A Comprehensive Framework for Zero Trust & Cross Domain Security

Michael A. Blake
Chief Architect
17-APR 2025

KEY OBJECTIVES & AGENDA

A Comprehensive Framework for Zero Trust & Cross Domain Security

- Introduction – Zero Trust. What do the eight pillars provide?
- Challenges We Solve - The unmanaged device threat to Zero Trust
- Our Approach - Zero-Trust, Diodes, and CDS
- Success Stories
- Questions and Next Steps

ABOUT ME

Michael Blake

CHIEF ARCHITECT

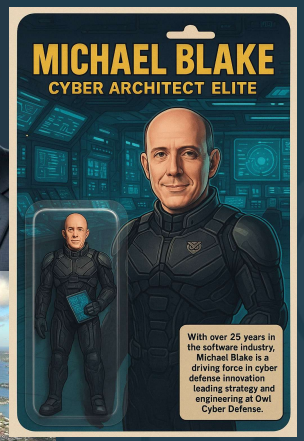
- With over 25 years of hands-on experience in the software industry, Michael Blake is a visionary IT professional known for driving the planning, architecture, deployment, and management of cutting-edge smart systems. His expertise extends to incorporating the latest technologies, including cyber defense, to develop innovative solutions. Michael has played a pivotal role in the acquisition of the ACS business unit by DC Capital, integrating it into Owl Cyber Defense's SPAC. Leading a team of 30 professionals, he oversees product roadmaps, sales strategy, technical engagements with certification boards, and corporate strategy.

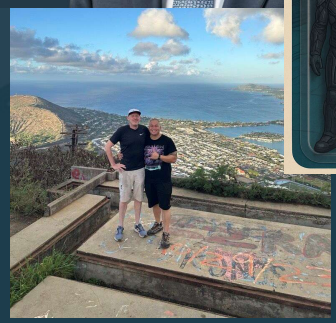
EDUCATION

- VIRGINIA POLYTECHNIC AND STATE UNIVERSITY, Master of Science in Chemistry
- MARSHALL UNIVERSITY, Bachelor of Science in Chemistry, Minor in Math and Computer Science

FUN FACT

- I started college as a music major (Brass), recently started learning guitar with my son





WHO OWL CYBER DEFENSE SERVES

Certified CDS solutions for both US Government and Commercial

Intelligence & Defense

- Deployed in all major branches of U.S. DOD
- Current products on NCDSMO baseline
- Helped develop DFDL data transformation technology
- Advise the NSA on CDS standards and development
- Data Center, Tactical, and Removable Media Solutions

Critical Infrastructure

- Deployed in over 90% of nuclear power plants in the U.S.
- Over 30 major power and water utilities and providers
- Hundreds of oil & gas deployments around the world
- Major transportation companies in rail and air transit
- DHS recommended technology for ICS security

Commercial

- Deployed in financial services, manufacturing, cloud services
- Securing data vaults, SIEM and IDS logs, cloud environments
- High-speed enterprise solutions for uni- or bi-directional, filtered or unfiltered data transfer
- Only commercially available government-certified CDS

ABOUT US

Our History

- Founded in 1998, pioneer in data diodes solutions
- Original data diode patent from Sandia National Labs
- Widely adopted in critical infrastructure sectors such as nuclear power plants, oil and gas facilities, defense and intelligence sectors

TRESYS

- Founded in 1998, merged with Owl in 2019
- Trusted advisors to the US Govt and cybersecurity standards bodies
- Advanced filtering capabilities, core contributors to Apache Daffodil community, and first US-certified exportable CDS

TRIDENT

- Assured Collaboration Systems (ACS) acquired in 2021.
- Partnered with AFRL since early 2000s to deliver cross domain collaboration capabilities to the DOD/IC
- First and only US Govt approved VoIP, VTC and FMV CDS

Big Bad Wolf Security

- Founded in 2014. Acquired in 2023
- Specialty in cross domain cloud and mobile cyber security
- Founded by former Tresys CTO and primary developer of SELinux

WHY OWL?

Present and Future

Over 25 years of securing the data mobility of the world's most critical networks – *We are the industry authority in cross domain solutions and data diodes*

Talon - Next Gen Diodes

- New Cockpit UI
- New Hardware Lineup - Reduced SWaP and Miniaturized Form Factors
- NSA Approved
- High Speed – 50G/100G+
- Path to HCFD and Hardware Based CDS

Ruggedized and Tactical

- Leverage Existing RTB certified CDS Software
- Functional and Performance testing on variety of platforms
- High Speed – 50G/100G+
- Path to HCFD and Hardware Based CDS

XD Vision 2.0

- Unify CDS Codebases of Owl
- Multi-Domain
- RTB 5.X

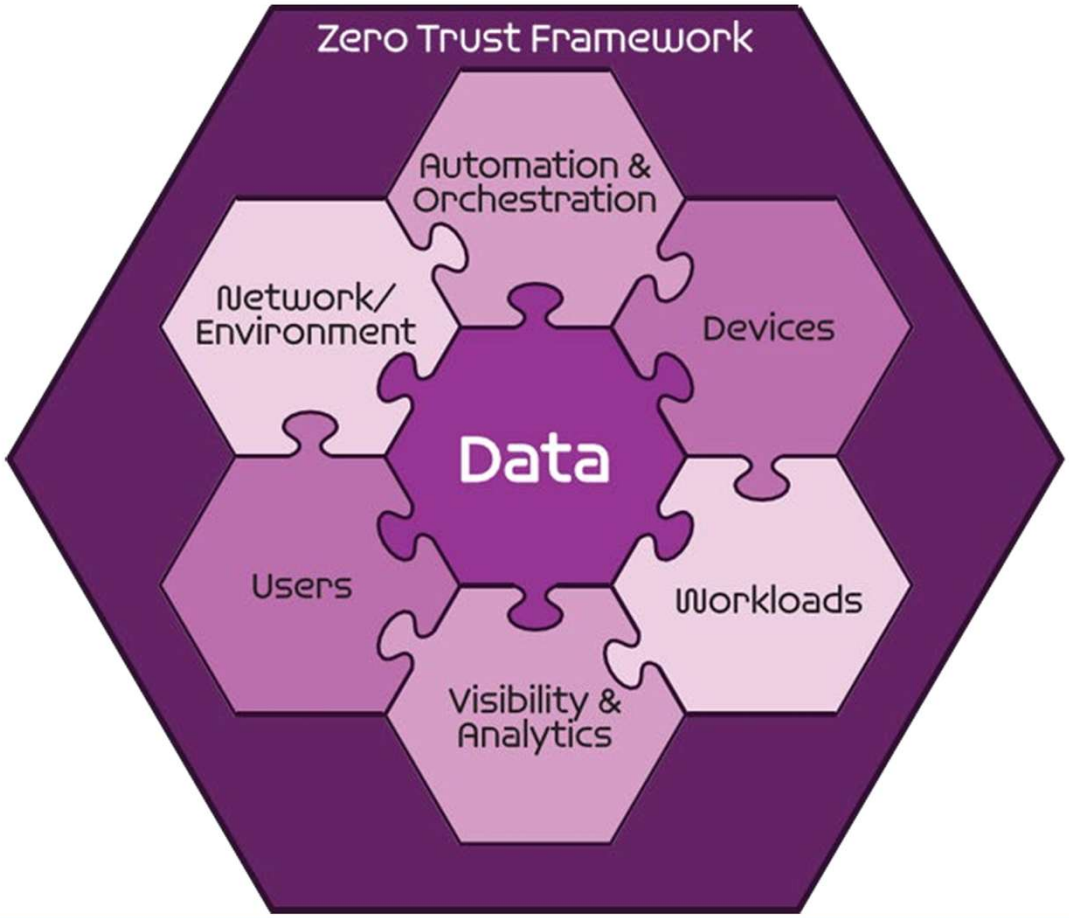
Zero Trust

What do the DISA 8 pillars provide?

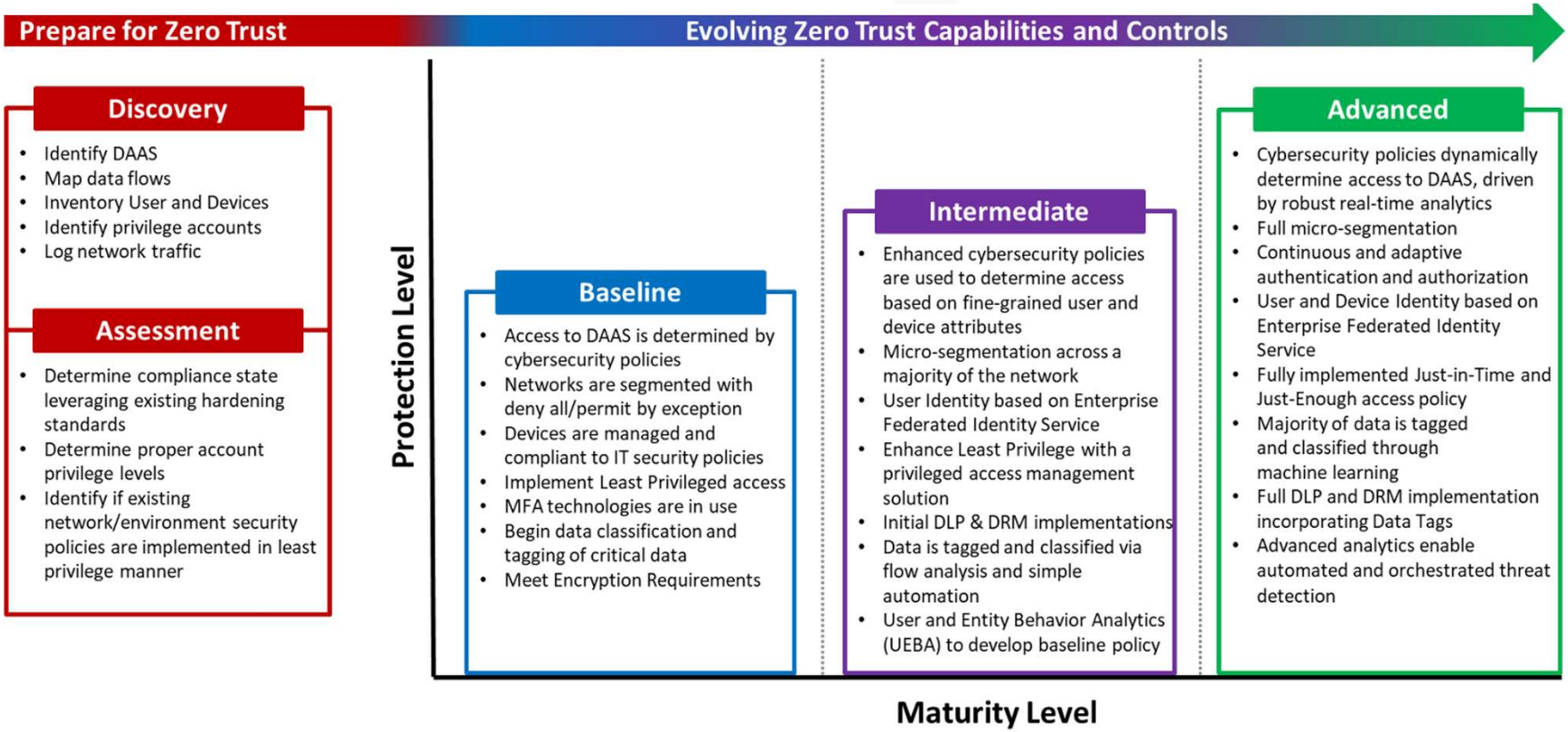
The 8 Pillars of Zero Trust

Zero Trust Pillars	
Pillar	**Description**
User	Involves focus on user identification, authentication, and access control policies which verify user attempts connecting to the network using dynamic and contextual data analysis.
Device	Performs "system of record" validation of user-controlled and autonomous devices to determine acceptable cybersecurity posture and trustworthiness.
Network	Isolates sensitive resources from being accessed by unauthorized people or things by dynamically defining network access, deploying micro-segmentation techniques, and control network flows while encrypting end-to-end traffic.
Infrastructure	Ensures systems and services within a workload are protected against unintended and unauthorized access, and potential vulnerabilities.
Application	Integrates user, device, and data components to secure access at the application layer. Security wraps each workload and compute container to prevent data collection, unauthorized access or tampering with sensitive applications and services.
Data	Involves focus on securing and enforcing access to data based on the data's categorization and classification to isolate the data from everyone except those that need access.
Visibility and Analytics	Provides insight into user and system behavior analytics by observing real-time communications between all Zero Trust components.
Orchestration and Automation	Automates security and network operational processes across the ZTA by orchestrating functions between similar and disparate security systems and applications.

ZTA Pillars Protect the Data



ZTA Journey

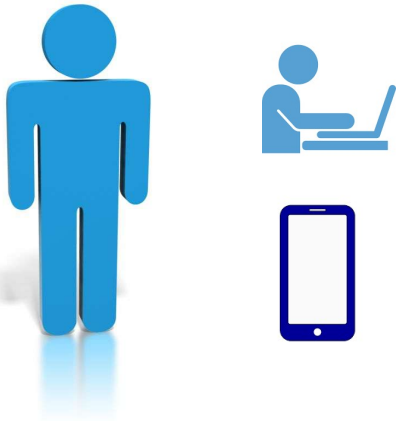


User – Nonrepudiation

Are you who you say you are?

- Something you know (Password)
- Something you have (Certificate)

Device – Similar to user



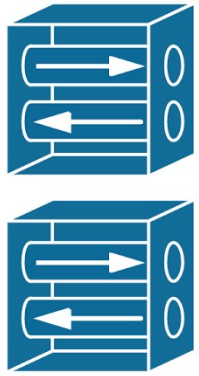
Certificate
Password
Face/finger

Trusted Boot Loader with TPM
Signed boot image
Whitelist Applications
Biometric Authentication
Device Certificate(s)
Geofencing

Network – Nonrepudiation and Confidentiality

Certificate
Password
Face/finger

Secure Boot
Whitelist Applications
Device Certificate(s)
Biometric Login

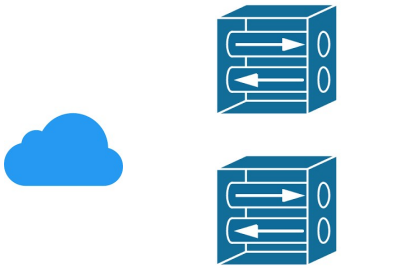


Mutual TLS
Authentication of user and devices
Encrypted data in transit
Double VPN Tunnel
MACSEC
IPSEC
Authenticator

Infrastructure

Certificate
Password
Face/finger

Secure Boot
Whitelist Applications
Device Certificate(s)
Biometric Login



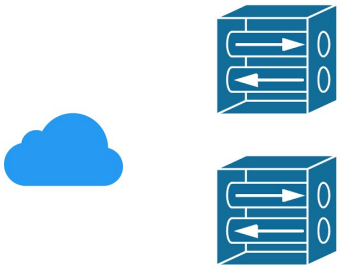
Double VPN Tunnel
MACSEC
IPSEC
Mutual TLS
MFA Authenticator

Infrastructure
- Firewalled Resources (ACLs)
- VLANS
- Physically Isolated Switches
- Internal CDPs and Domain Controllers

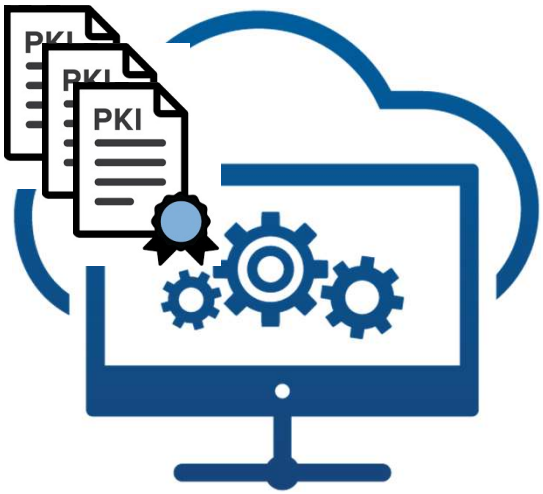
Application

Certificate
Password
Face/finger

Secure Boot
Whitelist Applications
Device Certificate(s)
Biometric Login



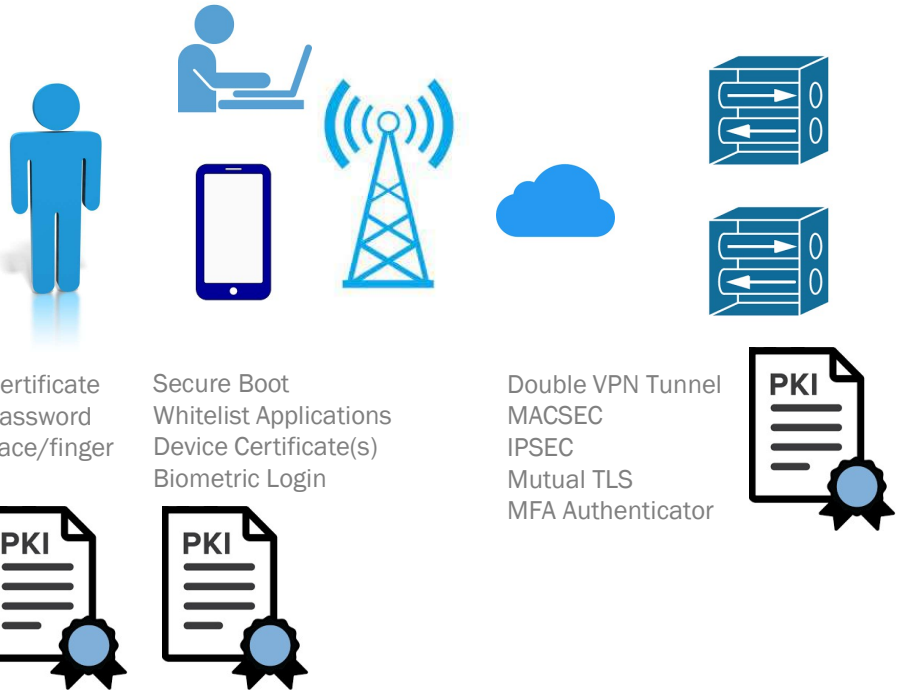
Double VPN Tunnel
MACSEC
IPSEC
Mutual TLS
MFA Authenticator



Infrastructure
- Firewalled Resources (ACLs)
- VLANS
- Physically Isolated Switches
- Internal CDPs and Domain Controllers

Applications
- Rootless Containers
- No processes running as root
- Mutual TLS between servers
- SAML

Data



Certificate
Password
Face/finger

Secure Boot
Whitelist Applications
Device Certificate(s)
Biometric Login

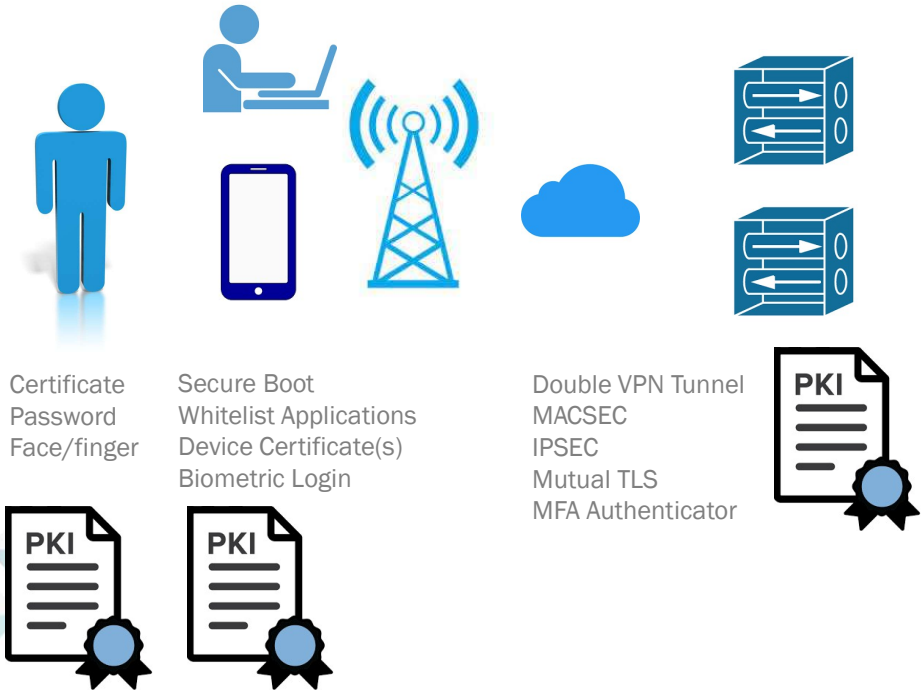
Double VPN Tunnel
MACSEC
IPSEC
Mutual TLS
MFA Authenticator

Infrastructure
- Firewalled Resources (ACLs)
- VLANS
- Physically Isolated Switches
- Internal CDPs and Domain Controllers

Applications
- Rootless Containers
- No processes running as root
- Mutual TLS between servers
- SAML

Data
- Database roles with views
- Business logic around data aggregation
- Security Markings
- XML Firewalls with Schema Validation

Visibility and Analytics



Certificate
Password
Face/finger

Secure Boot
Whitelist Applications
Device Certificate(s)
Biometric Login

Double VPN Tunnel
MACSEC
IPSEC
Mutual TLS
MFA Authenticator

Infrastructure
- Firewalled Resources (ACLs)
- VLANS
- Physically Isolated Switches
- Internal CDP

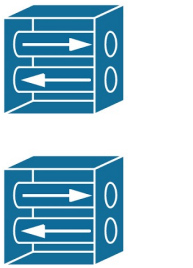
Applications
- Rootless Containers
- No processes running as root
- Mutual TLS between servers
- SAML

Data
- Database roles with views
- Business logic around data aggregation
- Security Markings
- XML Firewalls with Schema Validation

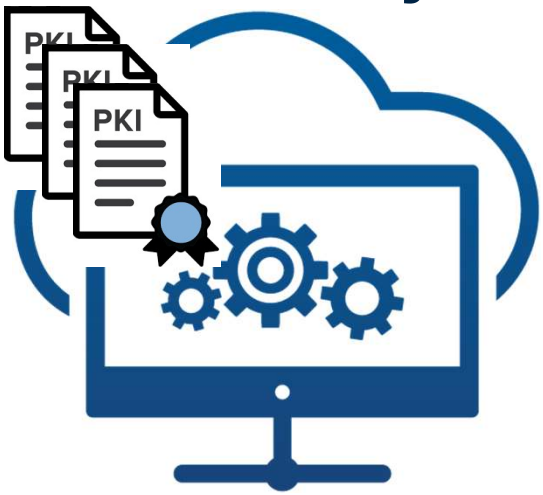
Zero Trust Intermediate Maturity

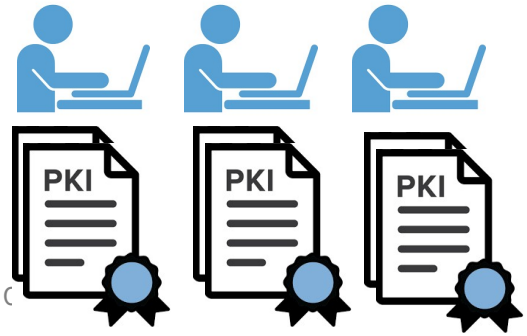
Certificate
Password
Face/finger

Secure Boot
Whitelist Applications
Device Certificate(s)
Biometric Login



Double VPN Tunnel
MACSEC
IPSEC
Mutual TLS
MFA Authenticator





Infrastructure
- Firewalled Resources (ACLs)
- VLANS
- Physically Isolated Switches
- Internal CDP

Applications
- Rootless Containers
- No processes running as root
- Mutual TLS between servers
- SAML

Data
- Database roles with views
- Business logic around data aggregation
- Security Markings
- XML Firewalls with Schema Validation

Visibility and Analytics - DCO
- Netflow, SNMP, logs
- IDS and SEIM

Automation and Orchestration
- ACAS and SCAP scans
- IP Blacklisting

User and Device Compromise – from the outside

Baseband Cellular Attack

- When the cellular baseband controller is on the same die as the cell phone processor, it can be exploited to write instructions into the processor from the cellular network (Ralf-Philipp Weinmann. 2012. Baseband Attacks: Remote Exploitation of Memory Corruptions in Cellular Protocol Stacks.. In WOOT. 12—21)
- Cellular Baseband Controllers run RTOS firmware that is rarely patched

How does DOD prevent such attacks?

- Phones manufactured for DOD with cellular baseband controller separate from smart phone processor DIE
- Partition phone (i.e. Redwall), boot into personal or secured image, secured image with cellular radio disabled connecting through hotspot

The Unmanaged Device risk to the Enterprise: MALWARE

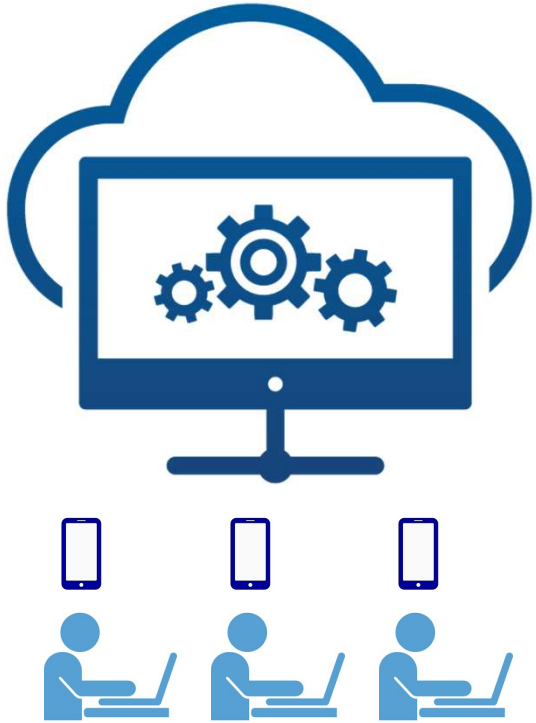
The BYOD threat to Zero Trust

Unmanaged/Legacy Device Challenges

Certificate
Password
Face/finger

~~Secure Boot~~
~~Whitelist Applications~~
~~Device Certificate(s)~~
Biometric Login

~~Double VPN Tunnel~~
~~MACSEC~~
~~IPSEC~~
TLS
MFA Authenticator



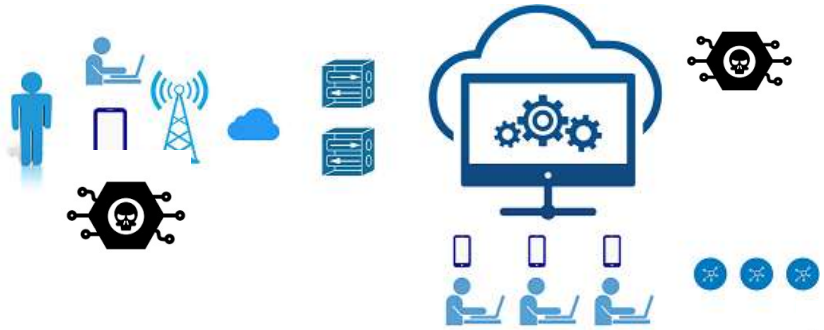
Infrastructure
- Firewalled Resources (ACLs)
- VLANS
- Physically Isolated Switches
- Internal CDP

Applications
- Rootless Containers
- No processes running as root
- Mutual TLS between servers
- SAML

Data
- Database roles with views
- Business logic around data aggregation
- ~~Security Markings~~
- XML Firewalls with Schema Validation

Summary

- Unmanaged, legacy, or IOT devices that cannot establish root of trust or run endpoint security expose the enterprise to unlimited risk
- Organizations and partners will inevitably be at different levels of maturity on their journey to Zero Trust (DOD at 14% compliance)
- Interoperable data tagging requires standards that have yet to be written or agreed to
- The zero- trust design will securely and confidentially deliver malware and malware augmentation from your employee's and customer's devices directly to the front door of your trusted networks



How to mitigate Zero Trust risks?

(U) BINDING OPERATIONAL DIRECTIVE FOR IMPLEMENTATION BOD-2025-001

(U) DATE: 3 March 2023

(U) SUBJECT: Restricting the use of the Zero Trust Framework as an alternative to Cross Domain Solutions between Security Domains

Software Defined Perimeter

7.1.2 Software Defined Perimeter (OV-2)

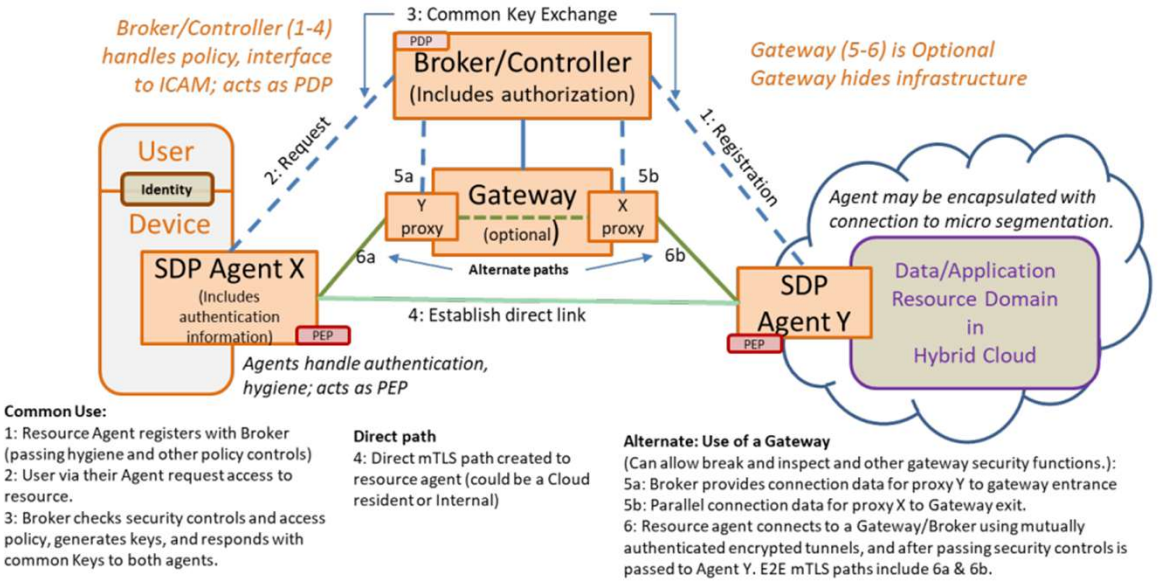


Figure 33 Design Pattern: Software Defined Perimeter (OV-2)

Zero Trust SDP secured by CDS

Zero Trust Architecture Software Defined Perimeter	Cross Domain Solution
Microsegmentation	2 physically separate network interfaces on a platform enforcing data flow by firewall, file permission, SELinux, Network Namespace, and in HTN a FPGA based diode preventing Policy Bypass.
Encryption	Encryption terminated as data enters CDS, encrypted as it leaves the CDS.
All data and applications direct visibility removed from the public internet	Pipelines of filtering processes with non-IP based IPCs separate dataflows between network interfaces
ZTA broker with policy enforcement points authorizing devices based on device identity, device hygiene, and user identity with confidence level scoring	Only possible if enterprise manages all end user instruments and servers. A CDS enables secure communication with unmanaged devices that are unable to provide metrics for a PDP and ZTA broker.
Optional but highly recommended Gateway to break and inspect traffic to view traffic for malicious actions and data loss.	Key function CDS provides for data – semantic and syntactic validation. CDS's that implement the required NSA filtering additionally mitigate covert channels, malware augmentation, and exfiltration.

ENABLING CJADC2

CDS - a critical enabler in a ZTA where multiple security domains must interoperate.

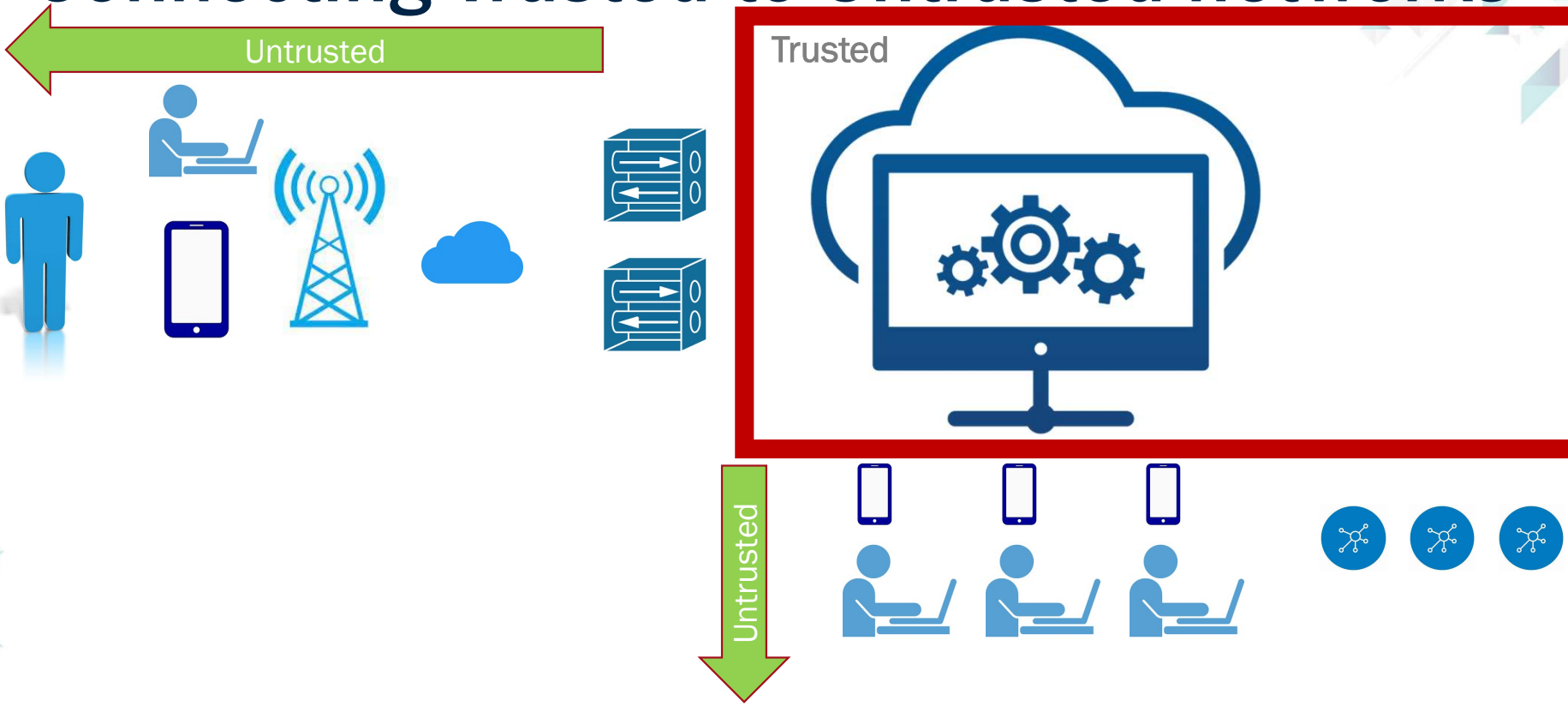
- 🔐 1. Enforces Strong Data Flow Control (Least Privilege Data Access)
- 🧱 2. Acts as a SDP Broker and Gateway
- 🔍 3. Enables High-Assurance Inspection and Sanitization
- 🛡️ 4. Hardware-Enforced Isolation – *RTB Compliance for HTN*
- 🌐 5. Supports Multi-Domain and Mission Partner Interoperability
- 📊 6. Provides Auditable, Deterministic Behavior

🎯 - A CDS IS LIKE A ZERO TRUST FIREWALL FOR YOUR MOST SENSITIVE DATA

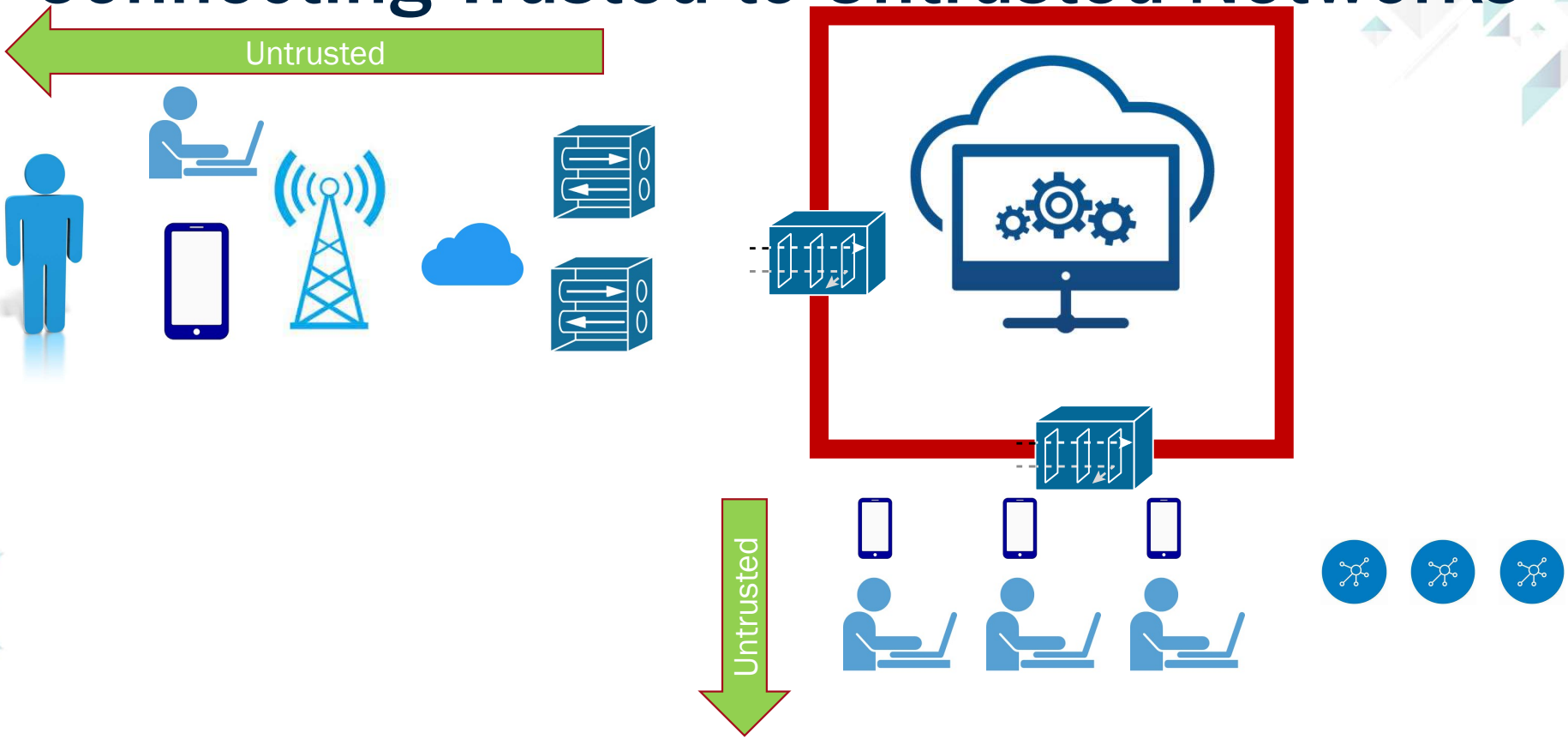
What is a Cross Domain Transfer Solution?

- A high-assurance controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains.
- Content / Data Filtering – Network / Application Layer
- Transfer vs. Access Solutions

Connecting Trusted to Untrusted networks



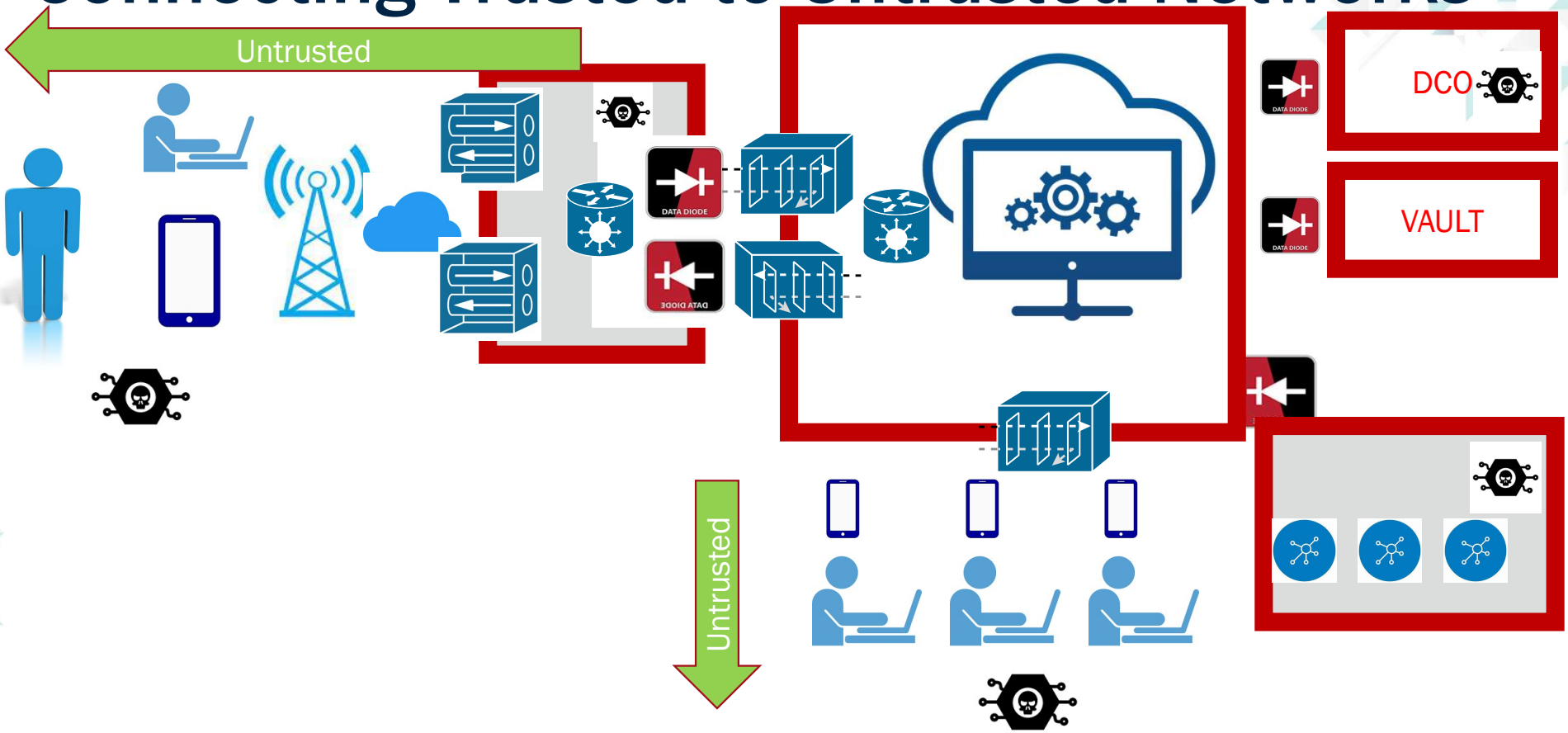
Connecting Trusted to Untrusted Networks



The Total Solution

Zero-Trust, Diodes, and CDS

Connecting Trusted to Untrusted Networks



Questions?

Michael A. Blake
Chief Architect

Mahalo!