Microsegmentation at the Department of Air Force

DAFITC Briefing

Mr. Jim Pickard

ZT.AF.MIL

MICROSEGMENTATION

ZERO TRUST TRANSITION TEAM

ILLUMINATE • CONTAIN • CONTROL

Today's Agenda

- DAF Enterprise Zero Trust Roadmap
- Zero Trust Capabilities
- Governance & Microsegmentation Enablers
- Microsegmentation Overview
- Microsegmentation Approach
- Current Project Status
- Q&A

DAF ENTERPRISE ZERO TRUST ROADMAP

Publication: 14 DEC 2023

IMPACT TO THE DAF

- *Disrupt adversaries through enhanced cyber readiness*
- *Increased resilience across all mission areas*
- *Provides rigorous authentication and authorization that takes into account numerous risk factors*

Focus on programmatics, capability use case assessment, and defining future state infrastructures.

Continue defining operational guidance for future state Enterprise services. Drive progress ahead of capability deployment and onboarding by preparing ZT infrastructure's architecture, services, and points of integration.

Scale capability onboarding and instill a focus on integration (e.g., API, AI/ML) and improving granularity of ZT maturation.

SERVICES AND STRATEGIC NARRATIVES

FY23 | FY24 | FY25+

Q3 | Q4 | Q1 | Q2 | Q3 | Q4 | Q1 | Q2+

User
Deliver a single enterprise ICAM solution serving all communities and environments with enhanced authentication and controls

- Reference ICAM Roadmap
- FIAR ICAM activities initiated
- Enterprise ICAM IOC deployed
- NPE rules established
- *Ongoing transition to attribute-based identity and continuing application integrations*
- Enterprise ICAM FOC deployed

Data
Integrate data ecosystem and provide support via Enterprise ZT services (e.g., NPEs)

- Lessons learned from NC3 assessed
- Common cyber data schema established
- Data Fabric Roadmap integrated with Data Services Environment (DSE) published
- Core tagging and labeling tools baselined
- NPE and data platform integration initiated
- Access attributes for data baselined
- *Ongoing data integrations with major data platforms*

Visibility & Analytics
Enable SIEM to process ZT relevant visibility data and exploiting data that includes application events and user behavior patterns

- DCO SIEM decision and associated programmatics formalized
- SOAR usage for ZT events decision formalized
- SIEM Threat alerting expanded to include CTI data feeds
- Standard cyber data schema for all SIEMs and SOARs implemented
- ELICSAR fully integrated with SIEM capabilities
- Policy and guidance gaps for implementing UEBA Tooling identified
- UEBA Tooling implemented

Automation & Orchestration
Establish SOAR as a major component of operational cybersecurity leverage; support APIs via enterprise services

- SIEM capabilities fully integrated into SOAR capabilities
- Enterprise SOAR expansion plan identified
- Responsible AI Guidebook published
- CSSPs and component SOCs roles and responsibilities reassessed
- Exemplar API use cases identified
- API strategy published and 'shared service product' defined
- DevSecOps API services IOC deployed

Application & Workloads
Standardize security control measures across enterprise applications

- Risk Management Strategy
- Current state Application ecosystem inventory initiated
- Enterprise SBOM Strategy published
- Common SBOM repository completed, and viable assessment tools identified
- 80% of Enterprise Application Inventory published

Network & Environment
Enforce micro segmentation with generally available SASE solution; deploy SDP solution at base level and tailor to applications

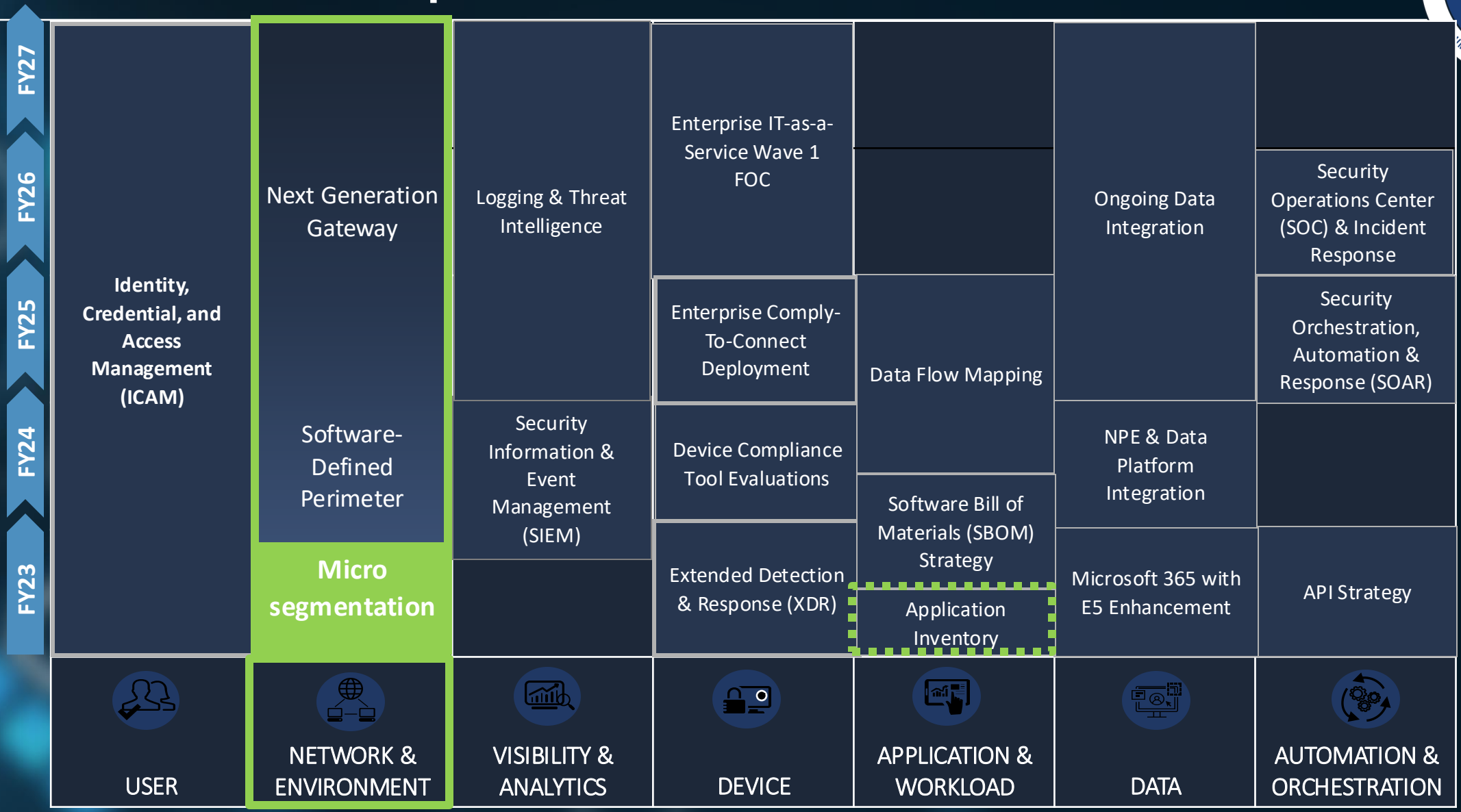
- Micro Segmentation
- Monitor Mode Data Flow Mapping initiated
- Plan for Monitor Mode Data Flow Mapping established
- Data Flow Mapping initiated for Enforcement Mode
- Micro operationalized
- *Ongoing application configuration*
- SDP
- Macro Segmentation
- Macro operationalized
- SDP and SASE continuous authentication, leveraging PDP/PEP best practices published
- BIM SDP phased rollouts initiated in CEDC locations
- SASE Solution services IOC deployed
- SDP for VPN replacement viable for user subgroup
- SASE Solution services FOC deployed
- JRSS sunset completed

Device
Automate and migrate tools to Cloud that manage device health and feed access decisions with Device-as-a-Service (DaaS) rolled out

- C2C
- Existing C2C solutions inventoried and mapped to DoD mandate
- C2C Strategy and reference architecture published
- C2C implementation plan approved
- C2C rollout to all supported environments completed
- Device Issuance & Support
- Device-as-a-Service (DaaS) Strategy published
- EITaaS Wave 1 Help Desk and ITSM deployed
- *Continuing EITaaS Wave 1 device rollout*
- Device Health
- Risk acceptance policy for Managed vs. Unmanaged Devices published
- Cloud-based XDR Platform deployed on NIPR for traditional and EITaaS devices
- Vulnerability analysis moved to cloud platform
- Cloud-based patch management and MDM implemented
- Cloud-based XDR integrated with SDP
- Joint User Device Health Strategy published
- Cloud-based XDR deployed for all environments

LEGEND: ○ *In Progress / To Do* ● *Completed*

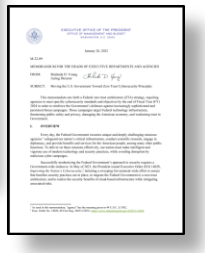
Zero Trust Capabilities



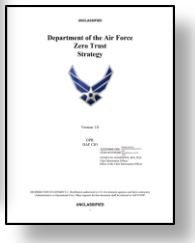
Governance & Microsegmentation Enablers

Executive Order 14028

DoD Zero Trust Strategy



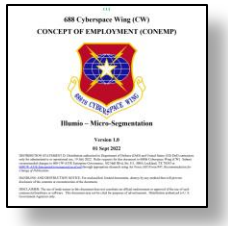
DAF ZT Strategy



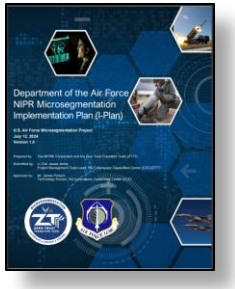
DAF Zero Trust I-Plan

Microsegmentation CONOP

Microsegmentation CONEMP



NIPR Microsegmentation Implementation Plan



Cyber Tasking Order 22-0035

CTO Fragos

Governance

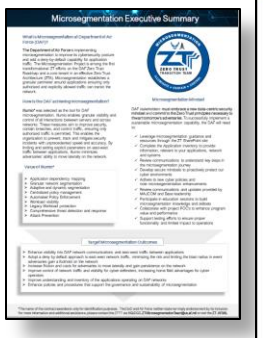
To access governance documents, visit the **Microsegmentation** tab on **ZT.AF.MIL**

Enablers

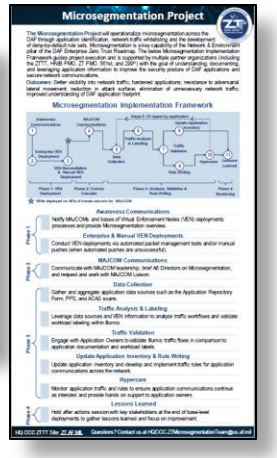
ZTTT Microsegmentation Playbook

Frequently Asked Questions

Microsegmentation Exec Summary



Activities by Phase



Executive Briefings

CFP Forum Messaging

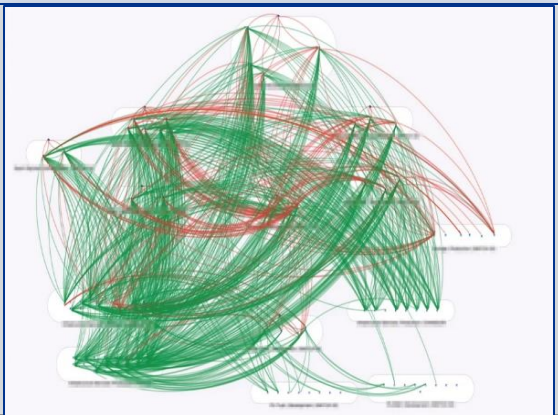
Microsegmentation Overview

Pre-Microsegmentation Challenges

Before Microsegmentation

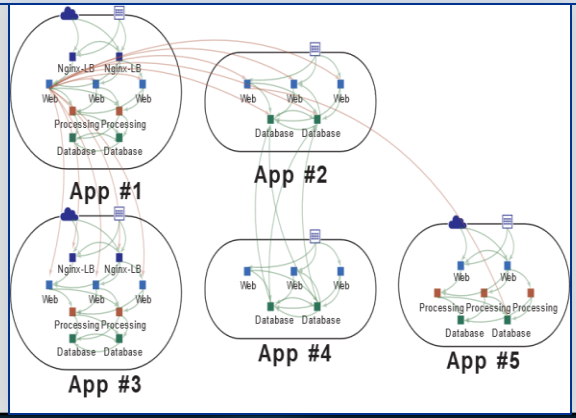
- Lack of granular application segmentation
- Network traffic flows largely unrestricted within base boundaries
- Reliance on macrosegmentation (VLANs and/or Subnets)
- Relatively easy lateral movement between applications post-exploitation
- Hardware firewalls provide bulk of network protections
- Vague understanding of allowed vs not allowed network traffic
- Poor visibility and understanding of application traffic and connections

Overly interconnected systems, open architecture, ad hoc visibility



After Microsegmentation

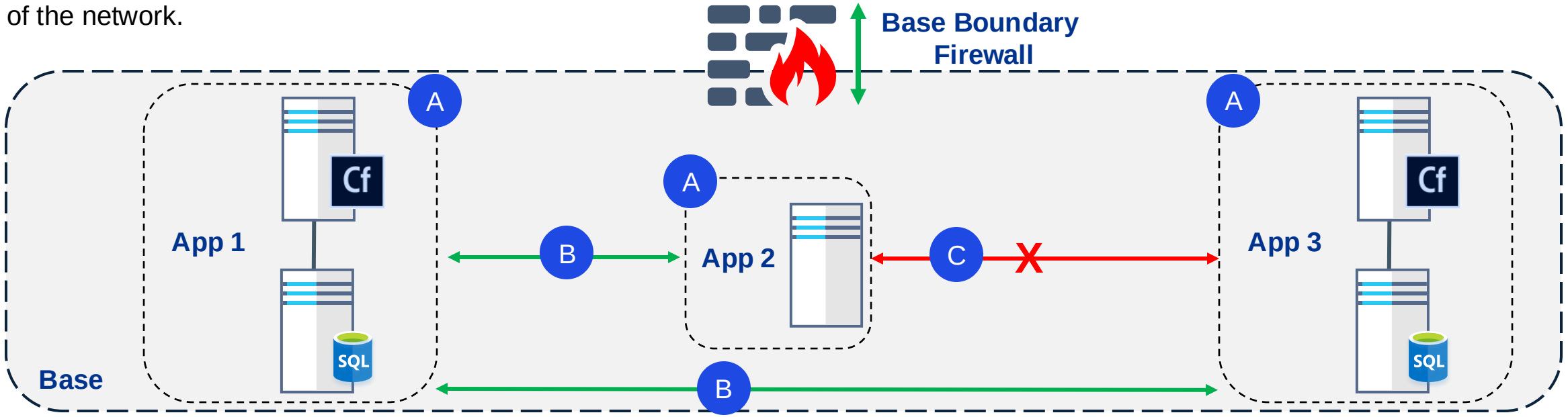
- Improved network visibility
- Enhanced breach containment
- Limited "blast radius" from unauthorized lateral movement
- Centralized defense of networks and applications
- Mature Zero Trust capabilities



Organized, clear, least privilege access

Background

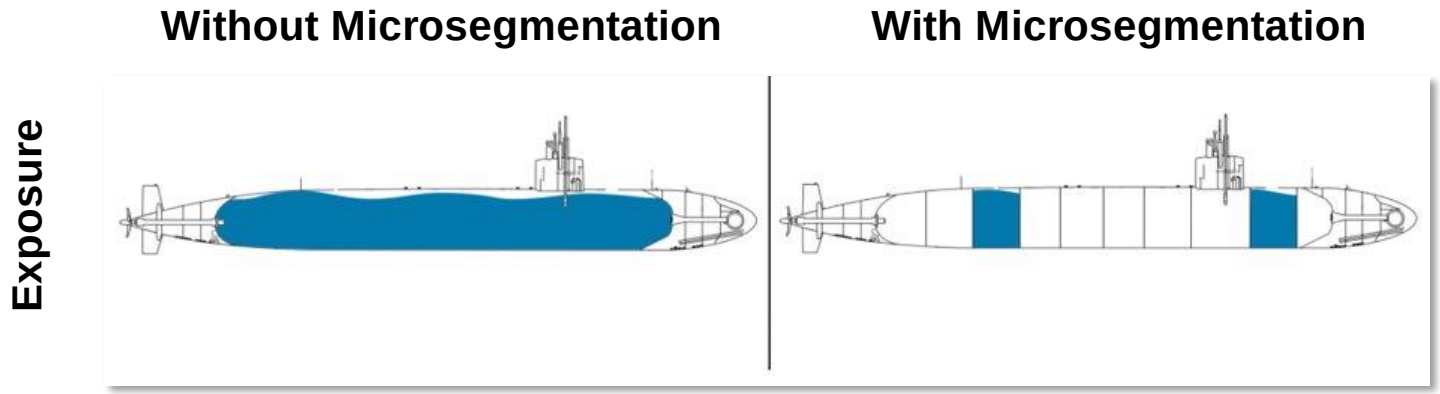
In accordance with CTO 22-0035, DAF is improving its cybersecurity posture by introducing a new technology to reduce the attack surface of Applications and Servers by only permitting explicitly authorized network traffic—microsegmentation of the network.



What is Microsegmentation?

- A core capability of an effective Zero Trust Architecture (ZTA).
- A process by which networks are sub-divided **(A)** to allow fine grained application of security controls and access requirements.
- The new ability to control East-West network traffic within and between applications **(B)** through the implementation of Illumio.
- A deny-by-default process, creating barriers between network resources, users, and applications **(C)** to ensure traffic is verified and secure.

Why Microsegmentation?



Why is microsegmentation important?

- Protect the most critical and sensitive assets and information impacting national security.
- Contain breaches by reducing DAF network attack surface.
- Enable cyber defenders with enhanced visibility and greater control of network traffic.
- Prevent, track and mitigate security incidents with unprecedented speed and accuracy.

How are we achieving this?

- Deploying Illumio, a leading microsegmentation platform, enterprise-wide.
- Software agents (VENs) on the endpoint manipulate host-based firewall to control access to the resource.
- Through cross-collaboration and engagement with the key Air Force leadership and stakeholders.
- By identifying and validating authorized network communications.
- By establishing rulesets, policies, and procedures that govern and protect DAF network traffic.

Future State and Value of Illumio

Scalable, Mature Zero Trust Capability

- With Illumio, the DAF can **increase segmentation without sacrificing security** or performance.
- Illumio will allow the DAF to **incrementally apply more granular levels of microsegmentation** as the capability evolves and wider adoption occurs.

Increased DAF Network Visibility

- Illumio agents (VENs) provide the ability to **report on application traffic and data flows, and to locate unknown, undocumented, or forgotten servers**.
- With Illumio, cyber defenders have clear understanding of traffic and can quickly identify potential vulnerabilities.

Enhanced Cybersecurity Posture

- Illumio's security policies prevent unauthorized access to systems, applications, and data.
- Microsegmentation **reduces attack surface by 90%-95%**.
- Granular control improves investigation and response times for **anomalous activity.**

Simplified Management

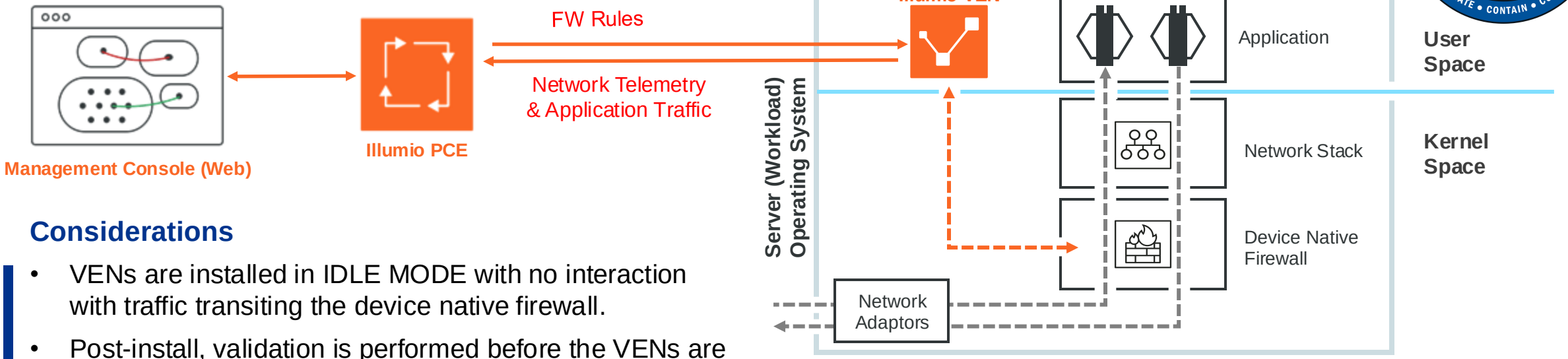
- Illumio's (PCE) allows set up consistent policies, control access across the network, and accelerate compliance.
- With Illumio, **microsegmentation can be implemented based on data flows between applications, users, and devices**, allowing for more granular control over network traffic.

Enhanced Breach Containment

- Illumio enables **consistent policy enforcement** and streamlines host-based firewall administration.
- Application **traffic will become more understandable** and anomalous network traffic will stand out allowing quicker investigation and response.
- Illumio can **easily adapt to changing security requirements.**

Microsegmentation Approach

How Does Illumio Work?

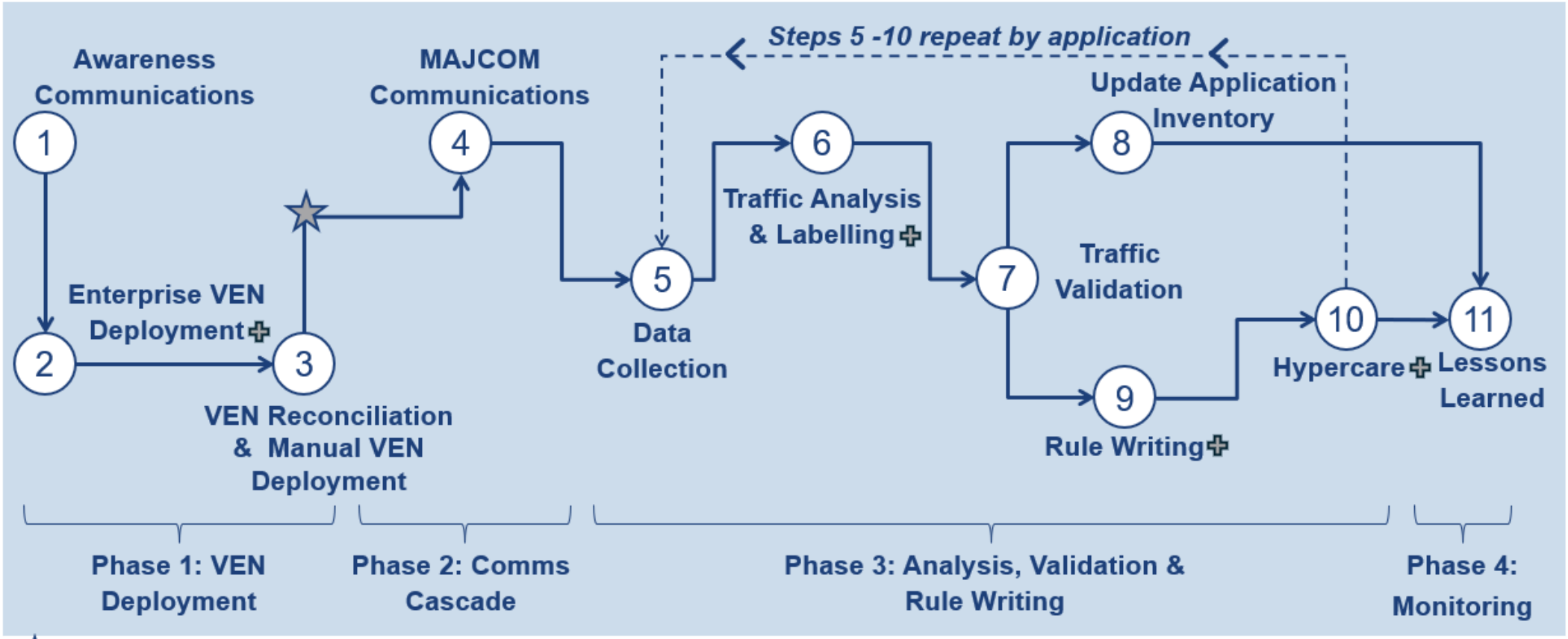


Considerations

- VENs are installed in IDLE MODE with no interaction with traffic transiting the device native firewall.
- Post-install, validation is performed before the VENs are moved into VISIBILITY MODE.
- Visibility Mode sends Network Telemetry and Application Traffic to the PCE for mapping.
- Visibility Mode does not allow or deny traffic through the device native firewall.
- Rules are drafted, validated, and deployed in conjunction with the 299th, 561st, and Application Owners.
- VENs are then moved from Visibility to ENFORCEMENT MODE. Deny by Default capability becomes operational.

Implementation Roadmap

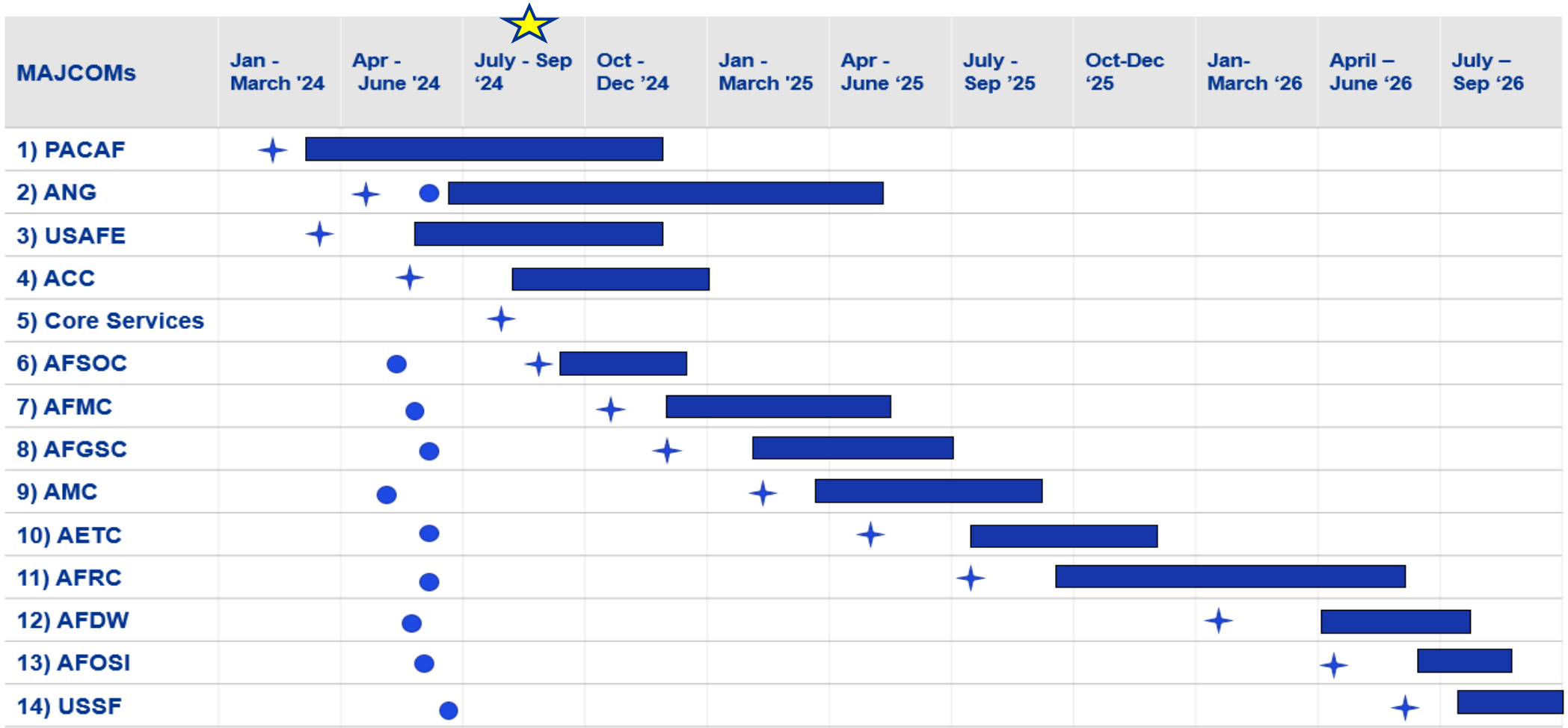
Microsegmentation Implementation Framework



★ VENs deployed on ~90% of known servers for MAJCOM

✚ Phase executed in collaboration with the 561st/299th

Microsegmentation Timeline



As of 8/20/24

Initial Communications

Initiation of Base Kickoff

VEN Deployment

Your Role in Microsegmentation

MAJCOM A6 Leaders

- ✓ Assign liaisons and connect MS Team with key Communications Squadron Commanders and Base Leaders
- ✓ Serve as a Champion by raising awareness and communicating benefits to cyber security
- ✓ Drive responsibility down to the bases for Microsegmentation as a Zero Trust capability

Communications Squadron Commanders

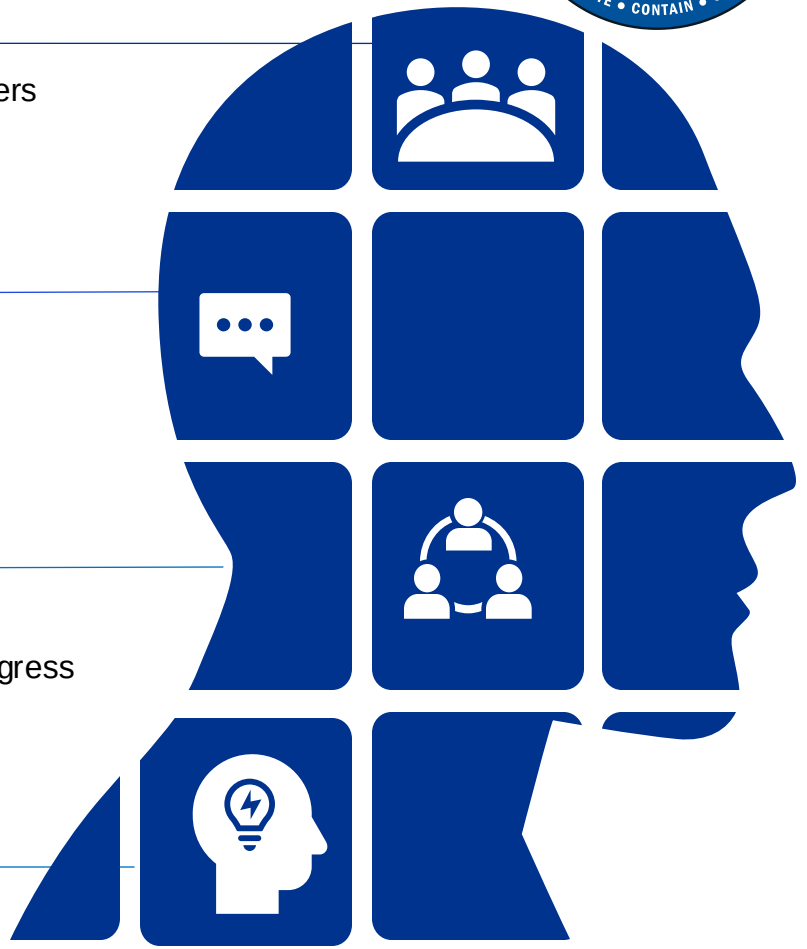
- ✓ Identify helpful and responsive stakeholder(s) with desired knowledge and skillset to support MS Team
- ✓ Nominate Base POC(s), Application Owners, and System Admins for data collection
- ✓ Check progress reports and hold POCs within your base accountable

Base POCs / Liaisons

- ✓ Help coordinate meetings, share communication, and engage appropriate stakeholders
- ✓ Provide the MS Team with MAJCOM/base specific expertise and access to repositories to accelerate progress and minimize operational impact
- ✓ Support with data collection, manage to data request to completion, and validate accuracy

Application Owners/ISSM

- ✓ Provide server/application data and expertise and actively engage with microsegmentation team
- ✓ Review and complete Base Server Questionnaire in a timely manner
- ✓ Validate traffic and ensure appropriate rules are drafted and enforced



Current Project Status

AFNET Microsegmentation

22
Strategic Comms Briefings
As of: 8/19/2024

700+
Stakeholders informed about Microsegmentation Project
As of: 8/19/2024

12
Liaisons Identified
As of: 8/19/2024

On Deck: Core Services, AFMC

In Progress: PACAF, ANG, USAFE, ACC, AFSOC

10,247 Known Servers
Identified servers through MECM, Illumio, etc. via Score
As of: 8/19/2024

8,037
Servers with VENs identified through PCE
As of: 8/19/2024

78%
Known Servers with VENs installed
As of: 8/19/2024

66
Unmanaged Workloads
As of: 8/19/2024

1,771
Fully labelled workloads (managed and unmanaged) in the PCE
As of: 8/19/2024

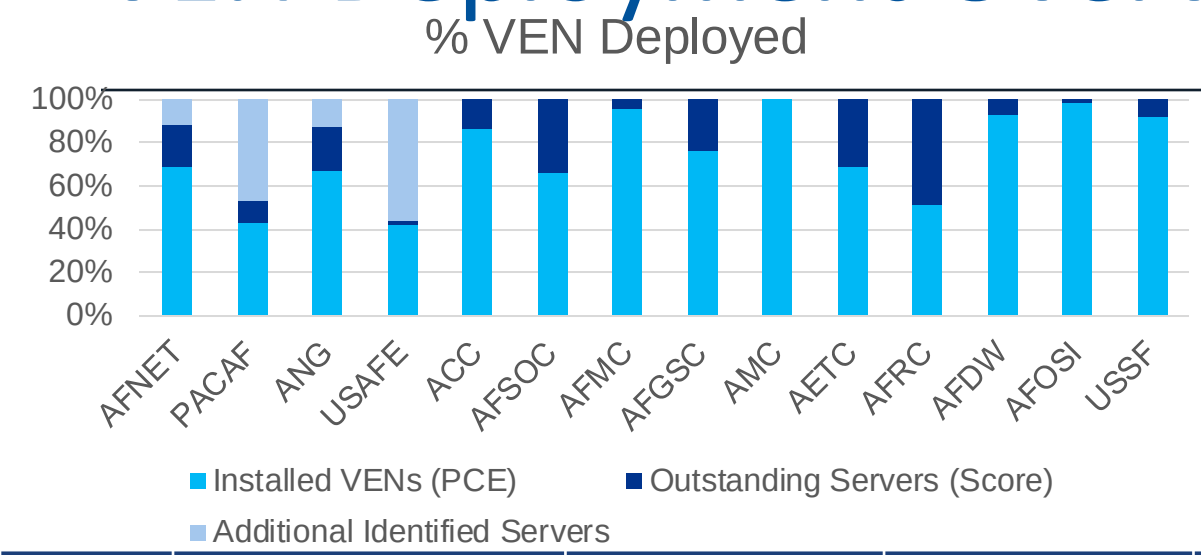
730
Applications in Microsegmentation
As of: 8/19/2024

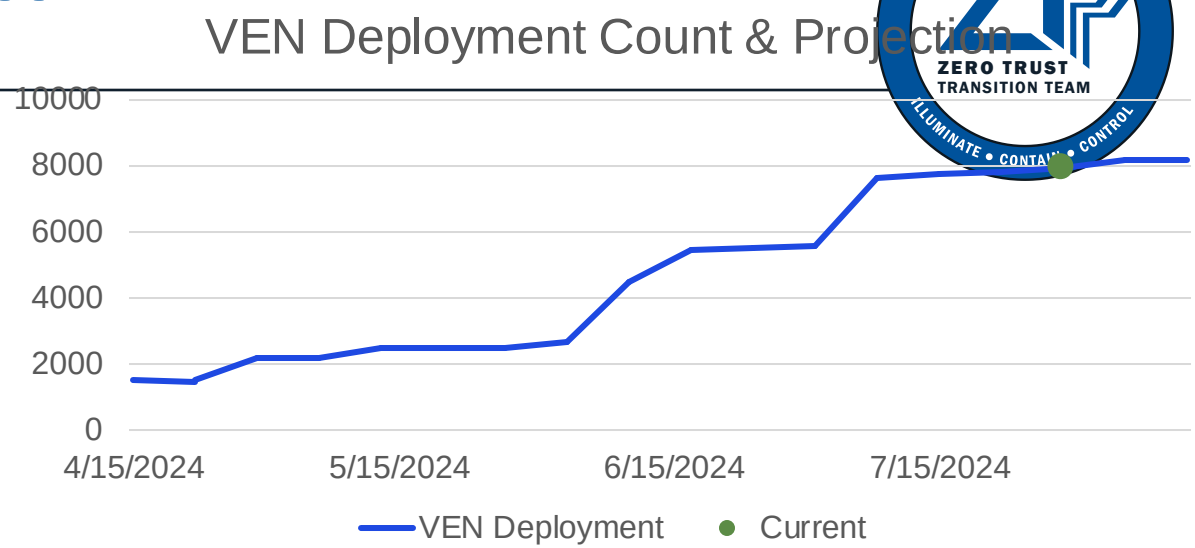
23
Application Transferred to Operations
As of: 8/19/2024

24
Servers in Enforcement
As of: 8/19/2024

Source: ZeroTrust - Power BI Report Server (usaf.mil)

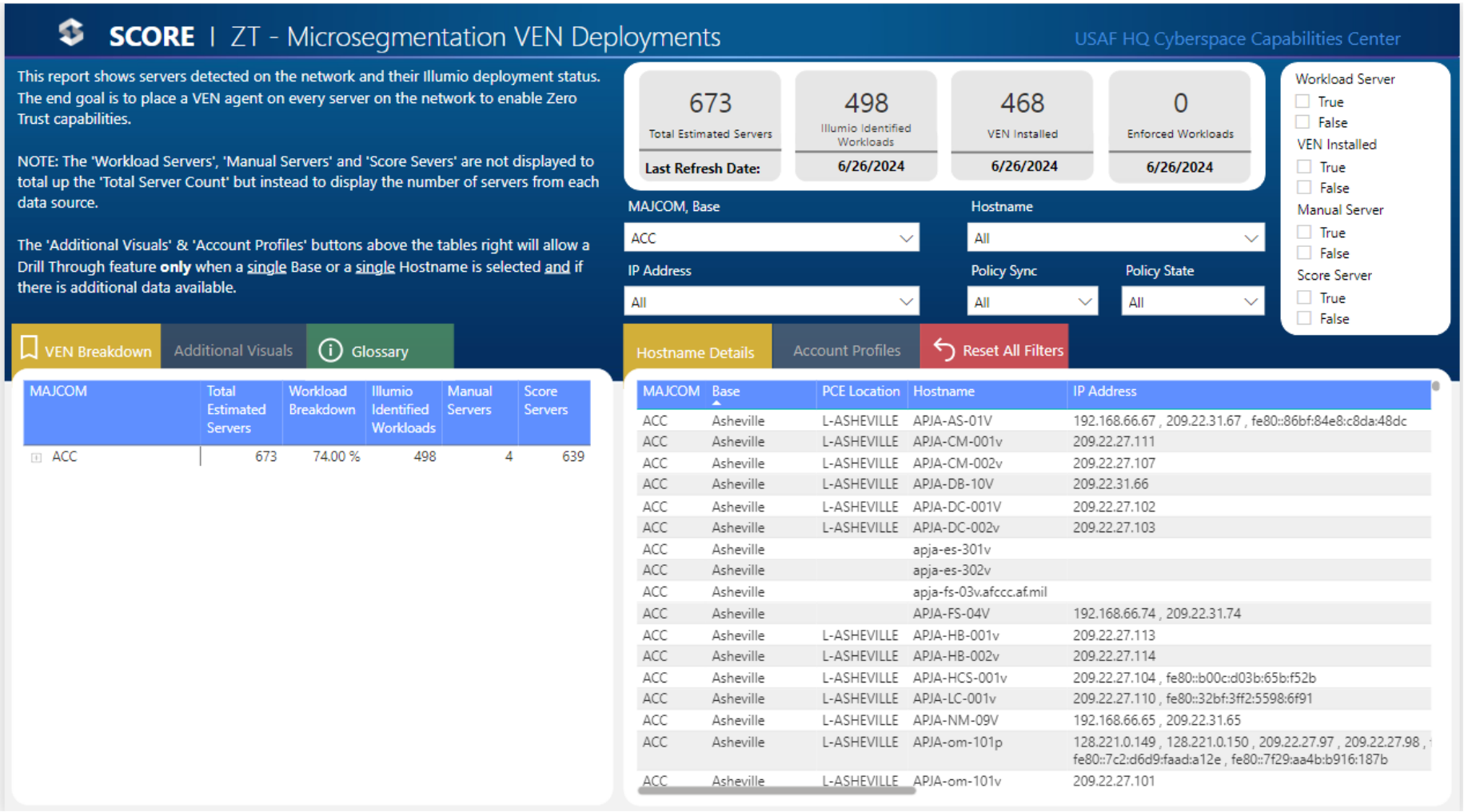
VEN Deployment Overview





MAJCOM	MAJCOM Status	Automated Deployment Status	Servers Requiring Reconciliation	Labeled Unmanaged Workloads	Servers with Exemption	Notes
PACAF	Analysis, Validation & Rule Writing	Complete – 370	415	46	0	Additional servers identified for Elmendorf and Eielson which require analysis and potentially manual install
ANG	VEN Deployment	Complete – 1919	586	4	-	ANG estimates 2505 total servers
USAFE	Ongoing	Complete – 377	868	1	0	Servers requiring reconciliation grows as data is provided through Base Server Questionnaire
ACC	MAJCOM Communications	Complete – 563	Not Started	-	-	MAJCOM Scheduled for July 2024
AFSOC	VEN Deployment	Complete – 64	Not Started	-	-	MAJCOM Scheduled for August 2024
AFMC	VEN Deployment	Complete – 1665	Not Started	-	-	MAJCOM Scheduled for November 2024
AFGSC	VEN Deployment	Complete – 154	Not Started	-	-	MAJCOM Scheduled for January 2025
AMC	VEN Deployment	Complete – 546	Not Started	-	-	MAJCOM Scheduled for March 2025
AETC	VEN Deployment	Complete – 431	Not Started	-	-	MAJCOM Scheduled for July 2025
AFRC	VEN Deployment	Complete – 373	Not Started	-	-	MAJCOM Scheduled for September 2025

VEN Deployment Tracking



Navigate to SCORE Dashboard

Lessons Learned

TASKORDs, TMTs, and Gen Admins not adequately disseminated and executed to collect the necessary data in a timely manner. Better coordination and communication put in place moving forward.

Multiple sources of truth. Leverage automation to cross reference multiple data sources to maximize data accuracy and veracity. Use an MVP mindset allowing forward progress while data certainty improves.

Inadequate data and long responses cycles resulted in process delays. Data request are consolidated into one view to improve data collection progress and reduce response time.

Activate key leaders early to receive buy-in for upcoming activities. Request liaisons to support with important insights about the MAJCOM and identify potential resistance to tailor outreach communications.

Lack of standardization in approach and terminology. The MS Team is establishing standardization in rule writing process, governance, key project terms and more.

The DAF's Zero Trust Journey

Upcoming 2024 Engagement…

AFA Air, Space, and Cyber; TechNet Indo-Pacific; Alamo ACE

Still curious about microsegmentation efforts, or the path forward with new Zero Trust capabilities?
Contact Mr. Jim Pickard directly, @ james.pickard@us.af.mil


MICROSEGMENTATION
ZERO TRUST
TRANSITION TEAM
ILLUMINATE • CONTAIN • CONTROL

Q&A


MICROSEGMENTATION
ZERO TRUST
TRANSITION TEAM
ILLUMINATE • CONTAIN • CONTROL

Thank you!