SAF/CN

Publication: 23 OCT 2024

DAF ENTERPRISE ZERO TRUST ROADMAP | *COVER PAGE*

Adapting and Modernizing DAF's Cybersecurity Architecture to enhance security and mission performance for the warfighter

Increasing competition on the global stage necessitates a more modern security architecture to protect our critical business and mission systems and promote digital readiness. The DAF intends to implement a Zero Trust (ZT) security posture in alignment with the DoD Zero Trust Strategy.

Implementing Zero Trust Will Advance the CIO Strategic Priorities and Address the DoD ZT Mandate

Implementing a Zero Trust architecture touches many areas of our IT delivery ecosystem and encapsulates everything DAF delivers.

CIO Strategy LOEs

The DAF CIO Public Strategy was published in September of 2022 and introduced six primary Lines of Effort (LOEs) to support DAF's IT priorities through FY23-FY28.

The LOEs directly address the needs of DAF's emerging strategic and technological environment. The implementation of Zero Trust is critical to the advancement of the three LOEs highlighted below.

1. Accelerate Cloud Adoption
2. **Future of Cybersecurity**
3. Workforce
4. IT Portfolio Management
5. **Excellence in Core IT & Mission Enabling Services**
6. **Data and AI**

September 2021

Sec. 1528 of NDAA for FY22

Instructed DoD CIO and US Cyber Command to jointly develop an implementation strategy for zero trust architecture across DoD's information network.

January 2022

OMB Policy Memo 22-09

Provided strategic guidance to departments and agencies and directed the achievement of specific zero trust security goals by the end of FY24.

October 2022

DoD Zero Trust Strategy

*Defined an approach for agencies to adopt and accelerate a modern ZT architecture. The DoD ZT Strategy requires all agencies to adopt, integrate, and operationalize baseline capabilities across **7 DoD-defined ZT Pillars by FY27**.*

April 2024

DAF Zero Trust I-Plan 1.2

Received SECAF signature after coordination with DAF EIT/Cyber community. This document is pivotal in outlining how the FMO is increasing ZT readiness and implementing ZT across the DAF.

July 2024

DAF Zero Trust Strategy

Published by SAF/CN in partnership with ACC to align the DoD ZT Strategy and DAF I-Plan with a focus on the higher-level strategic narratives that underpin capability delivery supporting ZT.

What is the Current State of DAF Zero Trust Maturity?

USER

Early Enterprise ICAM delivery to address inconsistent authentication and access management controls

DATA

Leveraging data brokers and platforms to provide policy enforcement around granular data pieces

DEVICE

Device management continues to mature but is still disconnected from authorization decisions

APPLICATION & WORKLOADS

Application protections are inconsistently applied across the enterprise

NETWORK & ENVIRONMENT

VPN as the primary tool to secure remote access, combined with legacy network practices

VISIBILITY & ANALYTICS

Need for integrating application-layer enforcement events with operational tools and processes

AUTOMATION & ORCHESTRATION

API support is nascent as early data automation lacks standardization and expansion

What is the Current State of Zero Trust Execution?

ACC/A60 stood up the DAF ZT FMO to facilitate ZT implementation efforts across-DAF following the publication of the DAF Enterprise ZT Roadmap v.1.0 in February 2023.

BUILT THE INFRASTRUCTURE

- ✓ Received SECAF signature on DAF ZT I-Plan 1.0 in April 2024
- ✓ Built real-time, streamlined task management system
- ✓ Submitted DAF ZT I-Plan 2.0 for internal coordination in August 2024
- ✓ Launched DAF ZT dashboard to report on enterprise progress towards ZT implementation

CENTRALIZED ZT EXECUTION EFFORTS

- ✓ Expanded scope of execution efforts through DAF Non-EIT Summit and DAF ZT SIPR Gap Assessment working session
- ✓ Hosting monthly DAF ZT governance forums to engage on strategy and progress updates
- ✓ Conducting regular ZT implementation progress report outs to Senior Leaders
- ✓ Aligning future year POM planning to ZT execution efforts to identify and mitigate any funding or resource disconnects

The DAF Enterprise Zero Trust Roadmap serves as a strategic guide to coordinate the delivery of Zero Trust enabling services that aim to shift the DAF to a more secure architectural baseline emphasizing robust application security, homogenized data exchange processes, and increased visibility, monitoring, and alerting.

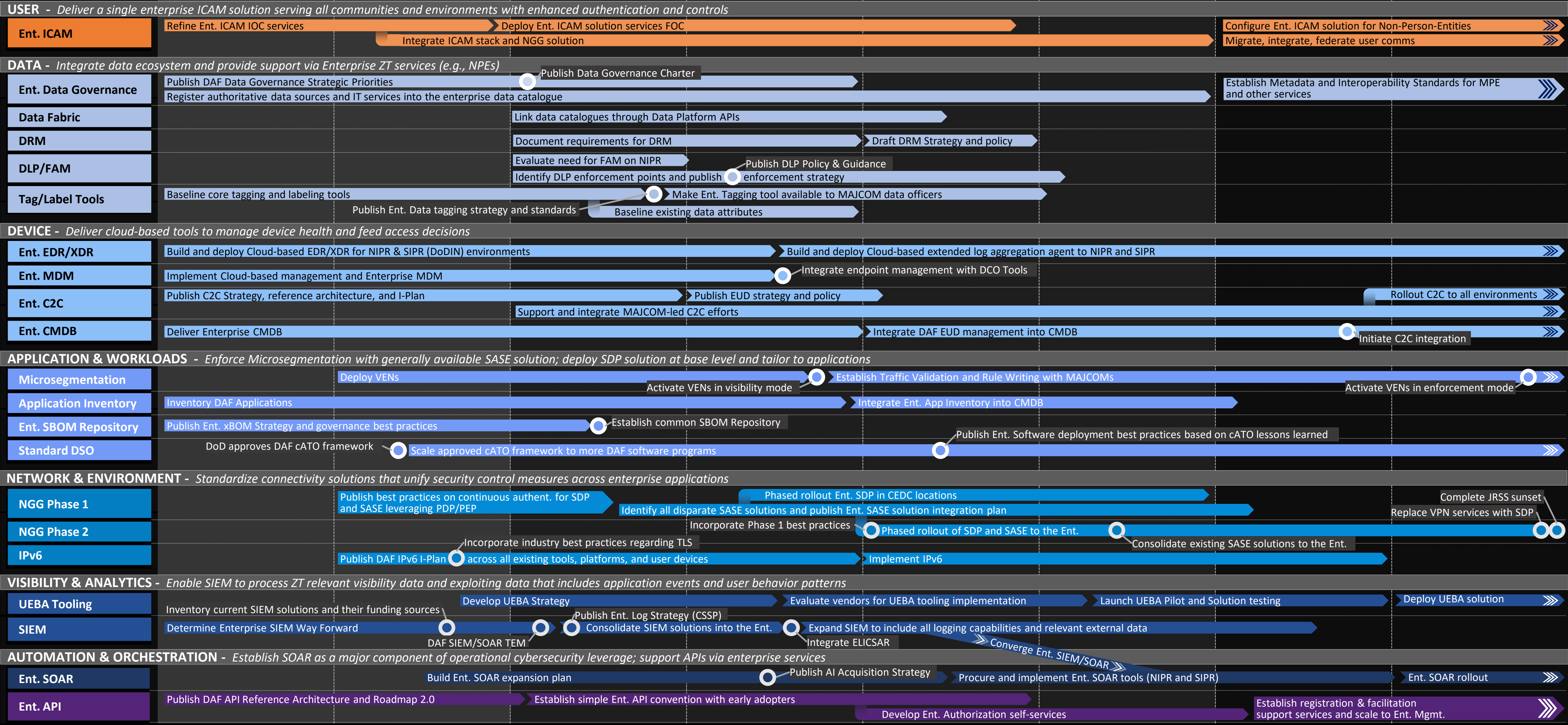
DAF ENTERPRISE ZERO TRUST ROADMAP

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

Publication: 23 OCT 2024

PILLARS & COMPONENTS	FY24	FY25	FY26+
	Focus on defining Enterprise services to drive ZT architecture, services, and delivery of identity and endpoint components.	*Continue scaling capability delivery, driving onboarding and defining advanced capabilities (e.g., API, AI/ML).*	*Drive comprehensive integration to consolidate services and replace with enterprise solutions for a seamless rollout across all environments.*
	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*

Ent. ICAM
- Refine Ent. ICAM IOC services
- Deploy Ent. ICAM solution services FOC
- Integrate ICAM stack and NGG solution
- Configure Ent. ICAM solution for Non-Person-Entities
- Migrate, integrate, federate user comms

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

Ent. Data Governance
- Publish DAF Data Governance Strategic Priorities
- Publish Data Governance Charter
- Register authoritative data sources and IT services into the enterprise data catalogue
- Establish Metadata and Interoperability Standards for MPE and other services

Data Fabric
- Link data catalogues through Data Platform APIs

DRM
- Document requirements for DRM
- Draft DRM Strategy and policy

DLP/FAM
- Evaluate need for FAM on NIPR
- Identify DLP enforcement points and publish enforcement strategy
- Publish DLP Policy & Guidance

Tag/Label Tools
- Baseline core tagging and labeling tools
- Make Ent. Tagging tool available to MAJCOM data officers
- Publish Ent. Data tagging strategy and standards
- Baseline existing data attributes

DEVICE - *Deliver cloud-based tools to manage device health and feed access decisions*

Ent. EDR/XDR
- Build and deploy Cloud-based EDR/XDR for NIPR & SIPR (DoDIN) environments
- Build and deploy Cloud-based extended log aggregation agent to NIPR and SIPR

Ent. MDM
- Implement Cloud-based management and Enterprise MDM
- Integrate endpoint management with DCO Tools

Ent. C2C
- Publish C2C Strategy, reference architecture, and I-Plan
- Publish EUD strategy and policy
- Rollout C2C to all environments
- Support and integrate MAJCOM-led C2C efforts

Ent. CMDB
- Deliver Enterprise CMDB
- Integrate DAF EUD management into CMDB
- Initiate C2C integration

APPLICATION & WORKLOADS - *Enforce Microsegmentation with generally available SASE solution; deploy SDP solution at base level and tailor to applications*

Microsegmentation
- Deploy VENs
- Activate VENs in visibility mode
- Establish Traffic Validation and Rule Writing with MAJCOMs
- Activate VENs in enforcement mode

Application Inventory
- Inventory DAF Applications
- Integrate Ent. App Inventory into CMDB

Ent. SBOM Repository
- Publish Ent. xBOM Strategy and governance best practices
- Establish common SBOM Repository

Standard DSO
- DoD approves DAF cATO framework
- Scale approved cATO framework to more DAF software programs
- Publish Ent. Software deployment best practices based on cATO lessons learned

NETWORK & ENVIRONMENT - *Standardize connectivity solutions that unify security control measures across enterprise applications*

NGG Phase 1
- Publish best practices on continuous authent. for SDP and SASE leveraging PDP/PEP
- Phased rollout Ent. SDP in CEDC locations
- Identify all disparate SASE solutions and publish Ent. SASE solution integration plan
- Complete JRSS sunset
- Replace VPN services with SDP

NGG Phase 2
- Incorporate Phase 1 best practices
- Phased rollout of SDP and SASE to the Ent.
- Consolidate existing SASE solutions to the Ent.

IPv6
- Incorporate industry best practices regarding TLS
- Publish DAF IPv6 I-Plan
- across all existing tools, platforms, and user devices
- Implement IPv6

VISIBILITY & ANALYTICS - *Enable SIEM to process ZT relevant visibility data and exploiting data that includes application events and user behavior patterns*

UEBA Tooling
- Develop UEBA Strategy
- Evaluate vendors for UEBA tooling implementation
- Launch UEBA Pilot and Solution testing
- Deploy UEBA solution

SIEM
- Inventory current SIEM solutions and their funding sources
- Determine Enterprise SIEM Way Forward
- DAF SIEM/SOAR TEM
- Publish Ent. Log Strategy (CSSP)
- Consolidate SIEM solutions into the Ent.
- Expand SIEM to include all logging capabilities and relevant external data
- Integrate ELICSAR
- Converge Ent. SIEM/SOAR

AUTOMATION & ORCHESTRATION - *Establish SOAR as a major component of operational cybersecurity leverage; support APIs via enterprise services*

Ent. SOAR
- Build Ent. SOAR expansion plan
- Publish AI Acquisition Strategy
- Procure and implement Ent. SOAR tools (NIPR and SIPR)
- Ent. SOAR rollout

Ent. API
- Publish DAF API Reference Architecture and Roadmap 2.0
- Establish simple Ent. API convention with early adopters
- Develop Ent. Authorization self-services
- Establish registration & facilitation support services and scale to Ent. Mgmt.

SAF/CN
10/23/24

DAF ENTERPRISE ZERO TRUST ROADMAP 2.0

RELEASE NOTES

EDITORIAL NOTES

The SAF initially published the Zero Trust Roadmap in February 2023 and followed up the initial publication with a second release in June 2023 and third release in December 2023. This roadmap update reflects the status of Zero Trust progress as a snapshot in time and will continue to serve as a guide for cross-enterprise adoption and execution.

SAF/CN has engaged with the DAF Zero Trust FMO (out of ACC/A6) to compile real-time adjustments to ensure this update encapsulated progress when viewed against the multi-faceted ZT plan. Changes to Roadmap milestones' timing and language provide an accurate snapshot of projected plans and an increased level of clarity and specificity.

✓ WHAT'S BEEN ACCOMPLISHED?

- Awarded Enterprise ICAM 2 Contract
- Drafted and released Enterprise C2C I-Plan for internal DAF coordination
- Completed Remedy transition to "read only" mode and deployed fully operational ITSM 3.0
- Initiated VENs deployment to endpoints for Microsegmentation implementation and published Microsegmentation Playbook
- Released EUD Strategy draft to internal DAF coordination
- Published the DAF API Reference Architecture and Roadmap 1.0
- Drafted and released xBOM Strategy for internal DAF coordination
- Held NGG PMO facilitated Phase 1 Critical Design Review
- Deployed NIPRGPT tool and 2025 AI Acquisition Guidebook drafted to incorporate ZT equities
- Deployed ELX solution to initial CEDC locations
- Developed UEBA requirements package and initiated solution gathering

IDENTIFIED CHALLENGES

IDENTIFIED CHALLENGE	NGG Phase 2 Delays	Pending SIEM/SOAR Integration Plan and Way Forward	Delay of Funding for C2C	Enterprise ICAM adoption and driving central authorization management
MITIGATION PLAN	*Acquisition community to develop an acquisition strategy after evaluating various COAs*	*Operational community to formalize platform selection and begin integration*	*MAJCOM-led efforts will continue through FY26*	*Technical and business process realignment acceleration support needed*

NEXT QUARTER'S PRIORITIES…

- Continue development of Cloud-based EDR/EXR implementation and enterprise integration efforts
- Complete deployment of Microsegmentation VENs
- Develop UEBA implementation strategy
- Publish Enterprise log strategy and determine Enterprise SIEM way forward
- Continue building Enterprise SOAR expansion plan and publish AI Acquisition strategy

DAF ENTERPRISE ZERO TRUST ROADMAP | *ACRONYMS AND EXPANSIONS*

SAF/CN
10/23/24

Acronym	Expansion
AI	Artificial Intelligence
API	Application Programming Interface
C2C	Comply-to-Connect
cATO	Continuous Authorization to Operate
CEDC	Component Enterprise Data Center
CMDB	Configuration Management Database
COA	Course of Action
CSSP	Cloud Software Service Provider
DCO	Defensive Cyber Operations
DSO	Development, Security, and Operations
DLP	Data Loss Prevention
DoDIN	Department of Defense Information Networks
DRM	Digital Rights Management
EDR	Endpoint Detection and Response
EIT	Enterprise Information Technology
ELICSAR	Enterprise Logging Ingest and Cyber Situational Awareness Refinery
ELX	Enterprise Logging Xtreme
Ent.	Enterprise
EUD	End User Device
FAM	File Activity Monitoring

Acronym	Expansion
FOC	Full Operational Capability
ICAM	Identity, Credential, and Access Management
I-Plan	Implementation Plan
IPv6	Internet Protocol Version 6
IOC	Initial Operational Capability
ITSM	Information Technology Service Management
JRSS	Joint Regional Security Stacks
LOE	Level of Effort
MDM	Mobile Device Management
ML	Machine Learning
MPE	Mission Partner Environment
NDAA	National Defense Authorization Act
NGG	Next Generation Gateway
NIPRNet	Non-secure Internet Protocol Routed Network
NPE	Non-Person-Entity
OMB	Office of Management and Budget
PAM	Privileged Access Management
PDP/PEP	Policy Decision Point/Policy Enforcement Point
PMO	Project Management Office
POM	Program Objective Memorandum

Acronym	Expansion
SASE	Secure Access Service Edge
SBOM	Software Bill of Materials
SDP	Software-Defined Perimeter
SIEM	Security Information & Event Management
SIPRNet	Secure Internet Protocol Routed Network
SOAR	Security Orchestration, Automation and Response
TLS	Transport Layer Security
UEBA	User and Entity Behavior Activity
VEN	Virtual Enforcement Node
VPN	Virtual Private Network
xBOM	Extensible Bill of Materials
XDR	Extended Detection and Response
ZT	Zero Trust