST
Virtual Symposium
DoD CIO ZERO TRUST
DATA
NETWORKS
ASSETS
APPLICATIONS
PORTFOLIO MANAGEMENT OFFICE
Join us April 2-4, 2025

Cyberpsychology, Cybersecurity and Maturing Zero Trust



- The term "Cyberpsychology" first appeared in 1998
- How people interact with online technology
- Cyberpsychology addresses the human factors
- It is now “The New Psychology”



Cyberpsychology Pioneers



Dr. Mary Aiken: Forensic Cyberpsychologist, author and Professor of Cyberpsychology at Capitol Technology University



Dr. Marshall S. Rich: Professor of Forensic Cyberpsychology and Senior Analyst for Operational Cyberpsychology at the U.S. Army Cyber Command (ARCYBER)

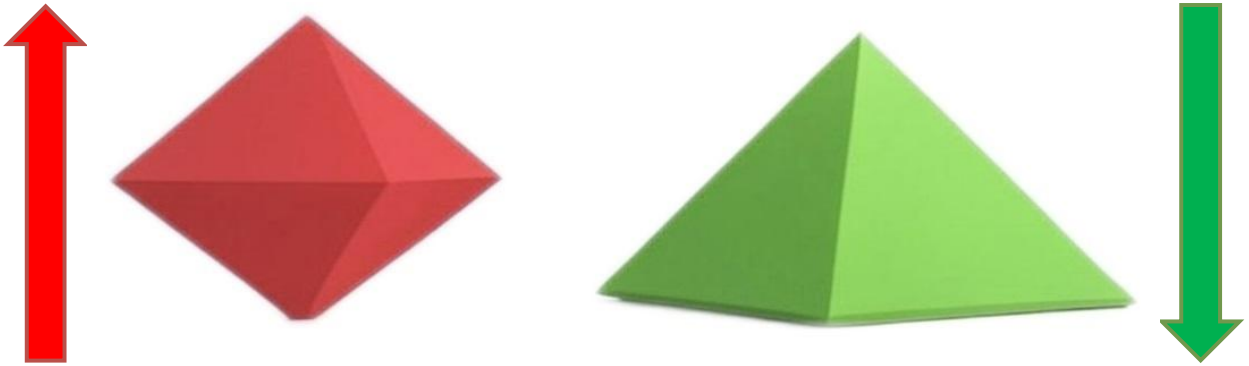




Leadership







Organization

Mindset Contributes Greatly to the Success or Failure of any Security Initiative

Technologies have limitations and may fail.

People, the weakest or strongest link?

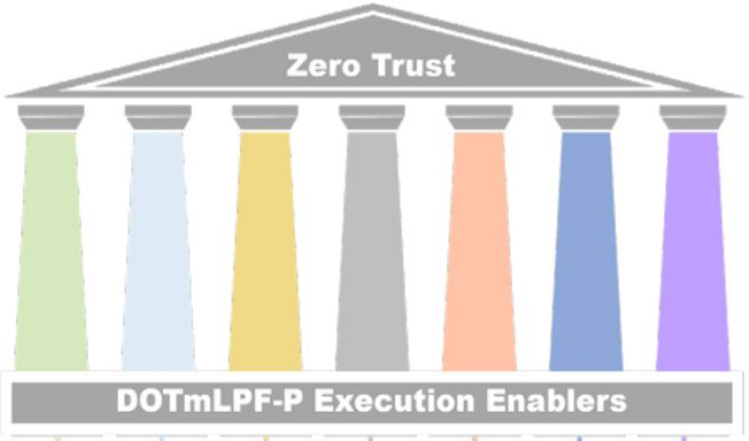
“People can also become a key security asset when they are properly trained and motivated to protect not only themselves but the security of the organization. It is important to not treat personnel as a problem to be solved, but as people who can become valued partners in a security endeavor.” Jen Easterly

Threats, a Growing Problem

ODNI'S 2025 ANNUAL THREAT ASSESSMENT: GLOBAL CHALLENGES FROM NATION-STATES AND TRANSNATIONAL CRIMINAL ORGANIZATIONS.

“IMPLEMENTING ZERO TRUST REQUIRES RETHINKING HOW WE UTILIZE EXISTING INFRASTRUCTURE TO IMPLEMENT SECURITY BY DESIGN IN A SIMPLER AND MORE EFFICIENT WAY TO IMPROVE WARFIGHTER PERFORMANCE." TIM DENMAN

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.

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.

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.

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.

EXECUTION ENABLERS Doctrine | Organization | Training | material | Leadership | Personnel | Facilities | Policy

Culture Supports Everything

(DoD Zero Trust Strategy, p. 10)

Jack Teixeira Pentagon Leak: Exposure of U.S. and Allied Intelligence Operations

Some causes:

- Excessive access privileges
- Inadequate supervision and monitoring
- Poor data exfiltration controls
- Failure to recognize social warning signs
- Leadership failed to act

US Treasury Breach: Compromised over 400 workstations and 3,000 files accessed

Some causes:

- Inadequate Monitoring and Detection: hackers operated outside normal hours to avoid detection
- Overreliance on External Cybersecurity Providers without stringent oversight
- Zero-Day Exploits and a lack of preemptive mitigation strategies

CIA Joshua Schulte spy case, sensitive data exfiltrated, including Vault 7 Hacking tools

Some causes:

- Poor Privilege and Access Controls
- Lack of Data Exfiltration Controls
- Cyber division had a culture of lax security
- No Employee Lifecycle Management Program

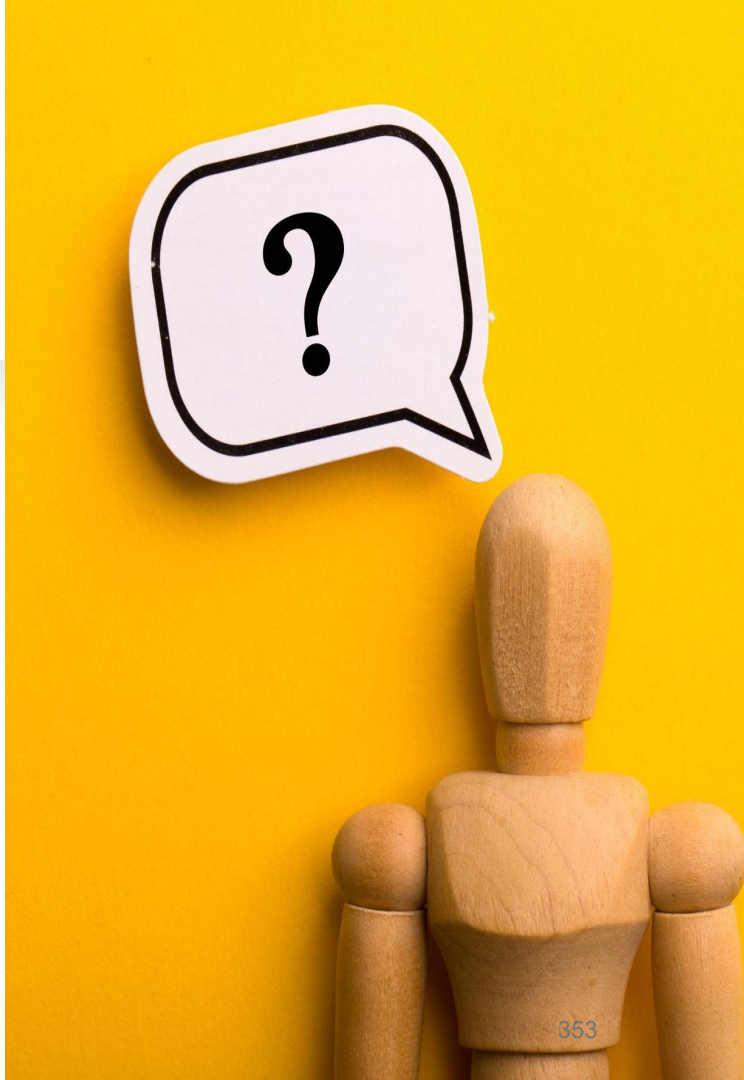


Why Did These Failures Occur?

We arrive at the intersection of cybersecurity and psychology

Were these incidents due to organizational culture or personal attitude?

- Preventing incidents requires shifting mindsets toward Zero Trust
- Cyberpsychologists and cybersecurity professionals stress the need to better understand how people interact with technology



Why Cyberpsychology Matters

There is a Relationship Between Cyberpsychology and Cybersecurity

Key Connections:

- Social Engineering and Human Vulnerabilities
- Behavioral Patterns in Security Practices
- Insider Threats and Workplace Security
- Trust and Risk Perception
- Designing Secure Systems
- Awareness and Training

SANS Institute 2024 Security Awareness Report

Human behavior is the top risk factor.

This requires changes to the organizational culture which must go beyond changing behavior.

It needs to involve changing the workforce's shared attitudes, perceptions, and beliefs about cybersecurity



The Human Factor

- CISO Online: Almost 1 million PCs compromised after users visited illegal streaming sites: Microsoft
- Gartner: 2022, 41% of employees engaged in Shadow IT, Forbes.
- By 2027, that number is expected to hit 75% for remote workers

Is it Time for Zero Trust?





How Do We Improve Zero Trust Adoption?

- Analysis
- Planning
- Action



Understand Target and Adversarial Thinking

The Intelligence Advanced Research Projects Activity (IARPA) ReSCIND Program

(Reimagining Security with Cyberpsychology-Informed Network Defenses)



IARPA

CREATING ADVANTAGE THROUGH RESEARCH & TECHNOLOGY



ReSCIND

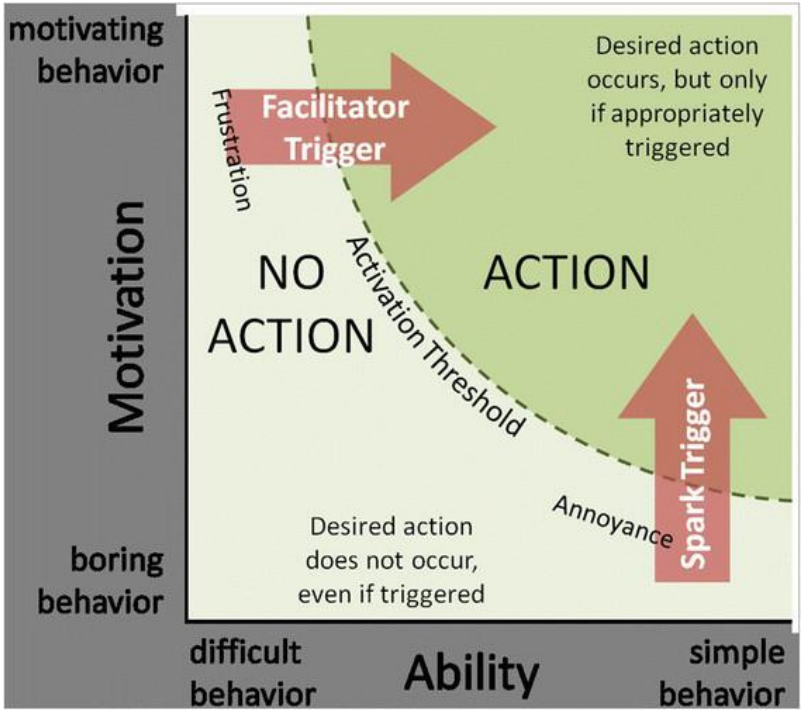
Consider Motivation and Ability

The Fogg Behavior Model

Motivation and Ability are predictors of the adoption of security initiatives

High motivation and ease of use lead to adoption

Low motivation and high difficulty lead to avoidance



Dr. BJ Fogg: Behavior Scientist and founder of the Behavior Design Lab at Stanford University, Graphic by Shih-Chung Jessy Kang

Consider the Human Factor

Unified Theory of Acceptance and Use of Technology (UTAUT/2)

- Performance Expectancy (PE)
- Effort Expectancy (EE)
- Social Influence (SI):
- Facilitating Conditions (FC)
- Behavioral Intention (BI)
- BI = PE + EE + SI + FC (Not weighted)

Russell, M. A. 2022. Dissertation: What are the Factors that Influence Consumers Use of Fully Autonomous Vehicles within the United States? Florida International University College of Business.
https://business.fiu.edu/academics/graduate/doctor-of-business-administration/docs/2022/michael-russell.pdf

Change the Mindset

Reactions to Cyber-social situations are pre-programmed

Dr. Erik Huffman: author of “Human Hacking: The Psychology Behind Cybersecurity

“Employees don’t have a sense of stranger danger”

Dr. Lee Hadlington: Nottingham Trent University and author of *Cybercognition: Brain, Behaviour, and the Digital World*

“People act in ways that are unpredictable, so while it’s great to have security technologies, it only takes one person to put the organization at risk”

Let's Build a Culture That Reduces Risk

Consider the Online Disinhibition Effect

Dr. John Suler: "ODE is where individuals exhibit less restraint in online interactions compared to face-to-face interactions"

Dr. Julie Ancis: "ODE creates a reduced behavioral inhibition and lowered regard for behavioral boundaries in cyberspace."

Risks of the Online Disinhibition Effect:

- Increased Risk of Social Engineering Attacks
- Weakened Security Compliance
- Insider Threats and Malicious Activity



How to Mitigate ODE in Cybersecurity

- Implement Cybersecurity Awareness Training
- Perform Simulated Tests
- Integrate Cyberpsychology into Zero Trust



Consider Emotional Intelligence (EI)

EI is the ability to recognize, understand and manage one's emotions

Adapting to Emotional Intelligence:

- Increase Cybersecurity Awareness
- Strengthen Security Culture
- Create Human-Tailored Security
- Create Behavior-Centric Training Programs
- Perform simulations



Verify then Trust?

User Behavior Analytics (UBA):

- Set Baselines
- Monitor for Anomalies
- Alert
- Remediate



How We Succeeded with Zero Trust at Florida's Economic Development Agency

- Created Policies
- Educated Organization Leaders
- Educated Staff
- Educated Partners and Vendors



Current Government Programs

- Intelligence Advanced Research Projects Activity (IARPA) – ReSCIND
- Minerva Research Initiative





Maturing Zero Trust at the Department of Defense

Building Zero Trust is Culture not just Technology

- Assume a hostile environment
- Presume breach
- Never trust, always verify

Understanding Cyberpsychology, we know human behavior is unpredictable

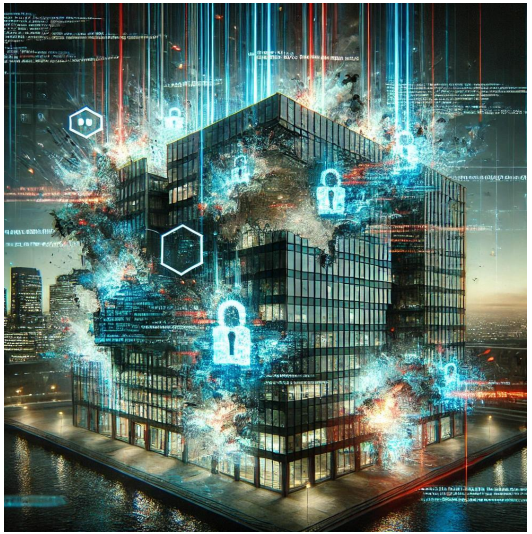


Cyber Losses

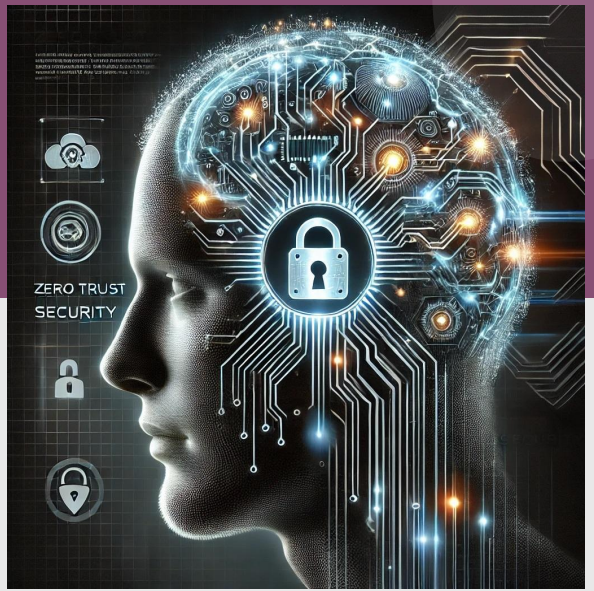
The 2024 worldwide cost of Cyber-incidents $9.5 Trillion

Total 2024 Department of Defense budget exceeded $800 billion

What would the cost be to your organization?



Zero Trust and Cyberpsychology



Cyberpsychology unlocks path to engaging the Zero Trust Mindset

2022 Department of Defense Zero Trust Strategy

- “Executing and achieving the objectives laid out in this strategy requires the coordinated efforts of the Joint Force and the entire defense ecosystem. Everyone in the Department has a role to ensure the success of ZT. While protecting data is central to ZT, successfully implementing our ZT Framework requires that the entire Department understands and embraces a culture of ZT.”

- “Cybersecurity in the world today is, by definition, a moving target, and while it may move, the concept and the culture will remain the same, even as the Department adapts and refines the strategy. Ongoing and open communication and coordination, underpinned by proper funding and resourcing, are key to the strategy's success.”



Adversaries are Not Stopping Their Attacks

Culture drives continuous improvement

Equip our Warfighters

Embrace Cyberpsychology awareness

Will Your Organization Be the Next News Story?









Want to learn more?



- Introduction to Cyberpsychology | Dr. Mary Aiken
- Using Psychology to Bolster Cybersecurity – RESCIND
- The Psychology of Cyberthreats | APA
- Cyberpsychology: Capitol Technology University

Les Call / Will Schmitt



FY25 DoD ZT "Under the Hood"

ZT PfMO DoD CIO(CS)

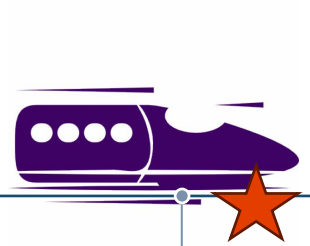
April 2025

Mapping the Journey

Instruction
- ***NDAA 2022***
- ***EO 14028***

Assessment methodology
- ***ZT RAT***
- ***ZT ROAM***
- ***Independent PTs***

Initiate Proof of Concepts



We are here

Policy Based Access Control (R/I/A)

DoD reaches Target Level

FY27

- ***ZT Strategy***
- ***ZT Roadmap***
- ***RMF Controls overlay***

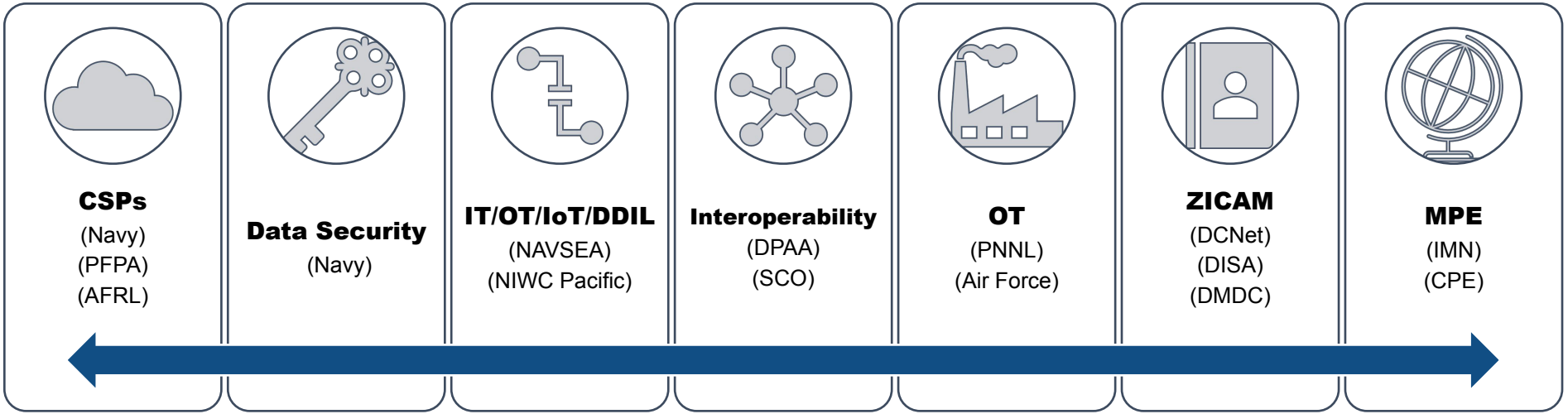
Guidance

- ***Culture change***
- ***Us versus Them***

Industry Engagement

Data Standard Prototype

ZT Proof of Concepts 2024 - 2026

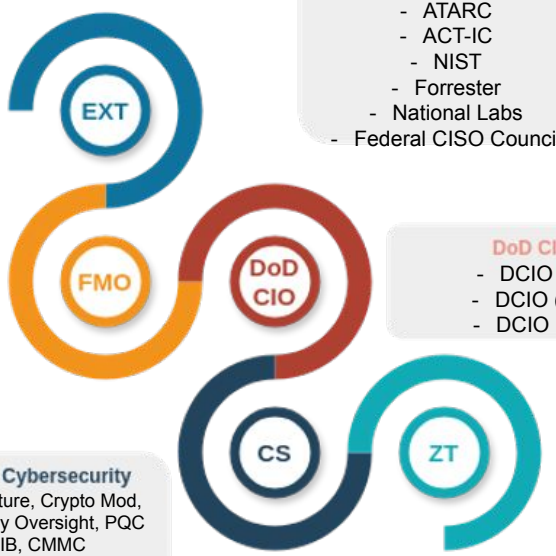


Let's Get Under The Hood!

Working Groups
- ZT Ecosystems
- ZT Attributes
- ZT Training
- CORA
- CNSS

External to DoD CIO
- NSA
- OUSD (A&S)
- ONCD
- DHS
- ADL
- AFRL
- OUSD (I&S)

Collaborations
- Open Framework
- CEDAR
- Cloud Security Alliance
- ATARC
- ACT-IC
- NIST
- Forrester
- National Labs
- Federal CISO Council



Component ZT Functional Management Offices
- OSD
- Joint Staff
- MilDeps
- CCMDs
- DAFAs
- Defense Agencies

DoD CIO
- DCIO (IE)
- DCIO (RA)
- DCIO (C3)

ZT PfMO
- Operations & Policy
- Strategy & Planning
- Technical Portfolio Mgmt

DoD CIO Cybersecurity
- Architecture, Crypto Mod, Capability Oversight, PQC
- DIB, CMMC
- Front Office
- Operations Support, Operations Risk Assessment, Cybersecurity Integration Policy and Strategy

Questions?

Questions, Comments, Concerns

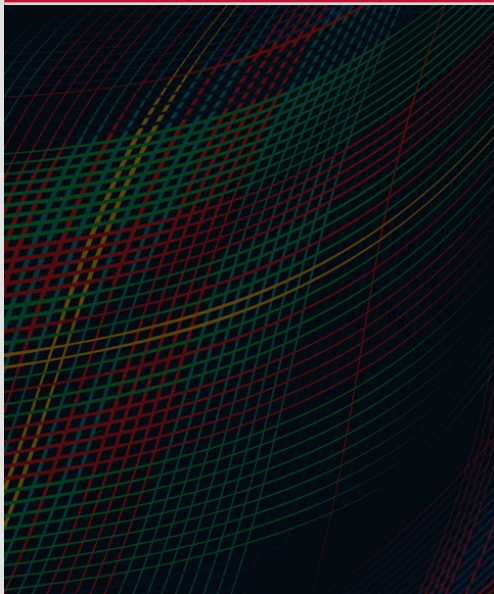
Greg Touhill

Carnegie Mellon University
Software Engineering Institute

Zero Trust For Everything

APRIL 3, 2025

GREG TOUHILL, CISSP, CISM, NACD.DC
BRIGADIER GENERAL, USAF (RET).
DIRECTOR, CERT DIVISION



© 2025 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Document Markings

Copyright 2025 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

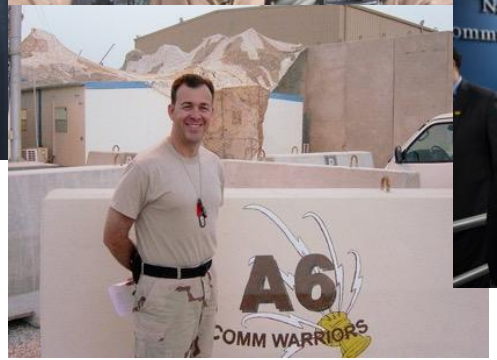
Notice to DoD Subcontractors: This document may contain Covered Defense Information (CDI). Handling of this information is subject to the controls identified in DFARS 252.204-7012 – SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING
WARNING - This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.). or the Export Administration Act of 1979, as amended, Title 50, U.S.C., App. 2401 et seq. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25.

DM25-0436

Who is this guy?















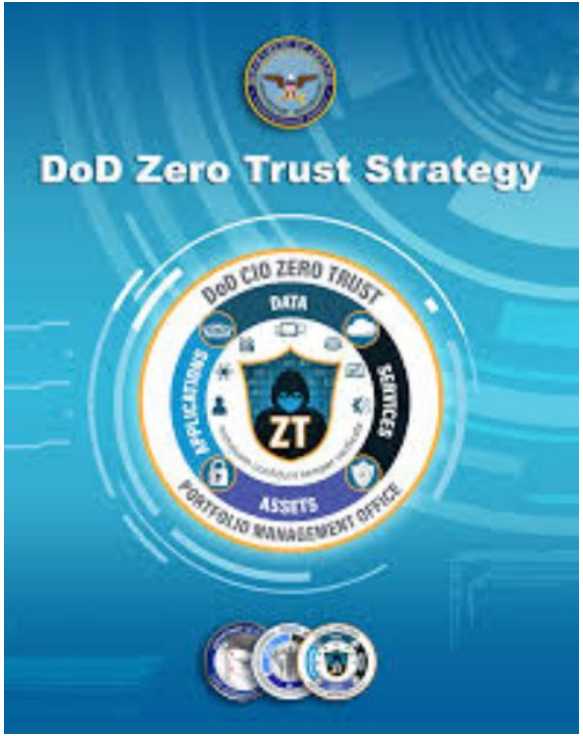
© 2025 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Our Current Vision for 2027

The Department of Defense's (DoD) risk-based Zero Trust Framework employed across the Joint Force and the defense ecosystem protects our *information systems* from increasingly sophisticated attacks as our adversaries seek to affect our warfighters and DoD mission success.

DoD ZT Strategy
21 Oct 2022



© 2025 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Zero Trust Is Not New



© 2025 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

An Alternate ZT Vision for Warfighters



Greg can only see what Greg is authorized to see…and nothing else

© 2025 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Other DoD Networked Computer Systems Need ZT Too















© 2025 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Don’t Forget OT, ICS, IoT Need Zero Trust too!



© 2025 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Zero Trust for AI? Absolutely!



Software

+



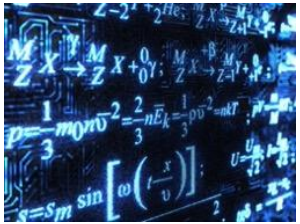
Data

+



Supply Chain

+



Algorithms

+



Infrastructure

= Risk Exposure

© 2025 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Actions for Successful ZT Execution

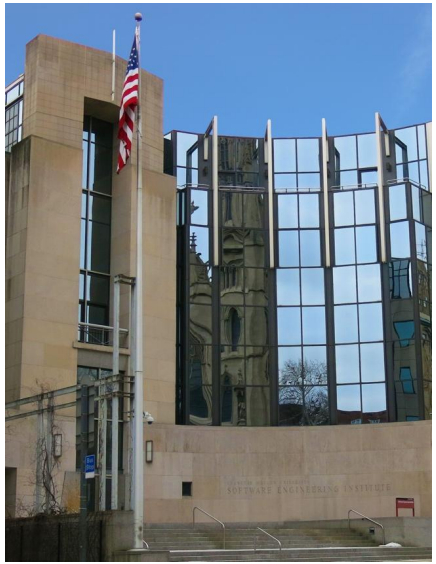
- Think and Act Like an Operator...think differently, move faster…and create decisive effects
- Out-think our adversaries…identify and manage mission risk
- Be like Admiral James T. Kirk: Work to protect the *entire* DoD Digital Fleet…and don’t be fixated solely on Enterprise IT
- Boxes don’t provide decisive advantage, data does...know your data
- Roles change. Identity Doesn’t. Define & Enforce Conditions and Entitlements
- Continually Test, Monitor, and Hunt for Signs of Trouble
- Mandate ZT requirements into acquisition and service contracts
- Complement with enhanced physical and personnel security controls
- Don’t be afraid to ask for help!

© 2025 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

CMU Software Engineering Institute (SEI)

Advances software as a strategic advantage for national security

Carnegie Mellon University Software Engineering Institute



- Serving the nation as a federally funded research and development center (FFRDC) sponsored by the U.S. Department of Defense (DoD)
- Leading and directing research and transition of software engineering and related disciplines at the intersection of academia, industry, and government
- Critical to the DoD's ability to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring

Carnegie Mellon University
Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, PA 15213
412-268-5800
gtouhill@cert.org

© 2025 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

DAY THREE

FRIDAY, APRIL 4TH

Al Kelly / Hieu Nguyen

State's Zero Trust Journey

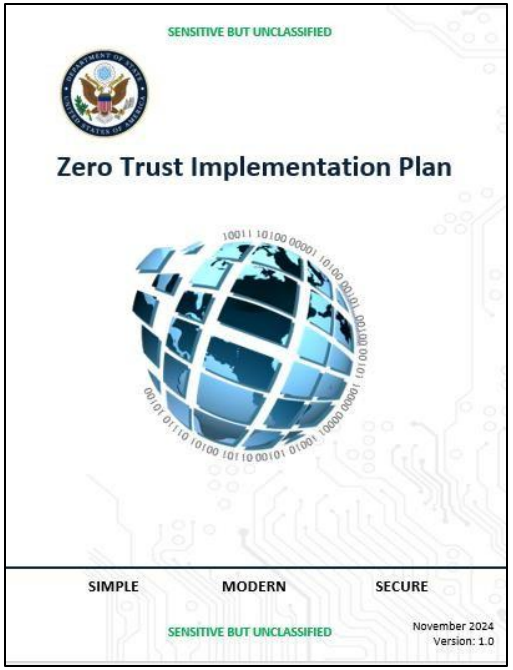
3rd Annual DOD Zero Trust Symposium

April 4, 2025

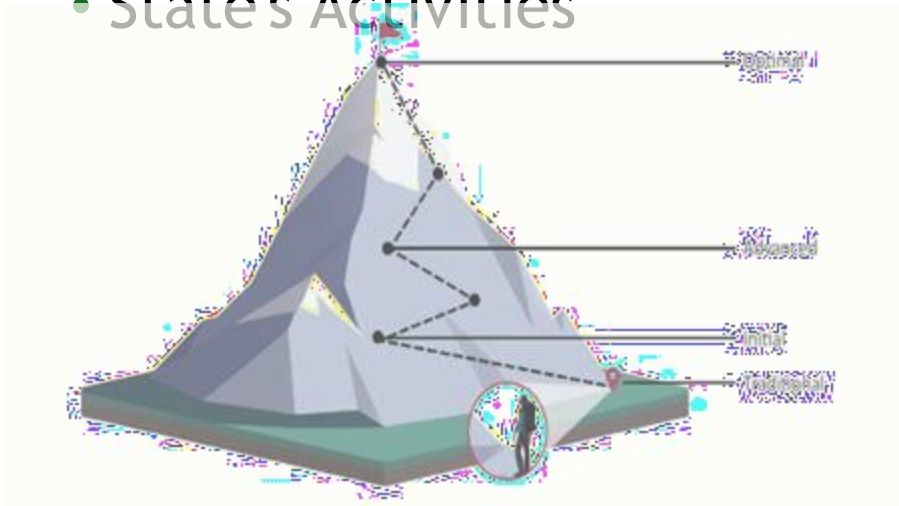
U.S. DEPARTMENT *of* STATE

TRADING PARTNER

Agenda



- Our Operating Environment
- Our Journey
- FY25-FY27 Roadmap
- State's ZT Maturity
- State's Activities



N C I A S S IFIED

TRADING PARTNER

Our Operating Environment

Strategic Approach:
- One size will not fit all
- Tailored approach and services to meet Bureau needs
- Established Working Groups

Vast Landscape:
- Over 270 global operating locations
- Over 230K Diplomats including:
  - Foreign Service
  - Local Employed Staff
  - Civil Servants
  - Other Government Agencies
  - Contracted work force

Mission Prioritization:
- Minimizing Bureau impact
- Collaborative communication

Legacy Technology Debt:
- Addressing legacy Technology
  - Diverse infrastructure/architecture
  - Local telephony services
  - Aging IT systems
  - Limited automation
  - Non-Friendly locations

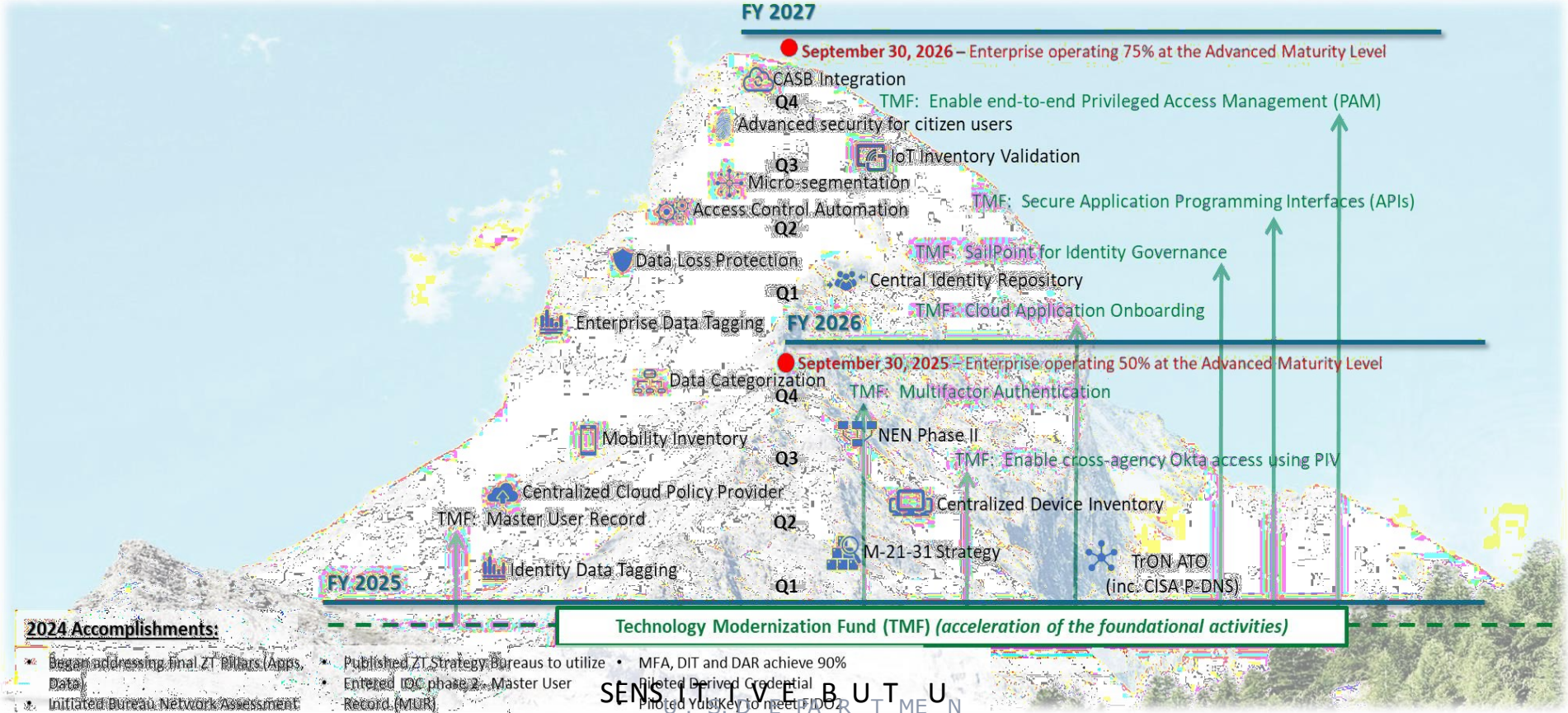
Governance:
- Navigating ever changing National and internation landscape
- Building upon Federal/International guidance and governance
- Inefficient processes

Simple, Modern, Secure environment empowering our diplomatic mission.

N_C_L_A_S_S_IFIED

TRADING PARTNER

Our Journey



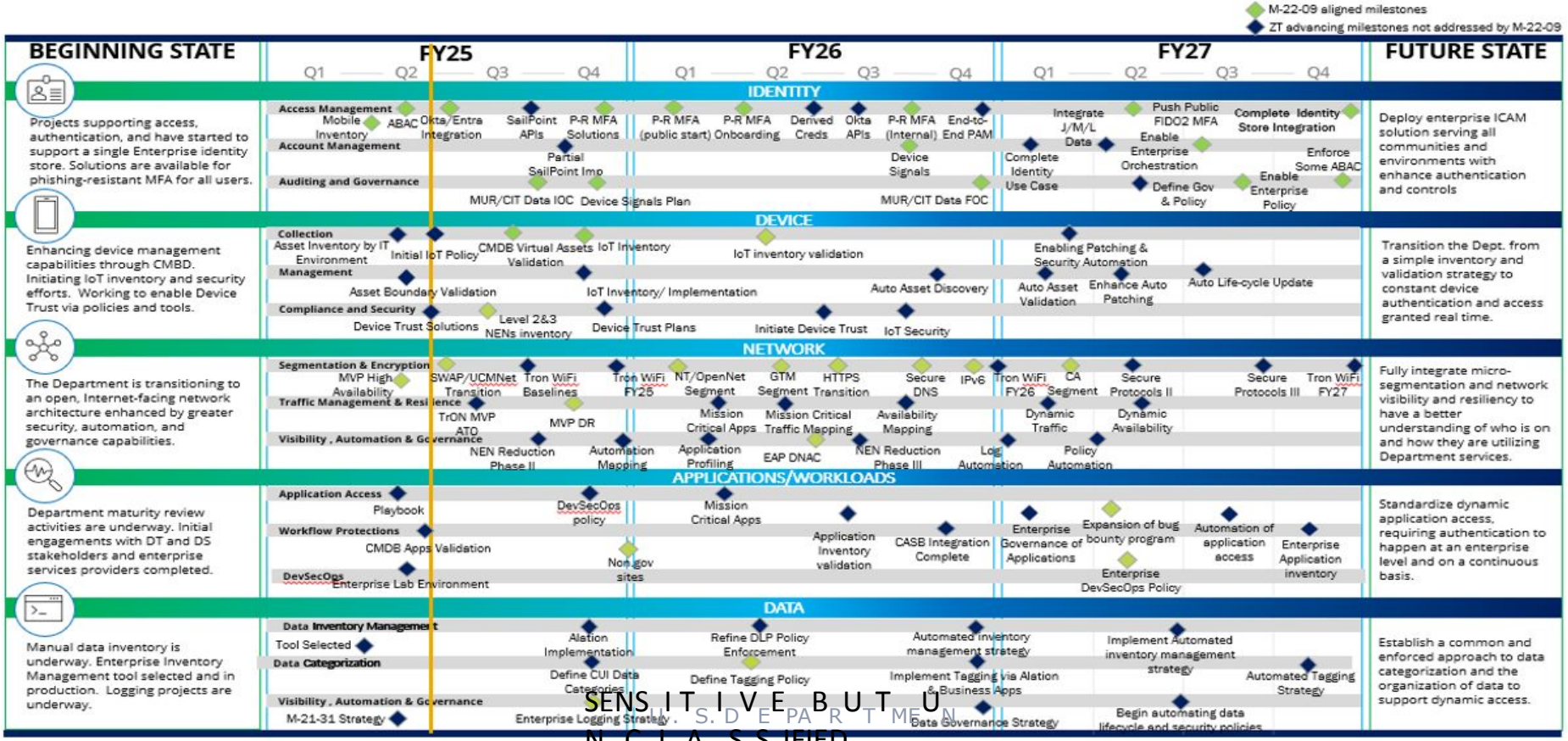
2024 Accomplishments:

- Began addressing final ZT Pillars (Apps, Data)
- Initiated Bureau Network Assessment Survey
- Published ZT Strategy Bureaus to utilize
- Entered IOC phase 2 - Master User Record (MUR)
- Single Sign On with Okta
- MFA, DIT and DAR achieve 90%
- Piloted Derived Credential
- Piloted YubiKey to meet FIDO2
- Enabled Data Classification (Microsoft)

SENSITIVE BUT UNCLASSIFIED

TRADING PARTNER

FY25 – FY27 Zero Trust Roadmap



SENSITIVE BUT UNCLASSIFIED
U.S. DEPARTMENT of STATE

TRADING PARTNER

Our Current Zero Trust Maturity

	IDENTITY	DEVICE	NETWORK	APPS & WORKLOADS	DATA
	MATURITY LEVEL **Advanced** **60%**	**MATURITY LEVEL** **Advanced** **54%**	**MATURITY LEVEL** **Advanced** **58%**	**MATURITY LEVEL** **Initial** **45%**	**MATURITY LEVEL** **Initial** **36%**
Optimal	○ Agency continuously validates Identity ○ Agency has global identity awareness	○ Agency constantly monitors and validates device security posture ○ Agency's access to data considers real-time analytics about devices ○ Agency integrates asset and vulnerability management across all agency environments, including cloud and remote	○ Agency network architecture consists of fully distributed ingress/egress micro-perimeters and deeper internal micro-segmentation ○ Agency integrates machine learning-based threat protection and filtering with context-based signals ○ Agency encrypts all traffic to internal and external locations, where possible	○ Agency continuously authorizes access to applications considering real time risk analysis ○ Agency strongly integrates threat protections into application workflows with comprehensive analytics ○ All applications are directly accessible to users over the Internet	○ Agency continuously inventories data with robust tagging and tracking. Agency augments categorization with machine learning models ○ Agency's access to data is dynamic, supporting just-in-time and just-enough principles,, and continual risk-based determinations ○ Agency encrypts all data at rest
Advanced	◑ Agency only authenticates identity using phishing-resistant MFA ◔ Agency consolidates and secures integration of identity stores ○ Agency performs automated identity risk assessments	◔ Agency employs compliance enforcement and tracking mechanisms for most devices and virtual assets ◔ Agency's access to data considers device posture on first access ◔ Agency uses automated methods to manage access, identify vulnerabilities, and patch assets	◔ Agency employs expanded isolation and resilience mechanisms ○ Configurations adapt based on automated risk-aware application profile assessments ◔ Agency encrypts applicable network traffic and manages issuance and rotation of keys	○ Most mission-critical apps are available to authorized users over public networks ◔ Agency has basic integration of threat protections into application workflows, primarily applying protections for known threats with some application-specific protections ◔ Agency has coordinated teams for development, security, and operations	○ Agency primarily conducts automated inventories with some tracking agency categorizes and labels data in a consistent, tiered, and targeted fashion ○ Agency governs access to data using automated context-based controls ○ Agency stores data in cloud or remote environments where they are encrypted at rest
Initial	● Agency uses both passwords and MFA ● Agency uses self-managed and/or hosted identity stores ● Agency conducts manual identity risk assessments ◑ User access expires with automated review	◕ Agency tracks all physical assets ● Agency has limited device-based access control and compliance enforcement ● Agency has some protections delivered via automation	● Agency has performed an initial isolation of critical workloads ● Agency's network capabilities manage availability demands for more applications ● Some portions of the agency's network feature dynamic configuration ● Agency encrypts more traffic and formalizes key management policies	● Some mission-critical workflows have integrated protections and are accessible over publish networks to authorized users. ◑ Agency uses formal code deployment mechanisms through CI/CD pipelines ● Agency performs static and dynamic security testing prior to deployment	◔ Agency uses limited automation for data inventory and access control ◔ Agency begins to implement a strategy for data categorization ◔ Agency has some highly available data stores ● Agency encrypts data in transit ◔ Agency implements initial centralized key management policies
Traditional	● Agency uses either passwords or MFA ● Agency only uses on-prem identity providers ● Agency makes limited determinations for identity risk	● Agency has limited visibility into device compliance ● Agency's access to data does not depend on visibility into the device that is being used to access the data ● Agency has a simplified and manually-tracked device inventory	● Agency defined their network architecture using large perimeter/macro-segmentation ● Agency bases threat protections primarily on known threated and static traffic filtering ● Agency explicitly encrypts minimal internal or external traffic	● Agency's access to applications is primarily based on local authorization and static attributes ● Agency threat protections have minimal integration with application workflows, applying general purpose protections for known threats	● Agency manually categorizes data and has poor data inventorying, leading to inconsistent categorization ● Agency governs access to data by using static access controls ● Agency primarily stores data in on-premises data stores and where they are unencrypted at rest

Key: ● Completed ◔ 25% Complete ◑ 50% Completed ◕ 75% Completed ◔ Updated within the last quarter

SENSITIVE BUT UNCLASSIFIED
U.S. DEPARTMENT OF STATE

TRADING PARTNER

State's Cross Pillar Activities

Identity Pillar Initiatives

Removal of Passwords: You are no longer required to remember passwords and change them.

Consolidated Identity Trust: Obtain access to department systems faster and with greater ease.

Phishing Resistant Multi-Factor Authentication: Access systems using a PIV card or alternative credentials to reduce the chances of someone accessing systems with your personal information.

Network Pillar Initiatives

Non-Enterprise-Network (NEN) Reduction: Offers you with a more dependable and secure infrastructure.

Encryption: Provides users with a more dependable and secure transaction of sensitive application data ensuring data integrity.

Segmentation: Ensure that applications are accessed by only authorized users and if a breach occurs, it cannot spread.

Device Pillar Initiatives

Configuration Management Database (CMDB): Assist with validating that only approved devices are operational within the environment.

Device Management: Ensure your devices are always compliant and updated for uninterrupted use.

Internet of Things (IoT): Provide a common strategy and enforcement of policies for IoT devices.

Data Pillar Initiatives

Inventory and Categorize: Provides users with an understanding of the Department's data, where it is stored and how it can be used.

Data Tagging: Develop and enforce a common enterprise approach for data tagging.

Data Loss Prevention (DLP): Prevent the loss of sensitive data while enforcing access controls to avoid department-wide impacts.

Application Pillar Initiatives

Migration to Cloud: Migrate on-prem application to cloud infrastructures to allow for greater security enforcement.

Cloud Access Security Broker (CASB): Assist with standardization, ease of authentication, and compliancy requirements for application owners.

Enforce DevSecOps: Enforce common security process to ensure standards throughout application lifecycles.

Cross Pillar Priorities

Enterprise Logging: Enterprise approach supporting the collection, consolidation, and analytics of Department logs.

Policy Enhancements: Enforce cyber policies, procedures, and processes to protect the Department's information.

Enterprise Automation: Integration of tools for improved decision support.

SENSITIVE BUT UNCLASSIFIED
U.S. DEPARTMENT of STATE

Larry Grate

Zero Trust Considerations for Critical Infrastructure

Larry Grate PE, CISSP, GICSP
Director of BD OT Infrastructure and Security

EOSYS
INVESTED IN YOUR SUCCESS



Larry Grate

Director of BD OT Infrastructure and Security

EOSYS

AGENDA

- Aspects of ZT deployment for CI/OT
  - OT definition from NIST SP800-37 Rev. 2:

    Programmable systems or devices that interact with the physical environment
- Considerations for deployment of ZT within CI
- Challenges of deploying ZT within CI

©2021 EOSYS | Confidential | For Internal Use Only

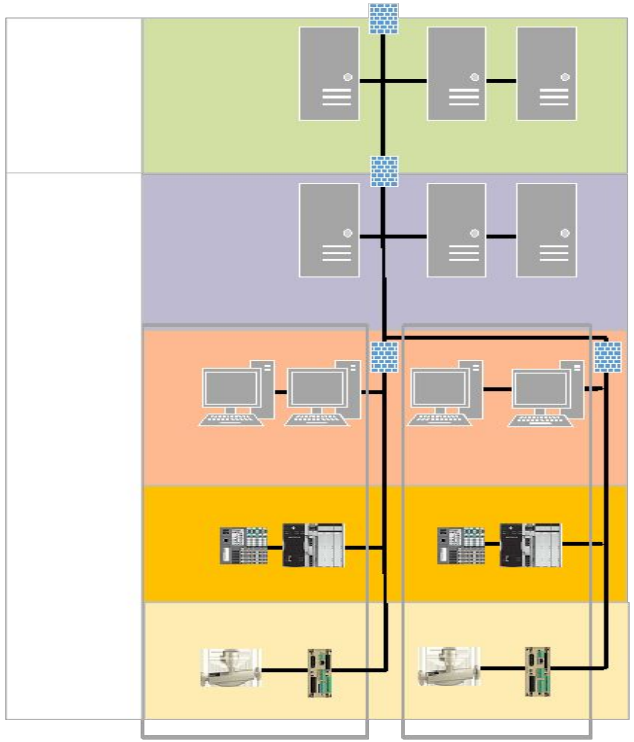
Aspects of ZT deployment for CI/OT

- What are your primary goals?
- What ZT Principles are you interested in?
  - No Implicit trust within network zone?
  - Identity-based authentication enforced at all connections?
  - Machine to Machine authentication/authorization?
  - Risk profiles on user and device behavior in near real time?
  - All sensitive data encrypted in transit and at rest?
  - All events continuously monitored, collected stored and analyzed?
  - Policy management and distribution being centralized?

©2021 EOSYS | Confidential | For Internal Use Only

Aspects of ZT deployment for CI/OT

- How did we get here?
- Types of OT Assets
  - Devices that don’t support Identity or Encryption
  - Devices that support Identity but not Encryption
  - Devices that support Identify and Encryption
- Level Definitions
  - Level 4 Enterprise
  - Level 3.5 iDMZ
  - Level 3 Site-Wide Supervisory
  - Level 2 Local Supervisory (HMI/UI)
  - Level 1 Controller (JACE, PLC, DCS, I/O)
  - Level 0 Field Devices (VFD, Smart Sensors)



©2021 EOSYS | Confidential | For Internal Use Only

Aspects of ZT deployment for CI/OT

- DoD Zero Trust Capabilities/Pillars
  - User
  - Device
  - Application & Workload
  - Data
  - **Network & Environment**
  - Automation & Orchestration
  - Visibility & Analytics

©2021 EOSYS | Confidential | For Internal Use Only

Network & Environment Pillar

NSA Advancing Zero Trust Maturity Throughout the Network and Environment Pillar – encourages the adoption of continuous identity and Micro-segmentation

NSA Model is challenging for most ICS/OT assets deployed at L0/L1

Considerations for ZT with CI

- Where do you start with Network & Environment pillar in OT?
- Identify your biggest risk/target within the system
  - OT starts with safety above all else:
    - FRCS Building system integration
    - ICS Machine Safety/Process Safety
    - Healthcare Equipment and Integration
  - Do you have sensitive data in your process?
  - Supply Chain considerations, are there critical missions that depend on CI?
  - Apply MITRE Crown Jewell Analysis

©2021 EOSYS | Confidential | For Internal Use Only

ZT Implementation

John Kindervag

“Don’t go too big too fast”

Find a strategy and a pace that works for you!

Considerations for ZT with CI

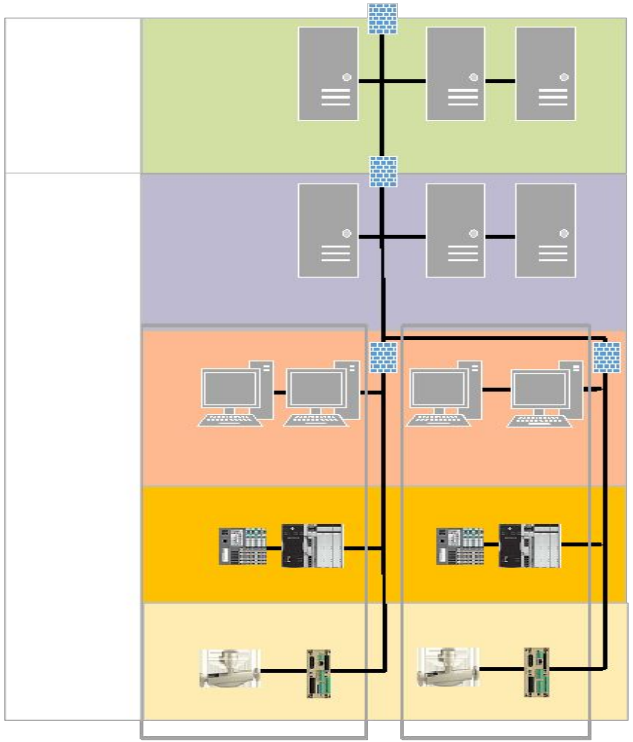
Network & Environment pillar

- Have your biggest risks now what?
  - Step 1 Macro-segmentation, use of Area/Zone/Cell model
  - Step 2 Micro-segmentation, use of SDN or device gateways
  - All while applying continuous authorization where possible
- Don’t forget CCE/CIE (What better way to do ZT)
  - Physical controls that prevent adversarial use of a digital system

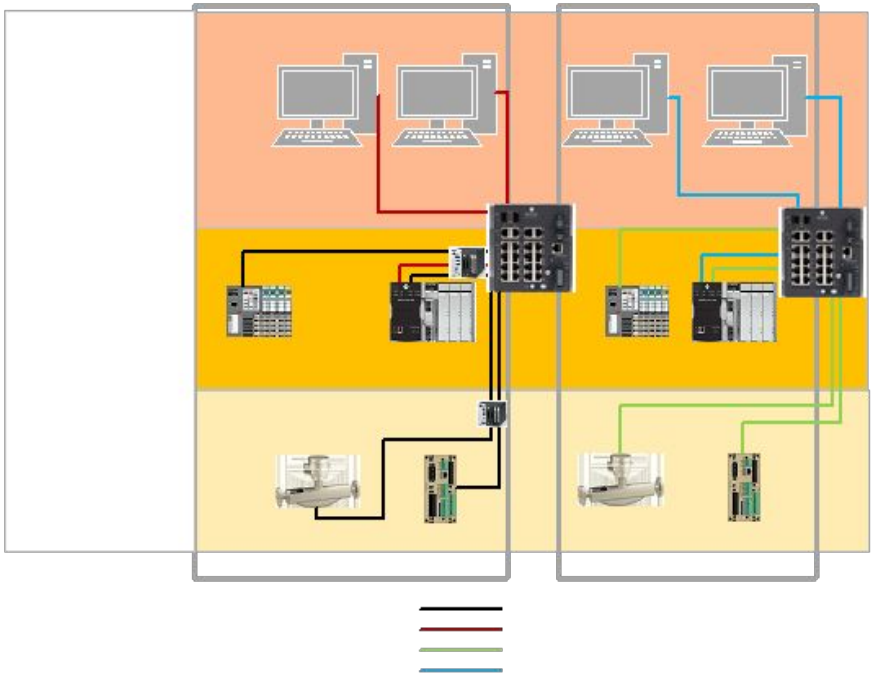
©2021 EOSYS | Confidential | For Internal Use Only

Considerations for ZT with CI

Macro:



Micro:



©2021 EOSYS | Confidential | For Internal Use Only

What about the other pillars?

Challenges Deploying ZT in CI

- New Installations (Greenfield)
  - Many new ICS platforms still don’t support authentication/encryption at the device level
  - Don’t forget security requirements in system requirements
  - Many CI OEM’s will not support unapproved agents installed on their platforms
- Legacy Systems/Upgrades (Brownfield)
  - Don’t have the concept of authentication or encryption natively in hardware
  - Many CI OEM’s will not support unapproved agents installed on their platforms
  - Often deployed with unmanaged network switches making segmentation difficult

©2021 EOSYS | Confidential | For Internal Use Only

Challenges Deploying ZT in CI

- Resiliency
  - IT can run a workload anywhere
  - CI/OT must interface with the physical world
    - Upgrades more expensive and require downtime
    - Can't move physical wires on the run
  - CI/OT systems sensitive to latency/jitter
    - Bigger issue the closer you get to Level 0 devices
  - Placing gateways or other ZT devices in front of legacy hardware will reduce reliability
- Downtime
  - Scheduling downtime for installation is challenging, no running upgrades
  - SOAR implementations may be unacceptably risky
    - Bigger issue at Level 0 then Level 3
    - No universal truths here, almost always system specific
- Support
  - CI/OT systems are already stretched thin for talent
  - Adding complexity makes finding appropriate resources more difficult
  - Skilled resources to architect and deploy ZT solutions are limited
- Cost
  - Budgets in OT/CI are tight
  - Don't forget ongoing support costs

©2021 EOSYS | Confidential | For Internal Use Only

Daniel Akridge

Don’t let your Zero Trust implementation cause you to have Zero Trust in your CI system.

GET IN TOUCH



Larry Grate
EOSYS
Larry.Grate@eosysgroup.com

THANK YOU!

Philip Griffiths

3rd Annual Zero Trust Symposium

Friday, April 4th

9AM - 12:30PM ET

Day #3 - Modernizing

Business Outcomes, Not Zero Trust:
Aligning Security with Real-World Needs
for OT and Weapon Systems

Co-Hosted By:



MIT Lincoln Laboratory

ATARC
Powered by GovExec

CSA cloud security alliance

DAU



Background







©2025 NetFoundry | netfoundry.io | Confidential & Proprietary. All Rights Reserved.

My experience



"I am not going to sell ZTA to my customers, I am going to sell IT/OT convergence, AI/ML, Digital Twins, and cloud!"

Head of Cyber for Portfolio

©2025 NetFoundry | netfoundry.io | Confidential & Proprietary. All Rights Reserved.

My talk – Putting the horse before the cart

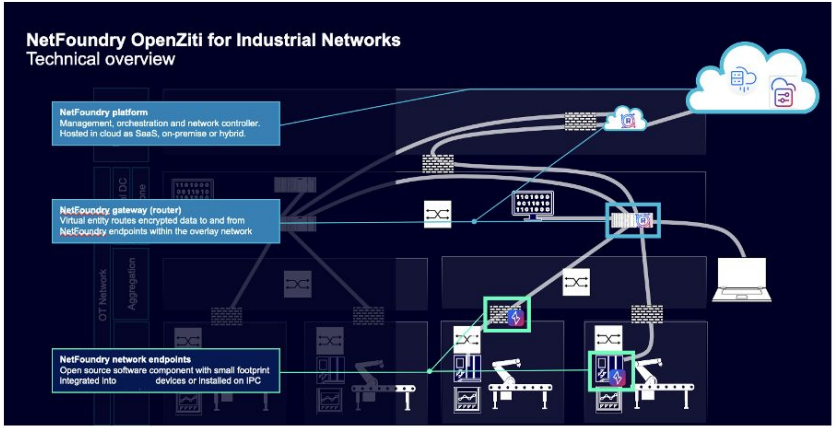
Business Outcomes, Not Zero Trust:
Aligning Security with Real-World Needs for OT and Weapon Systems

Using 4 real-world examples, using the following pattern:

- **Desire business outcomes**
- **Challenges:**
- **Solution**:

©2025 NetFoundry | netfoundry.io | Confidential & Proprietary. All Rights Reserved.

Industrial automation OEM



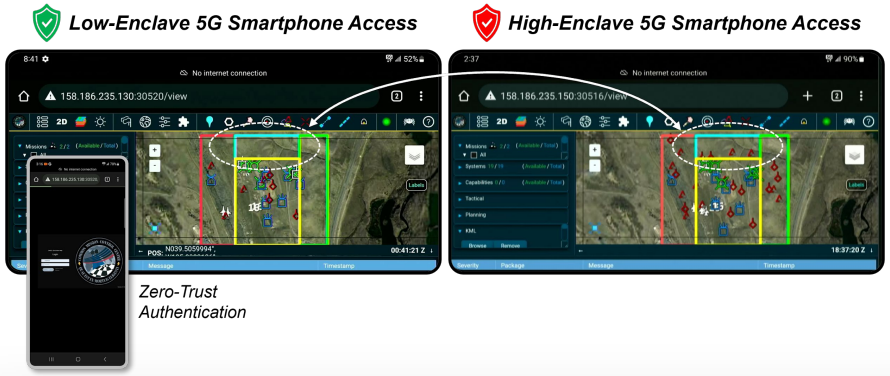
"Over 80% of traffic in a factory is M2M; we must be able to support any use case, not just SRA"

Leader for Zero Trust

- **Desire business outcomes:** Global industrial OEM wants to increase digitization & automation in their own factories & for products they sell to their customers.
- **Challenges:** (1) OT is unique, safety & availability are paramount, (2) compliance to 62443, (3) 'brownfield' and clientless, (4) need to coordinated and yet local control.
- **Solution**: ZTA Overlay embedded into their Industrial FWs, IPCs, PLCs, and more for supporting many use cases, built on OSS (so competitors can adopt).

©2025 NetFoundry | netfoundry.io | Confidential & Proprietary. All Rights Reserved.

Top U.S. military contractor



"the best adherence to NIST 800-207, including micro-segmentation and E2E encryption… with a breadth of architectures so we can run on anything. It includes its own CA/PKI to start without doing expensive integrations with ability to provide their own CA."

Technical Fellow

- **Desire business outcomes:** Provide secure, authenticated, encrypted access across warfighting domains with different security levels over a tactical 5G network.
- **Challenges:** (1) Guaranteed info segmentation (high-medium-low), (2) low SWaP-C tactical (mobiles, drones, etc), (3) DDIL & resilient system, (4) air gapped.
- **Solution**: ZTA Overlay embedded into cutting-edge commercial 5G with advanced defence tech, and for supporting many use cases, built on OSS.

©2025 NetFoundry | netfoundry.io | Confidential & Proprietary. All Rights Reserved.

Power utilities and grid

- **Desire business outcomes:** Grid integration/automation OEM wants to simplify inter-network coordination needs, particularly substations and DERs.
- **Challenges:** (1) Resolve challenge of legacy technology which is highly manual (expensive and unreliable), (2) difficult to audit and control, (3) alignment to NERC CIP
- **Solution**: ZTA Overlay embedded into their Distribution Mngt System, and more for supporting many use cases, built on OSS (so competitors can adopt).

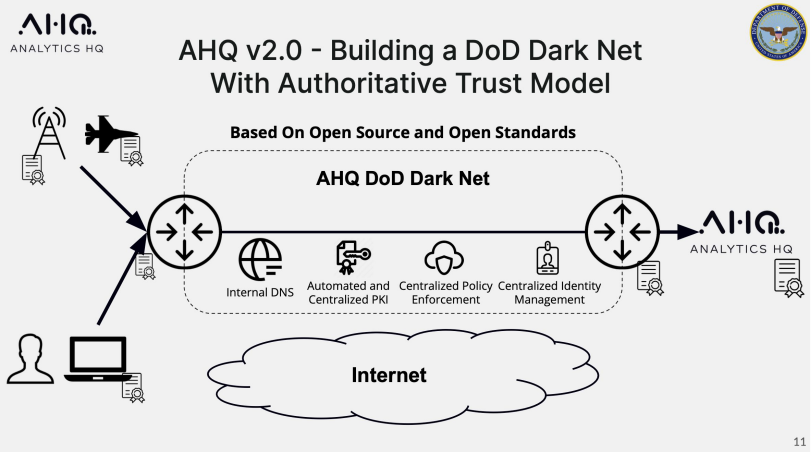


"We created a theoretical whitepaper on what 'service mesh for DER' should look like, it basically described OpenZiti before we knew Ziti existed"

Senior Engineer

©2025 NetFoundry | netfoundry.io | Confidential & Proprietary. All Rights Reserved.

Secure, Integrated Analytics.



"We can connect services, from K8S to legacy (non-K8S), with each service completely 'air gapped', 'dark' and Secure by Default"

Chad, CTO, OSSYS

- **Desire business outcomes:** OSSYS builds and operates AHQ for advanced analytics and insights
- **Challenges:** (1) Secure/privately ingest external data sources, (2) needs to support edge, to cloud, to IoT, (3) requires secure-by-default security model
- **Solution**: ZTA Overlay embedded into their AHQ Platform (KubeZT), and more for supporting many use cases, built on OSS (so competitors can adopt).

©2025 NetFoundry | netfoundry.io | Confidential & Proprietary. All Rights Reserved.

Other use cases

- **Public safety operations platform:** To connect legacy workload to their cloud, they want a SW-only, outbound & private network solution, instead of shipping dedicated HW to each customer.

- **Marposs:** Developed new Digital Grid product, which needed secure operational access to customer manufacturing sites. Purdue requirements mandated private, outbound only solution.

- **Industrial automation leader (grid):** Fleet Management system for Energy Distribution Systems requires varied connectivity needs. Wanted it to be “baked in” rather than bolted on VPN, while providing “maximum efficiency of managing the connection security”

- **Cloud Hyperscaler:** Wants to replace 150k Cisco AnyConnect and ICE while being feature parity. Needed alignment to zero trust as well as ability to support future multi-cloud use cases, and sell to their customers.

©2025 NetFoundry | netfoundry.io | Confidential & Proprietary. All Rights Reserved.

Summary and takeaway

“I am not going to sell ZTA to my customers, I am going to sell IT/OT convergence, AI/ML, Digital Twins, and cloud!”

Head of Cyber for Portfolio



©2025 NetFoundry | netfoundry.io | Confidential & Proprietary. All Rights Reserved.

Andy Ellis

Zero Trust Leadership Small changes, Big outcomes

Andy Ellis
Partner, YL Ventures



Andy Ellis

www.csoandy.com

@csoandy

Partner
YL Ventures

Author
1% Leadership

2021 inductee
CSO Hall of Fame

Podcast Co-host
CISO Series

CEO/Principal
Duha

Former CSO
Akamai

Former Officer
US Air Force

Graduate – CS/Math
MIT

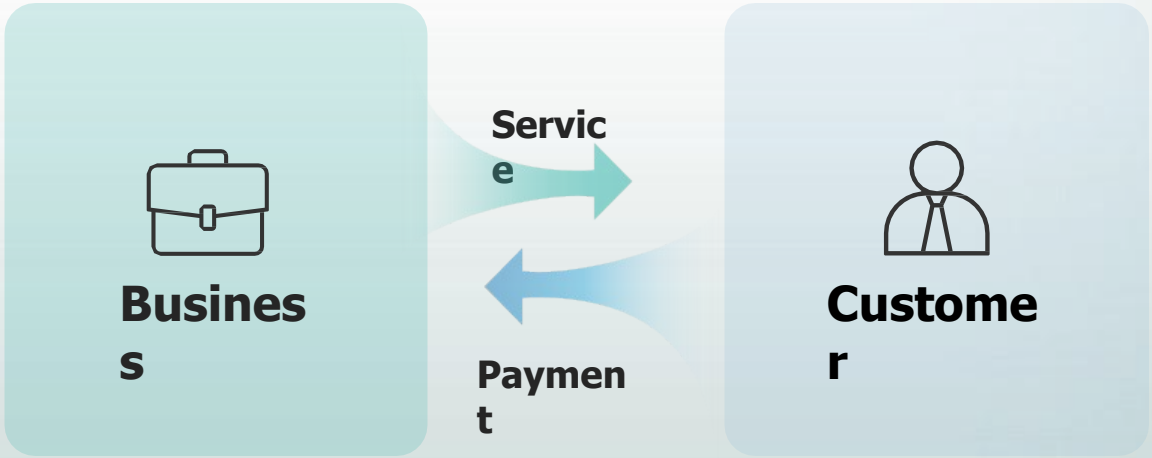
Spirit of Disneyland
Disneyland

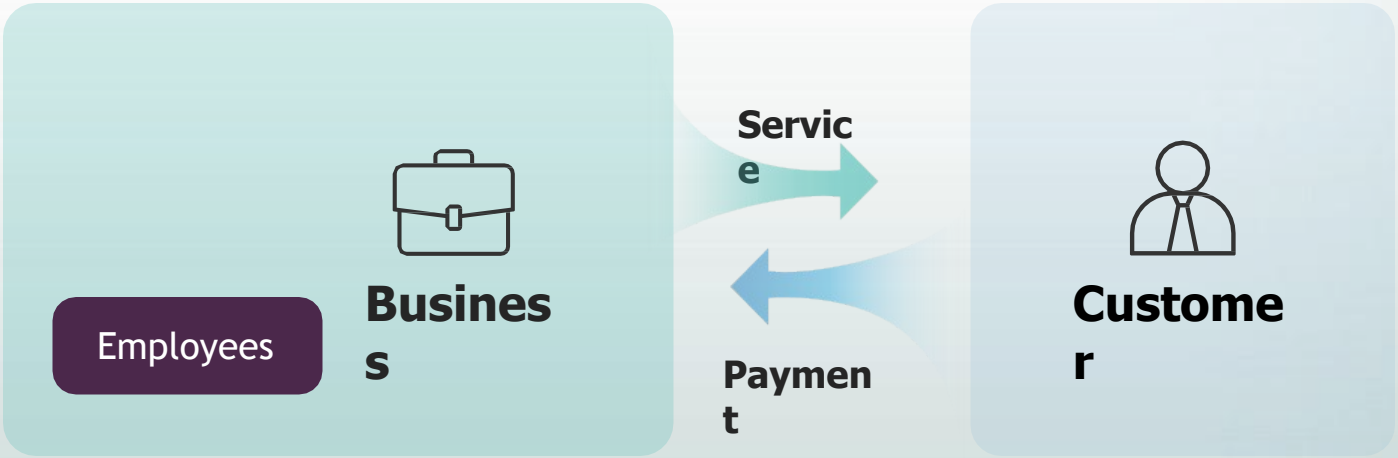
Award of Excellence
Wine Spectator

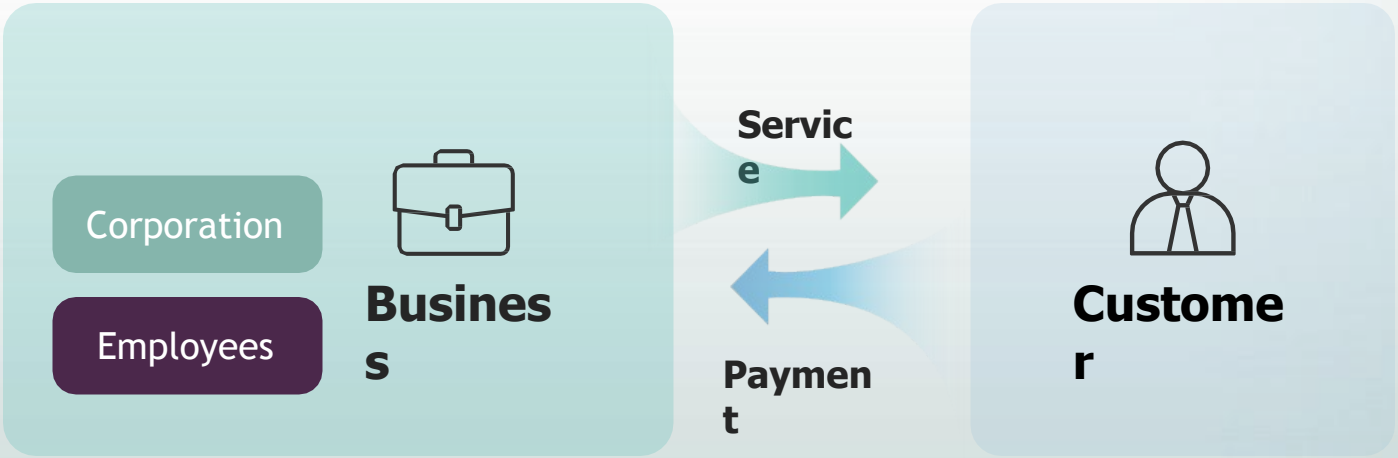
A Brief History of Trust

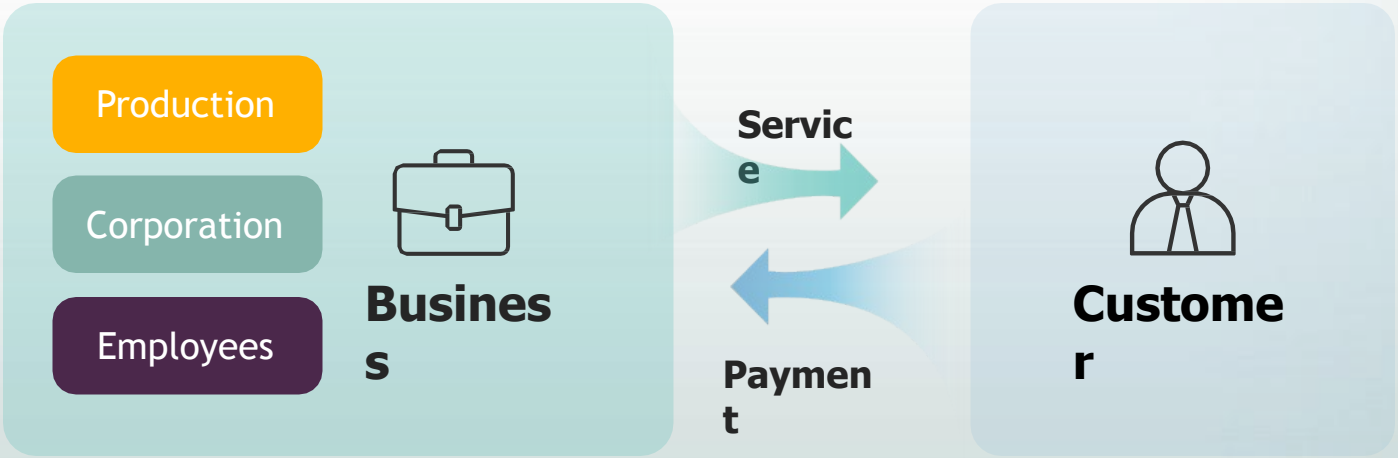
A Brief History of IT

A Brief History of Business


Business
Service
Payment
Customer

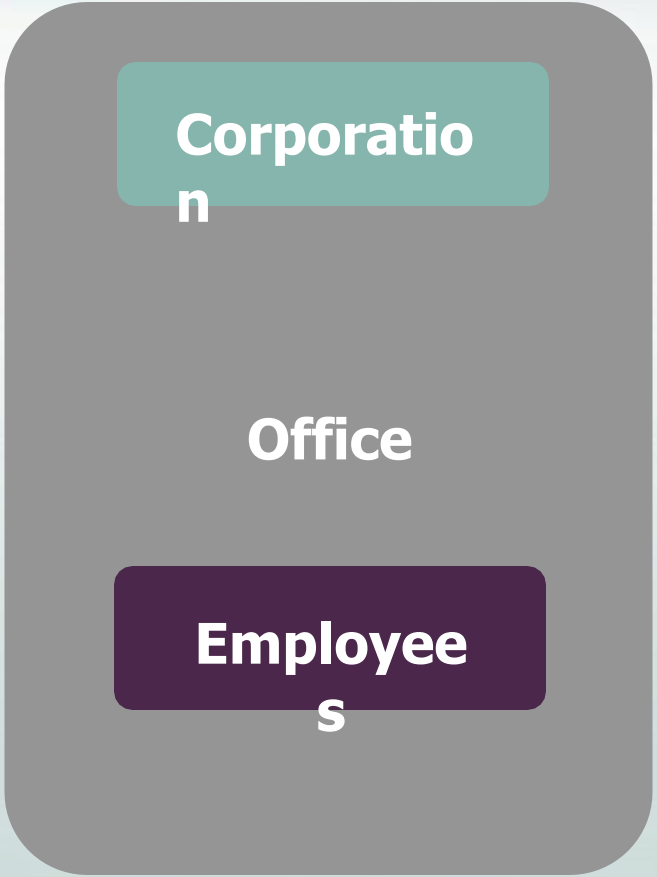

Employees
Business
Service
Payment
Customer

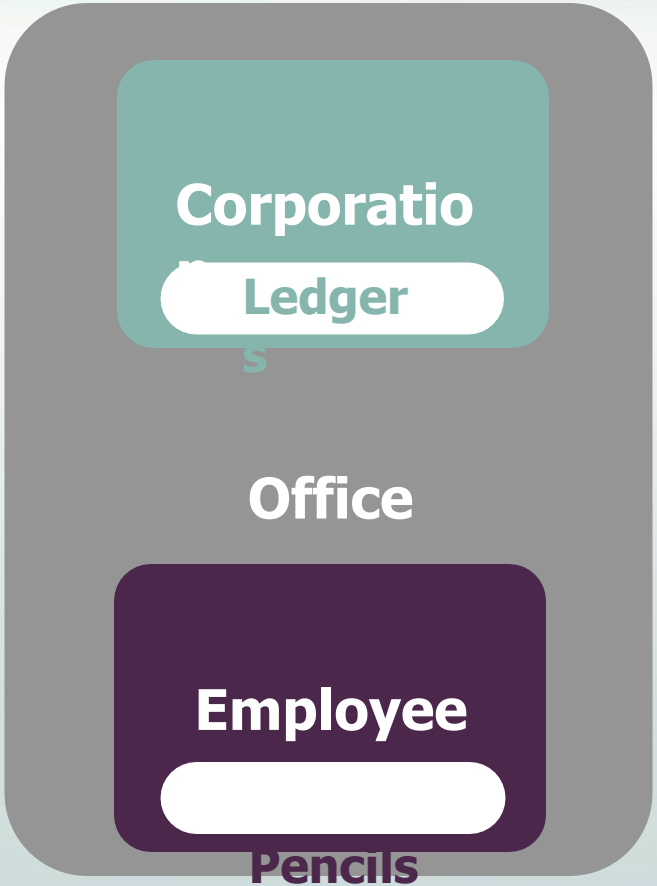

Corporation
Employees
Business
Service
Payment
Customer


Production
Corporation
Employees
Business
Service
Payment
Customer

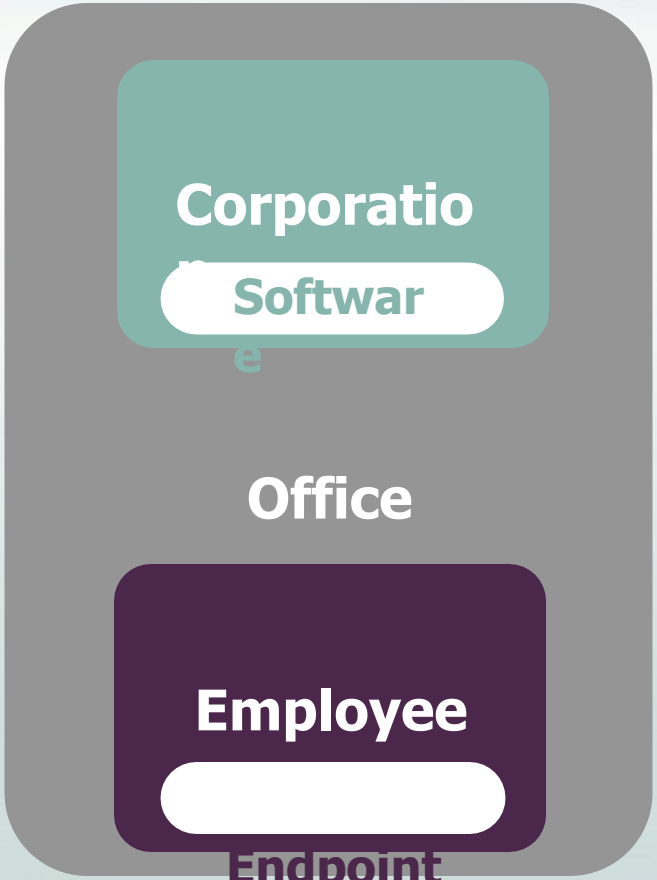
Corporation

Employees

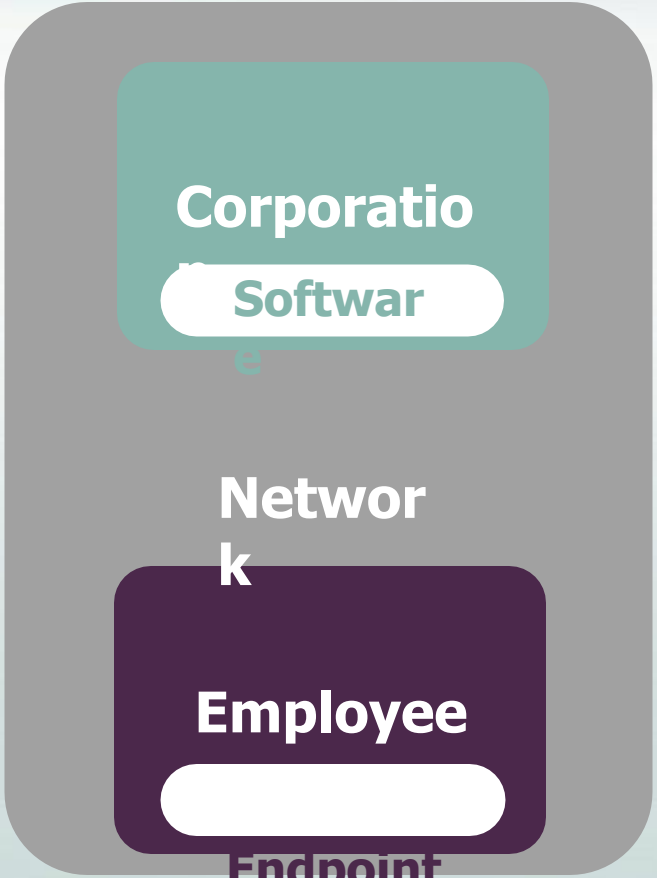

Corporation
Office
Employees



YL VENTURES



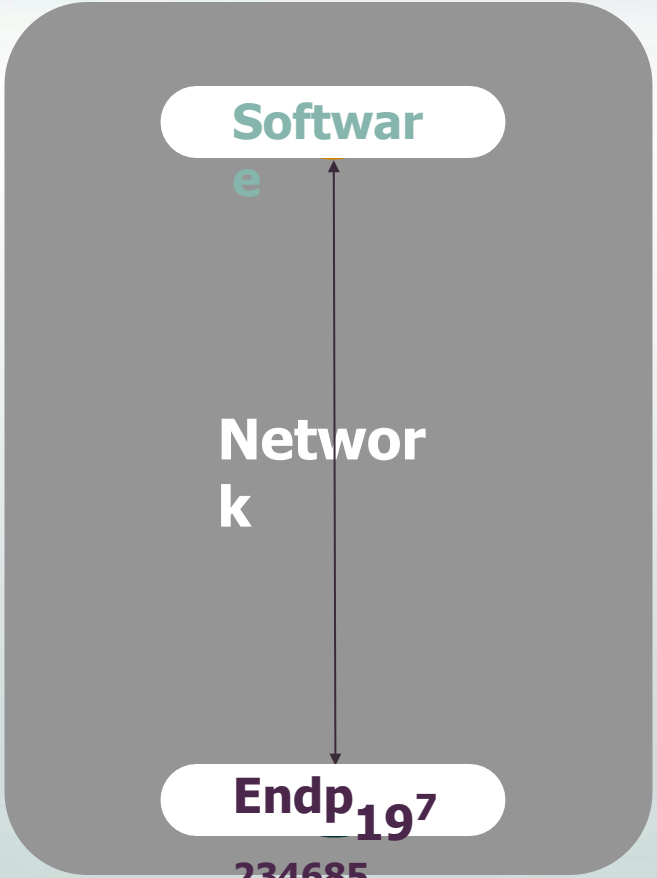
YL VENTURES



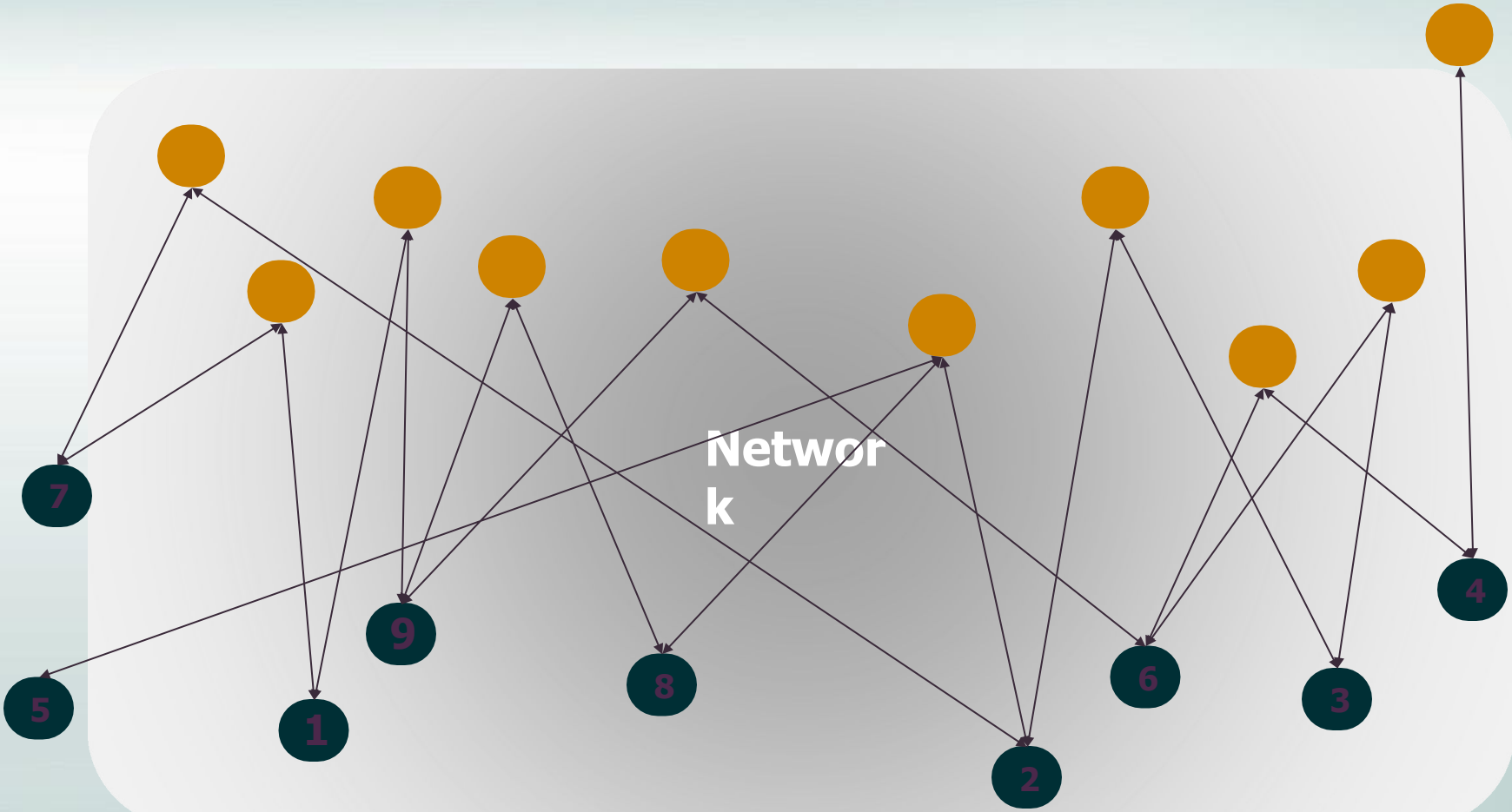
YL VENTURES



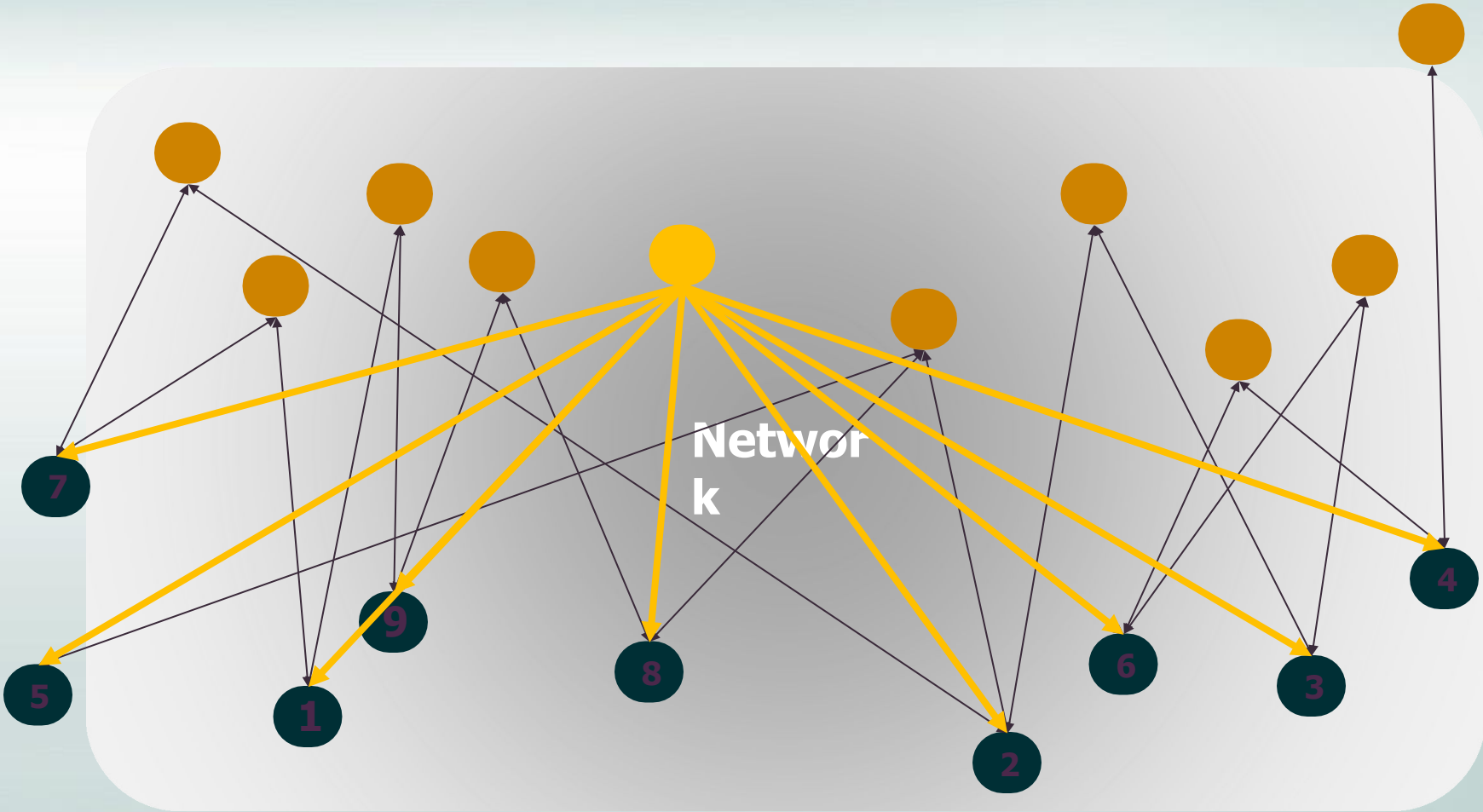
YL VENTURES



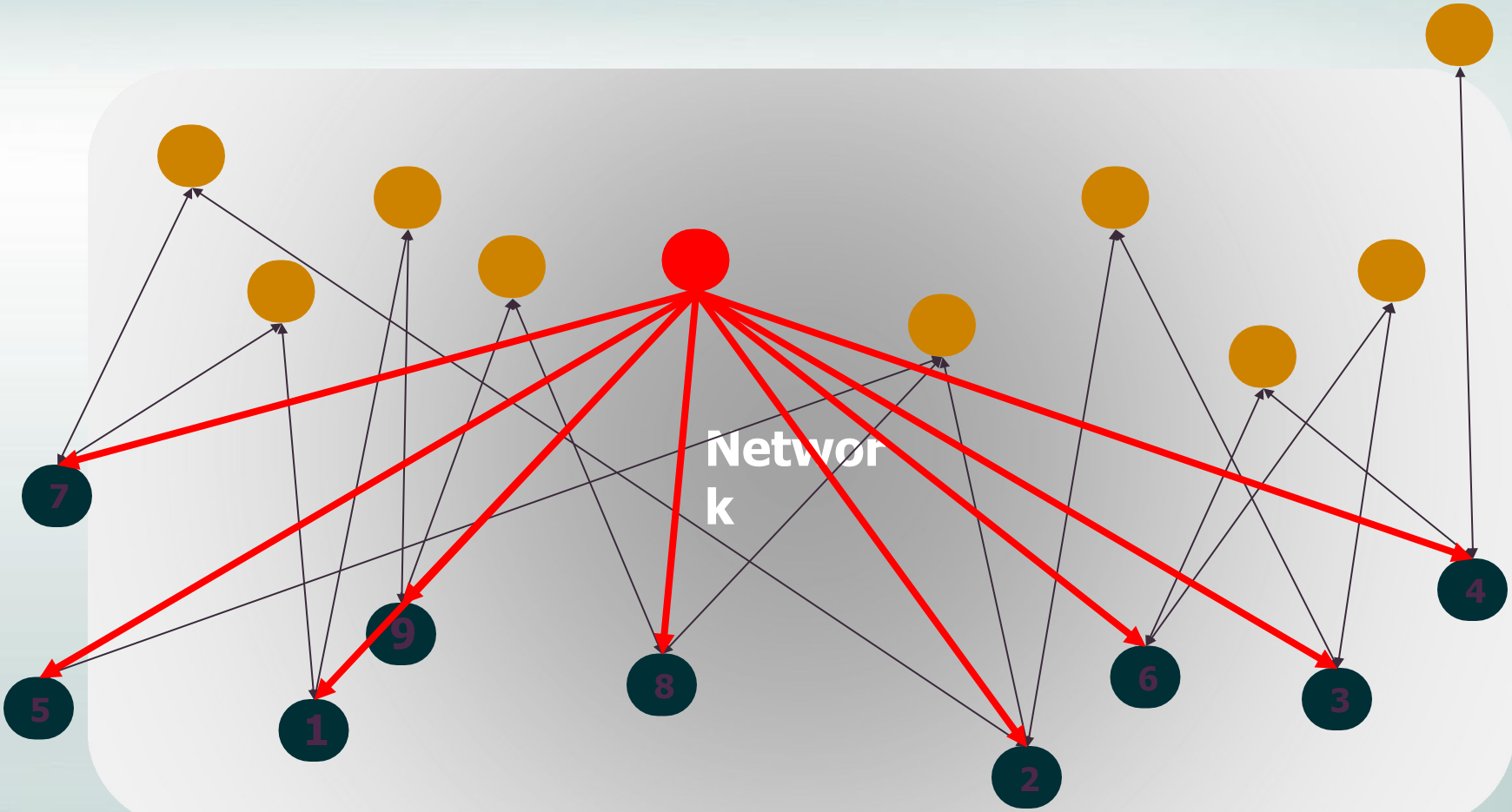
YL VENTURES



YL VENTURES



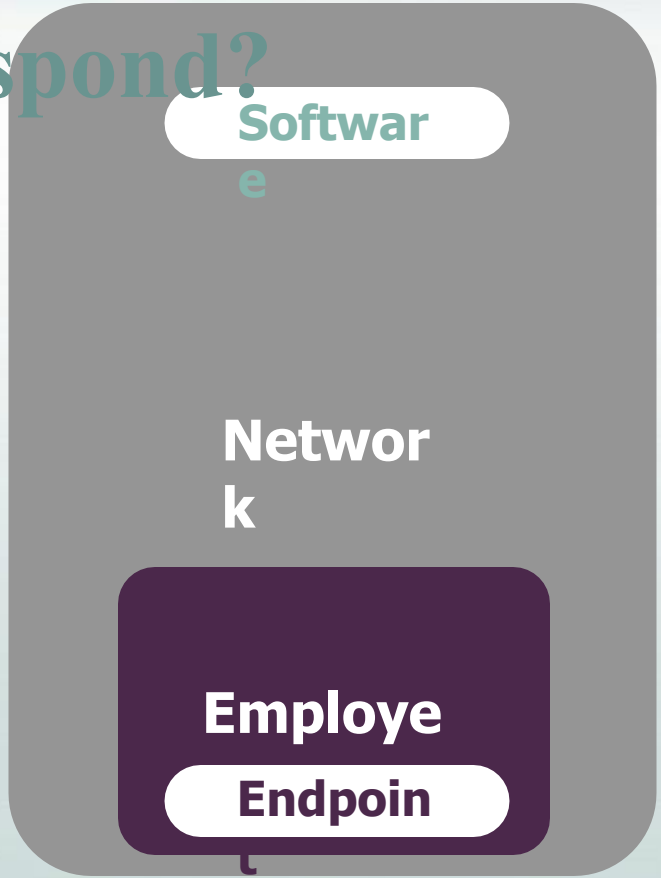
YL VENTURES



YL VENTURES

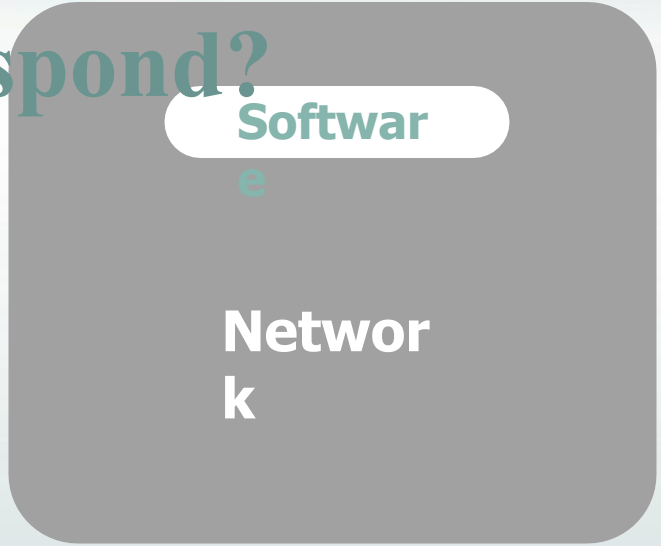


How did we respond?



YL VENTURES

How did we respond?

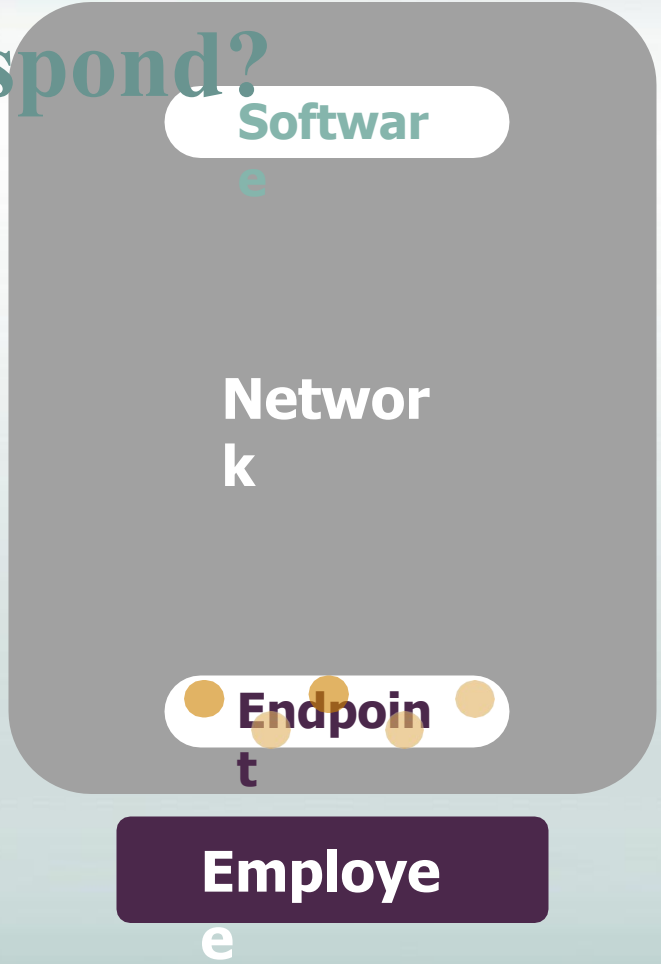


We *should* have removed trust on the endpoint

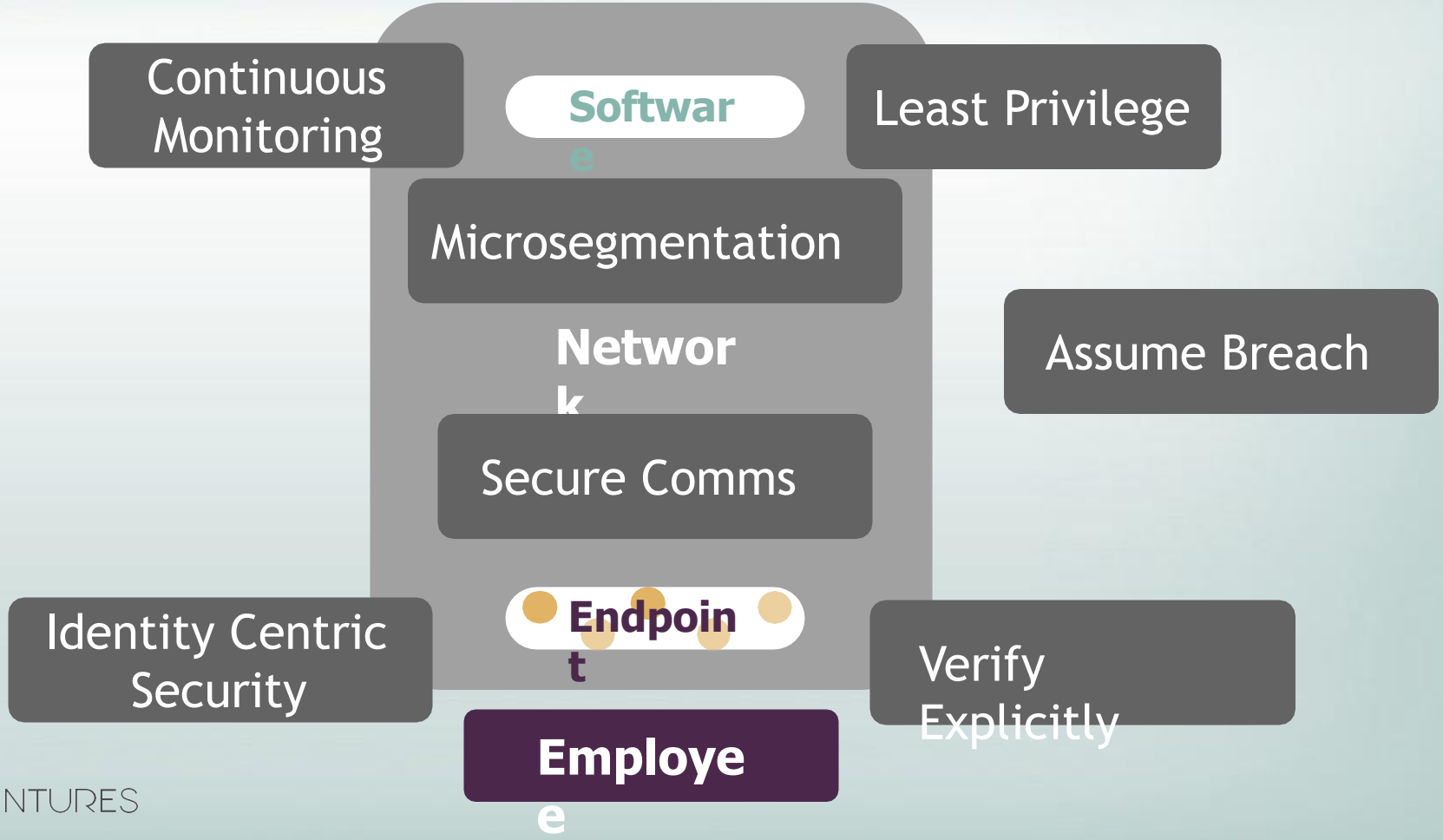


How did we respond?

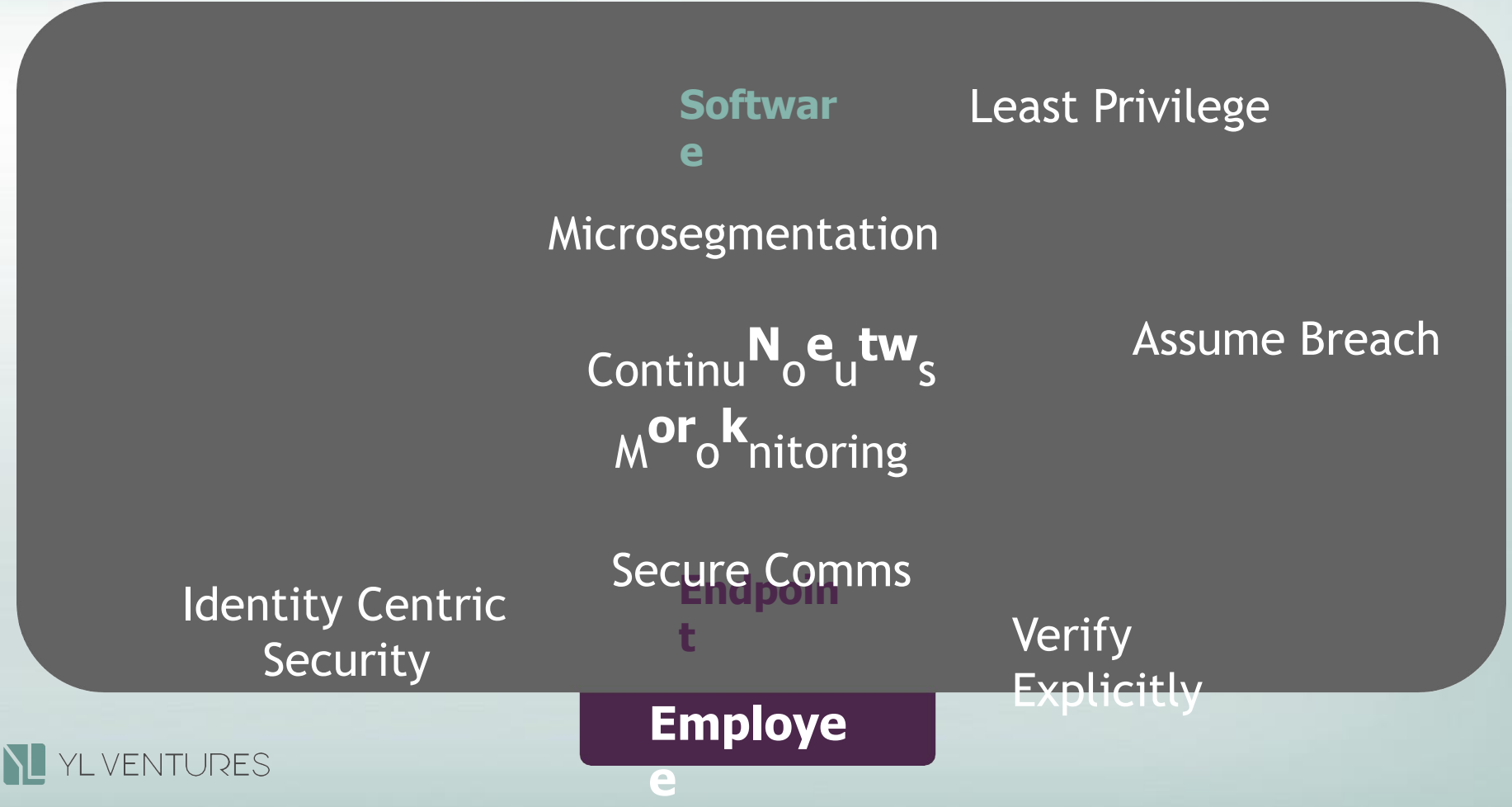
We *should* have removed trust on the endpoint



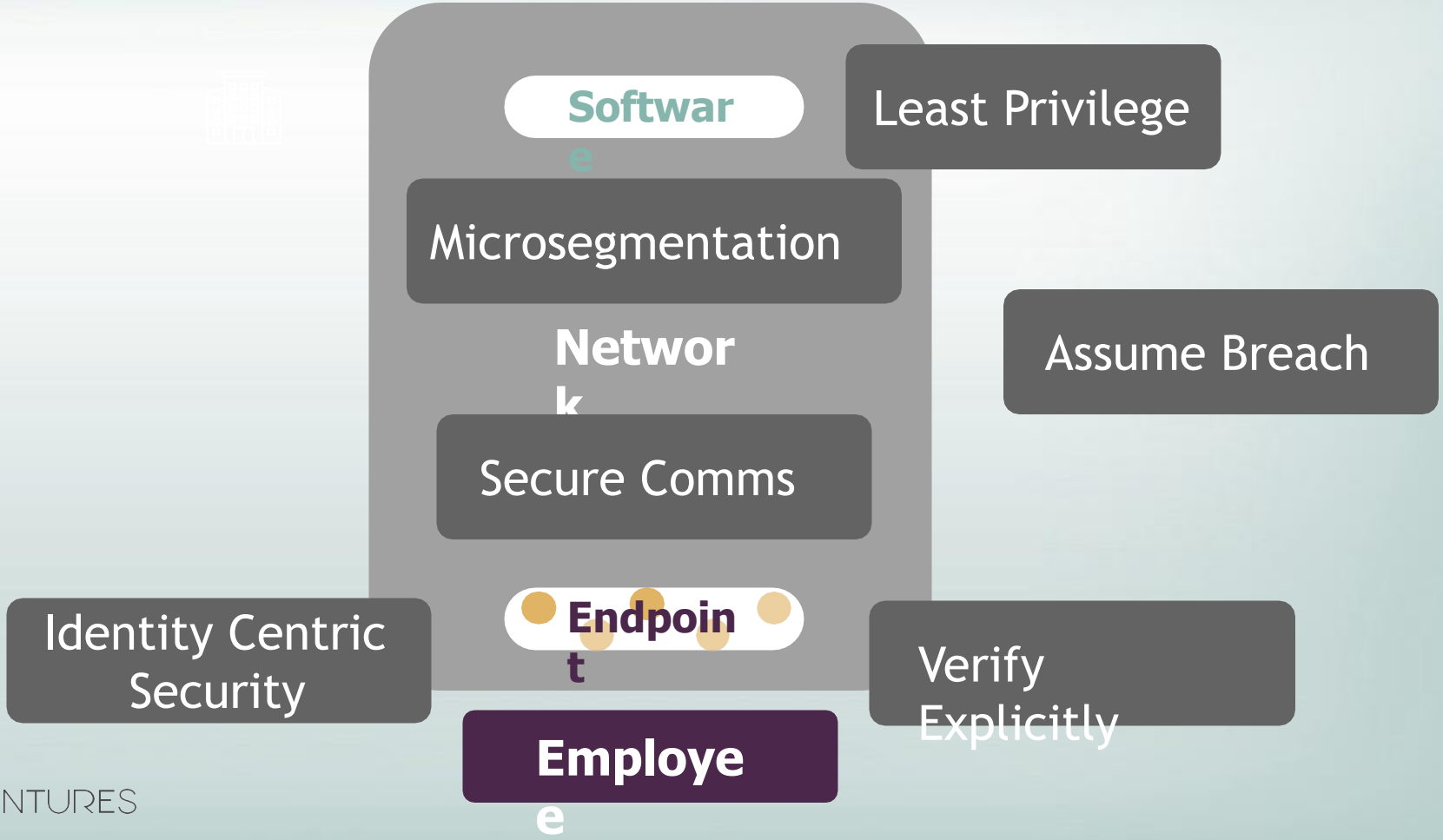
Instead, we made the endpoint trust *more* software


Continuous Monitoring
Softwar
e
Least Privilege
Microsegmentation
Networ
k
Assume Breach
Secure Comms
Identity Centric Security
Endpoin
t
Verify Explicitly
Employe
e

YL VENTURES


Softwar
e
Least Privilege
Microsegmentation
Continu
N
o
e
u
tw
s
Assume Breach
M
or
o
k
nitoring
Secure Comms
Identity Centric
Security
Endpoin
t
Verify
Explicitly
Employe
e

YL VENTURES


Softwar
e
Least Privilege
Microsegmentation
Networ
k
Assume Breach
Secure Comms
Identity Centric
Security
Endpoin
t
Verify
Explicitly
Employe
e

YL VENTURES

Softwar
e

Least Privilege

Microsegmentation

Ass**N**um**et**e**wo**B

rre**k**ach Secure

Identity Centric
Security

**Endpoin
t**Comms

Verify
Explicitly

**Employe
e**

YL VENTURES

Limited Assumption of Privilege

Network

Identity Centric Security

Endpoint

Verify Explicitly

Employee

Limited AsNsuemtwpotirokn of Privilege

Identity Centric Security

Endpoin

Employe e

Verify Explicitly

YL VENTURES

Limited AsNsuemtwpotirokn of Privilege

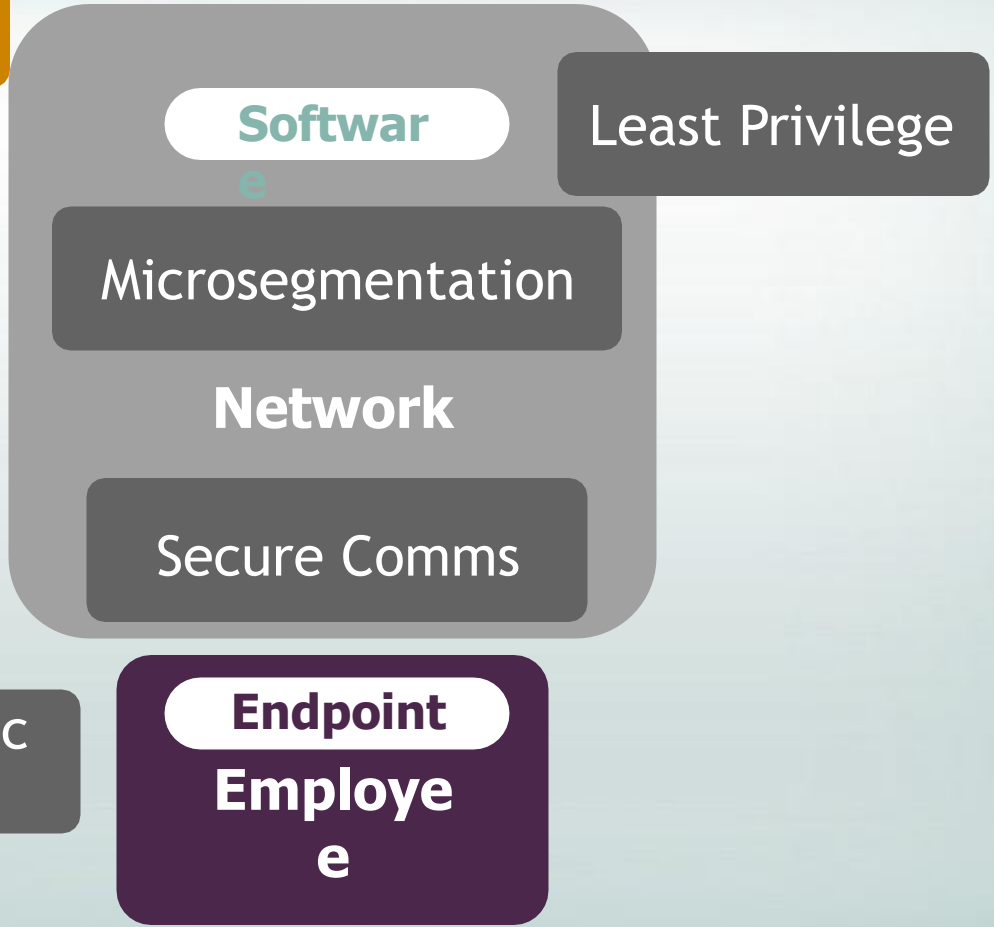
Identity Centric Security

Endpoint

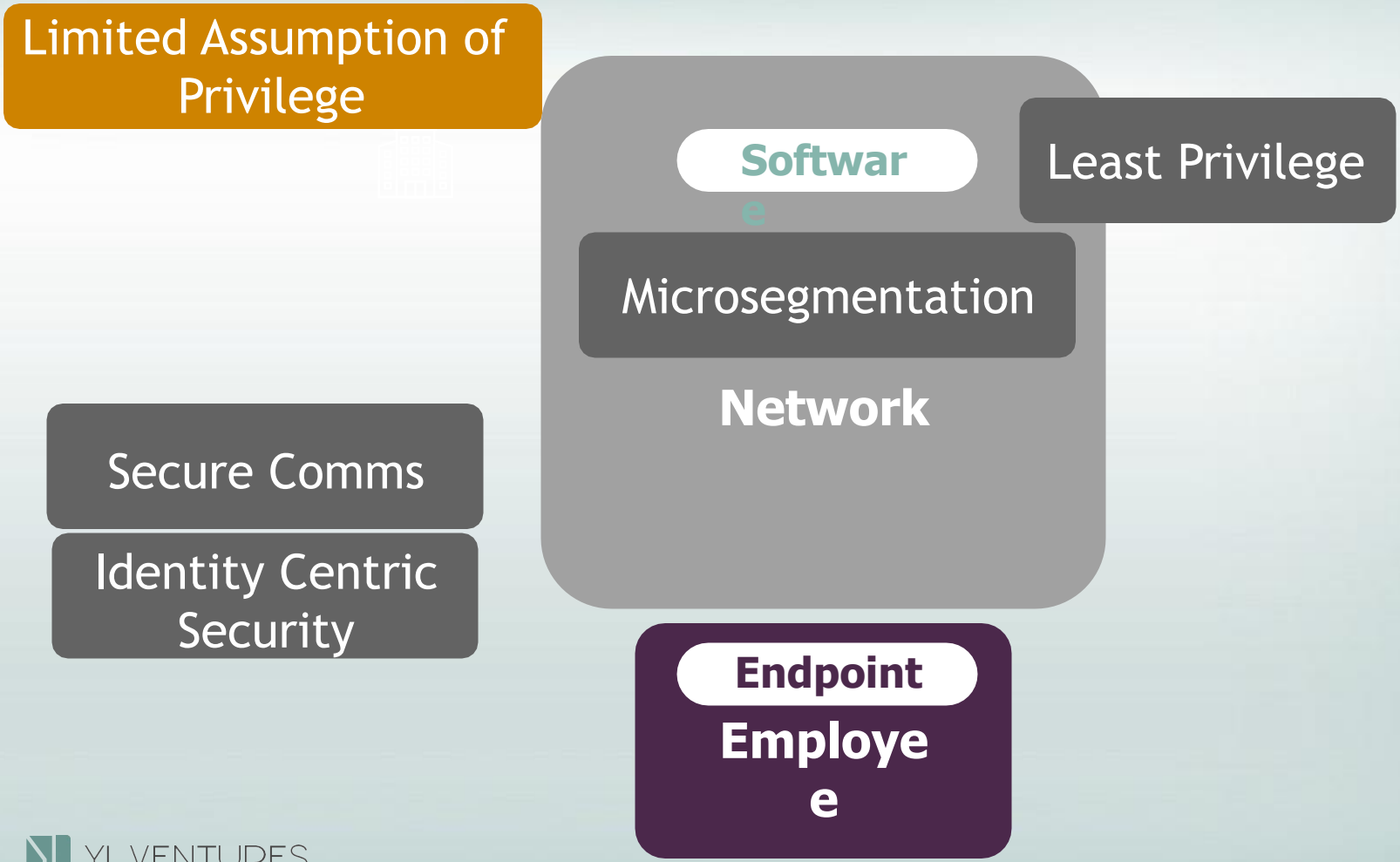
Employe e

YL VENTURES

Limited Assumption of Privilege

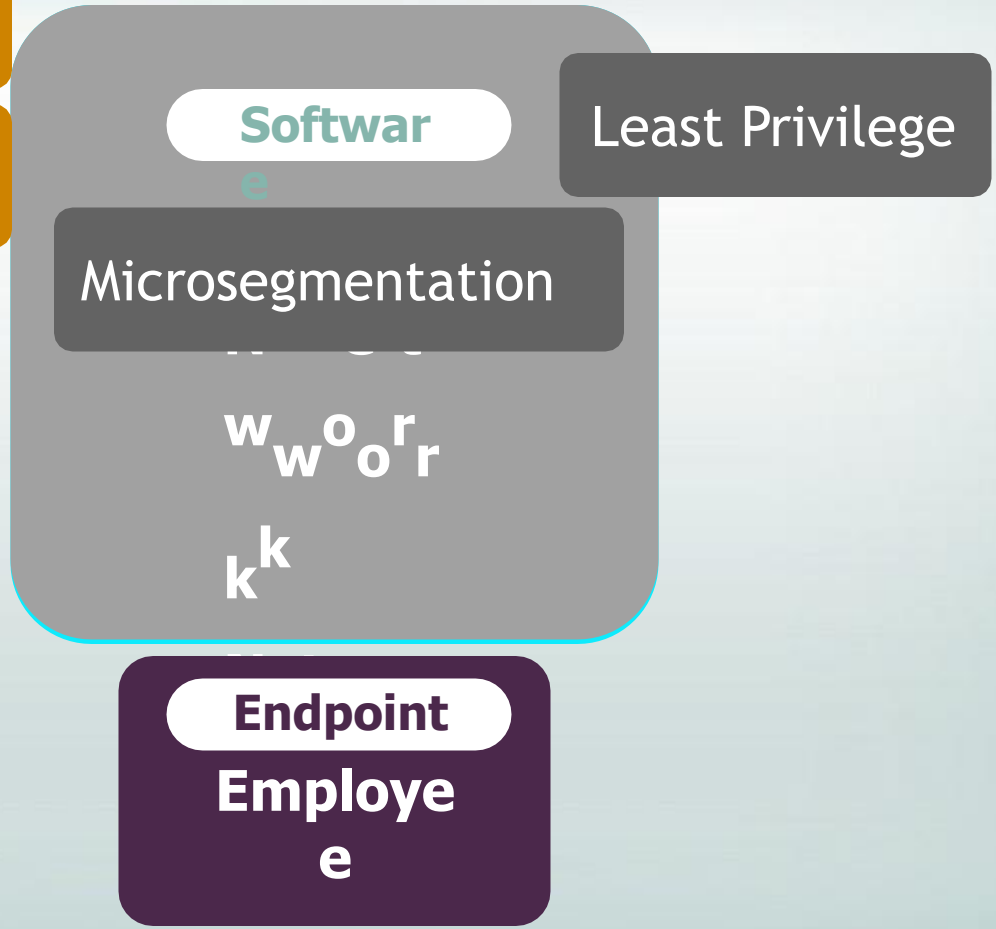


YL VENTURES

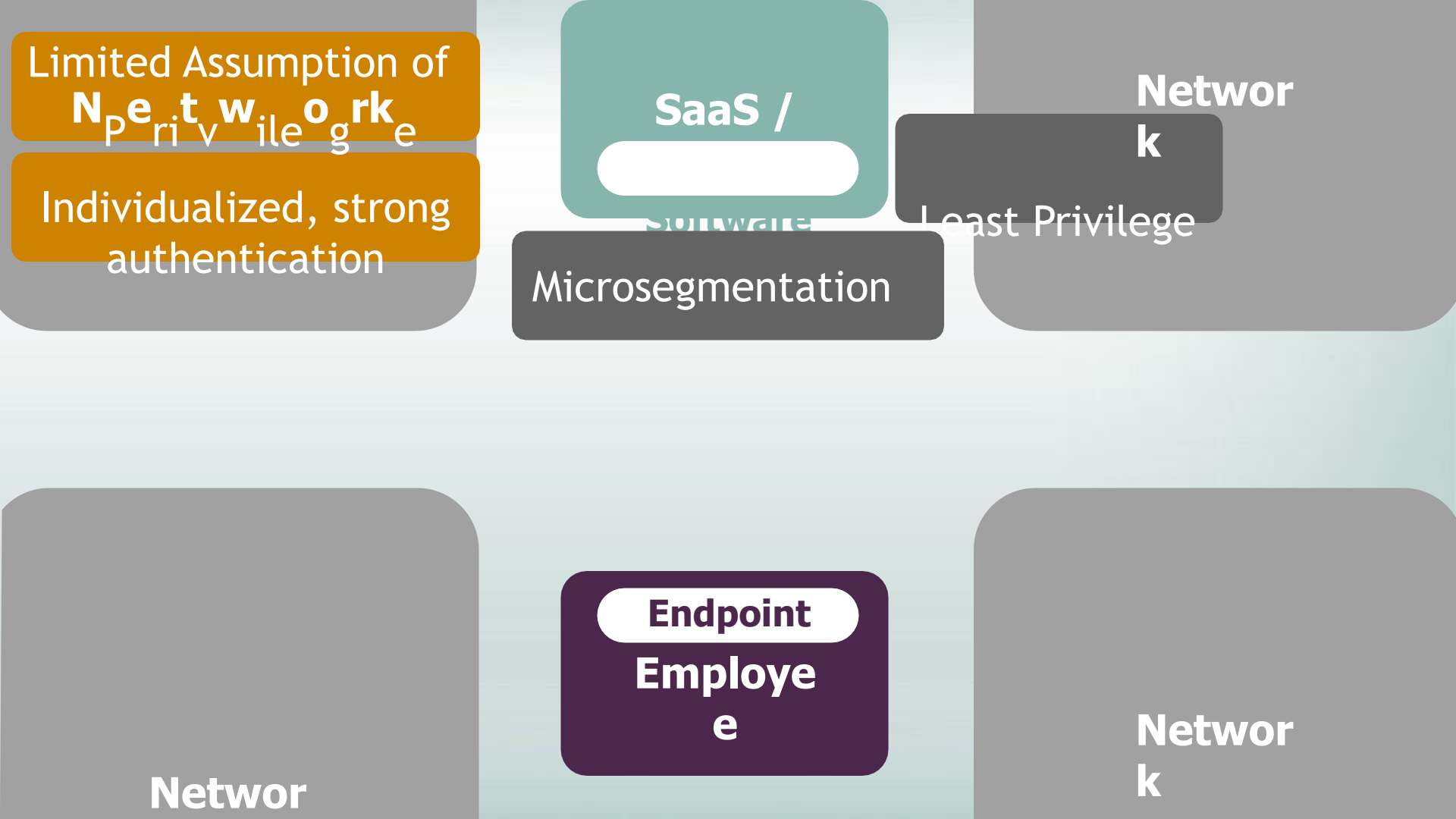

Limited Assumption of Privilege
Softwar
e
Least Privilege
Microsegmentation
Network
Secure Comms
Identity Centric Security
Endpoint
Employe
e

Limited Assumption of Privilege

Individualized, strong authentication



YL VENTURES


Limited Assumption of Network Privilege
Individualized, strong authentication
SaaS /
Microsegmentation
Network
Least Privilege
Endpoint
Employee
Network
Network

Limited Assumption of Privilege

Individualized, strong authentication

SaaS / Software

Least Privilege

Endpoint

Employe e

YL VENTURES

Limited Assumption of Privilege

Individualized, strong authentication

Minimize unused privilege



Limited Assumption of Privilege

Individualized, strong authentication

Minimize unused privilege

Limited Assumption of Privilege

Reduce/Eliminate Admin

Non-copyable access tokens

Individualized, strong authentication

Minimize unused privilege

Limited Assumption of Privilege

Reduce/Eliminate Admin

Non-copyable access tokens

Endpoint is part of the User

Individualized, strong authentication

Cryptographically strong auth

Minimize unused privilege

Limited Assumption of Privilege	Reduce/Eliminate Admin
	Non-copyable access tokens
Individualized, strong authentication	Endpoint is part of the User
	Cryptographically strong auth
	Separate *Authorization* & *Grant*
Minimize unused privilege	
	Streamline grant provisioning

Limited Assumption of Privilege	Reduce/Eliminate Admin
	Non-copyable access tokens
Individualized, strong authentication	Endpoint is part of the User
	Cryptographically strong auth
	Separate *Authorization* & *Grant*
Minimize unused privilege	
	Streamline grant provisioning

APPLY

- Limited Assumption of Privilege
- Individualized, strong authentication
- Minimize unused privilege

APPLY

- Limited Assumption of Privilege
- Individualized, strong authentication
- Minimize unused privilege

Rethink Your Architecture

Take Baby Steps

APPLY

- Limited Assumption of Privilege
- Individualized, strong authentication
- Minimize unused privilege

Rethink Your Architecture

- Stop trusting admin tools
- Phish-proof authentication
- Enable authorization without grants

Take Baby Steps

APPLY

- Limited Assumption of Privilege
- Individualized, strong authentication
- Minimize unused privilege

Rethink Your Architecture

- Stop trusting admin tools
- Phish-proof authentication
- Enable authorization without grants

Take Baby Steps

- Find duplicate credentials
- Tie authentication to the endpoint
- Make provisioning easy

Thank You