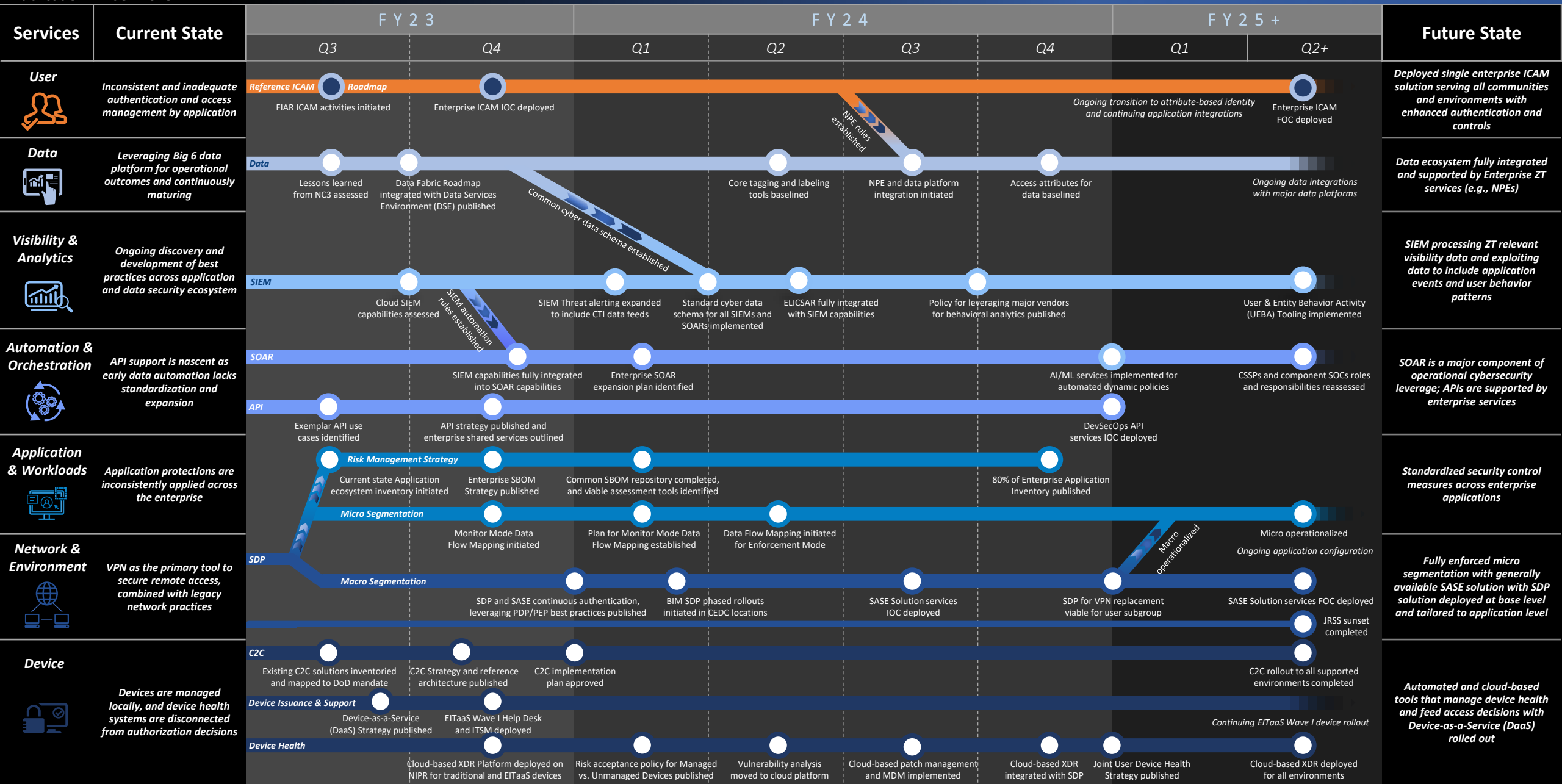
DAF ENTERPRISE ZERO TRUST ROADMAP

Publication: 12 JUL 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*



SAF/CN
7/12/2023

DAF ENTERPRISE ZERO TRUST ROADMAP

RELEASE NOTES

EDITORIAL NOTES

Following publication in February 2023, SAF/CN updated this roadmap to accurately reflect the status of DAF Enterprise Zero Trust as a snapshot in time so that it can continue to serve as a guide to the cross-enterprise adoption and execution of Zero Trust.

To ensure this update encapsulated the multi-faceted implications of ZT, we aligned the roadmap to the DoD Zero Trust Framework and re-engaged extensively with ZT DAF stakeholders, industry partners, and other government stakeholders for feedback while gaining clarity on sequencing of milestones. This collaborative effort led us to not only rethink and refine a variety of milestones, but also our roadmap update processes as well.

The next iteration will leverage DAF Zero Trust FMO's task management system (out of ACC/A60) to ensure that updates are streamlined and based off real-time data.

WHAT'S BEEN ACCOMPLISHED?

- Began ICAM FIAR integrations for first two groupings of FIAR systems
- Established phasing for way ahead for Next Gen Gateway (NGG) and Micro Segmentation (M-S)
- Reached consensus on C2C's strategic way forward via phased approach to Enterprise consolidation
- Stood up ZT FMO to begin implementation and coordination with DoD ZT PfMO
- Continued consolidation and modernization of end user device baseline by Cloud-based device management
- Launched Data Services Environment (DSE) and metadata maturity assessments
- Reformatted roadmap services to better align with DoD ZT Strategy

NEXT QUARTER'S PRIORITIES…

- Publish DAF Enterprise Zero Trust Strategy
- Continue FIAR application migration for ICAM
- Establish IOC and FOC conditions for Micro Segmentation (M-S), Next Gen Gateway (NGG), and Extended Detection & Response (XDR)
- Publish and socialize C2C Strategy and reference architecture
- EITaaS Wave I fully underway
- Develop Zero Trust Implementation Plan and present to Congress

WHAT'S CHANGED?

SERVICE	SWIMLANE	UPDATES TO ROADMAP
THEME: Alignment to DoD Zero Trust Framework		
General Updates	N/A	Changed names of Zero Trust services to match DoD Zero Trust Pillars; Updated both the Current State and Future State language for services
Policy	N/A	Removed Policy service from roadmap and reallocated the Policy milestones to their applicable services/swimlanes
Continuous Monitoring	N/A	Removed Continuous Monitoring service and added Automation & Orchestration and Visibility & Analytics services in its place; Reallocated Continuous Monitoring milestones throughout roadmap in alignment with DoD's framework
Visibility & Analytics	SIEM	Broke out SIEM swimlane from original SIEM/SOAR swimlane and updated/added new milestones accordingly based on the status of related tasks; Added convergence from SIEM swimlane to SOAR swimlane to reflect the upcoming integration efforts planned for these two solutions
Automation & Orchestration	API	Moved API swimlane from Application service to Automation & Orchestration service
THEME: Clarity, Specificity, & Consistency		
User	ICAM	Shifted 'Enterprise ICAM FOC deployed' milestone back from FY24 Q2 to FY25 Q2+ to align with latest ICAM roadmap timeline
Data	Data	Shifted 'Lessons learned from NC3 assessed' milestone up from FY24 Q1 to FY23 Q3 to reflect latest progress; Added updated language to 'Data Fabric Roadmap published' milestone; Added convergence from Data swimlane to SIEM swimlane to show when a common cyber data schema will be established
Applications & Workloads	Risk Mgmt. Strategy	Changed language in first milestone from 'Current state Application ecosystem inventoried' to 'Current state Application ecosystem inventory initiated'
	Micro Segmentation	Shifted both 'Monitor Mode Data Flow Mapping initiated' and 'Data Flow Mapping initiated for Enforcement Mode' milestones back a quarter to reflect latest timeline of anticipated tasks; Added new milestone in between these two milestones (in FY24 Q1); Shifted 'SASE Solution services IOC deployed' milestone back a quarter and moved it down to the Macro Segmentation swimlane because it is more closely aligned to SDP-related tasks
Network & Environment	Macro Segmentation	Removed 'PACAF SDP Pilots deployed' milestone to reflect latest decision for these pilots to cease and desist; Added additional milestone (from original Policy swimlane) in late FY23 Q4 and another in FY25 Q2+ to show timeline for when SASE solution FOC will be deployed; Added clarifying language to 'BIM SDP phased rollouts initiated' milestone to clarify that the initial phase of NGG execution will begin with CEDC locations before transitioning to Special Purpose Processing Nodes (SPPNs)
Device	Device Issuance & Support	Updated name of swimlane to better reflect milestones (originally "Device Inventory"); Updated "Device 4 Life" language in first milestone to "Device-as-a-Service (DaaS)" to reflect a recent name change for this effort
	Device Health	Added two milestones (from original Policy swimlane) and updated both milestones' timing and sequencing; Added in two net-new milestones to show cloud-related tasks in FY24

DAF ENTERPRISE ZERO TRUST ROADMAP | ACRONYMS AND DEFINITIONS

Acronym/Term	Definition
AI	Artificial Intelligence
API	Application Programming Interface
BIM	Base Infrastructure Modernization
C2C	Comply-to-Connect
CEDC	Component Enterprise Data Center
CSSPs	Cloud Software Service Providers
CTI	Cyber Threat Intelligence
DAF	Department of the Air Force
DaaS	Device-as-a-Service
DevSecOps	Development, Security, and Operations
DSE	Data Services Environment
EITaaS	Enterprise Information Technology-as-a-Service
ELICSAR	Enterprise Logging Ingest and Cyber Situational Awareness Refinery
FIAR	Financial Improvement and Audit Readiness
FOC	Full Operational Capability
ICAM	Identity, Credential, and Access Management
IOC	Initial Operational Capability
ITSM	Information Technology Service Management

Acronym/Term	Definition
JRSS	Joint Regional Security Stacks
MDM	Mobile Device Management
ML	Machine Learning
NC3	Nuclear Command, Control, and Communications
NIPR	Non-secure Internet Protocol Router
NPE	Non-Person-Entity
PDP/PEP	Policy Decision Point/Policy Enforcement Point
SASE	Secure Access Service Edge
SBOM	Software Bill of Materials
SDP	Software-Defined Perimeter
SIEM	Security Information & Event Management
SOAR	Security Orchestration, Automation and Response
SOC	Security Operations Center
UEBA	User and Entity Behavior Activity
VPN	Virtual Private Network
XDR	Extended Detection and Response