DoD Zero Trust Capability Execution Roadmap (COA 1)

06 January 2023

There is one destination (ZT) with many paths (COAs) – COA 1 will be the focus

Focus of this Briefing

COA 1

ZT Baseline

- Leverages current infrastructure and environment using Brownfield approach
- Zero Trust “on the ground” modernization: ~ 5+ yr. (FYDP beginning FY23) Implementation Plan
- Establishes set capabilities and activities needed to achieve Target and Advanced-levels of Zero Trust
- No constraints on tools or methods to accomplish ZT

Under Development

COA 2

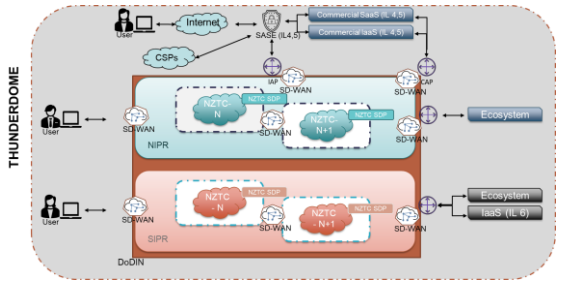
Commercial Cloud

- Relies on commercial provider(s) to develop ZT compliant cloud environments using Greenfield approach
- Achieves DoD ZT quicker than COA-1
- Mandate would be to achieve DoD ZT “Target” level, at a minimum
- Provides standardized tools and capabilities to support ZT execution

COA 3

Private Cloud

- Government Owned/Operated high-performance Native ZT Cloud (NZTC) using Greenfield approach
- Achieves DoD ZT quicker than COA-1
- Achieves immediate DoD ZT “Advanced” level by design, which needs to be independently validated



Zero Trust by 2027

Over the last several months, the ZT Portfolio Management Office (PfMO) has worked to establish the capabilities necessary to successfully accomplish Zero Trust, and laid them out on a roadmap for execution across the DoD with the following method:

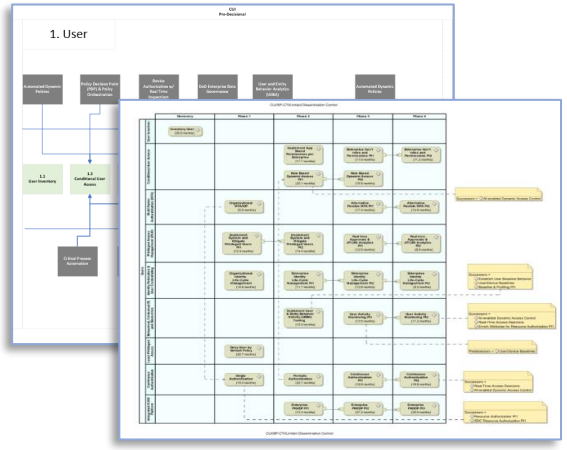
Define

Zero Trust Capability Planning
as of: 04-05-2022 0930

ID #	Capability	Pillar	Increment	Predecessor(s)	Successor(s)	Capability Achieved (Target FY)	Capability Description (Outcome)
1.1	User Inventory	1 - User	Increment 1	None Identified	1.2	FY2023	System owners have control (visibility and administrative rights) of all authorized and authenticated users on the network
1.2	User Credentialing (Good)	1 - User	Increment 1	1.1	1.3	FY2023	DoD organizations manually issue, manage, and revoke credentials bound to DoD user identities
1.3	Conditional User Access (Good)	1 - User	Increment 1	1.2; 5.2	1.4; 1.5; 1.8; 1.9	FY2023	DoD organizations control user access to DAAS based on real-time user attributes and situational awareness
1.4	Multi-Factor Authentication (MFA)	1 - User	Increment 1	1.3	1.6; 1.7	FY2023	DoD organizations require users to authenticate using at least two of the following three attributes: knowledge (user ID/password), possession (CAC/token), or something you are (inherence, e.g., iris/fingerprints), in order to access DAAS resources
1.5	Privileged Access Management (PAM)	1 - User	Increment 1	1.3	1.9	FY2023	DoD organizations control, monitor, secure, and audit privileged identities across their IT environments
1.6	Identity Federation	1 - User	Increment 2	1.4	1.11	FY2024	DoD organizations develop and share identity information across entities and trust domains providing "single sign-on" convenience and efficiencies to identified

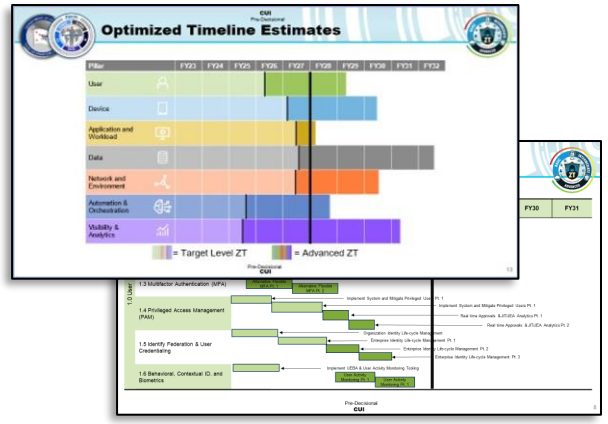
Producing a common lexicon on capability descriptions, outcomes, and impact statements, activity outcomes, and providing appropriate references were the necessary first steps

Understand and Contextualize



Realizing the relationships and dependencies helped to drive timeline development

Develop and Refine

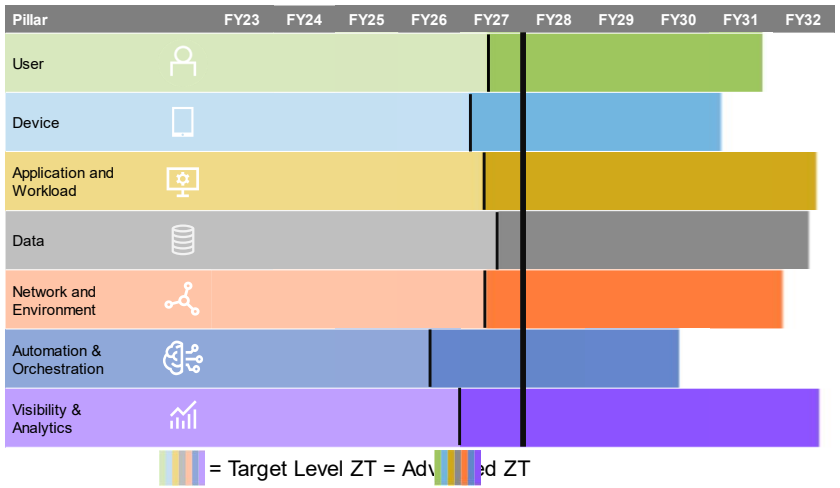


Multiple iterations resulted in one primary COA, opportunities for acceleration with cloud, and other considerations supporting an executable plan

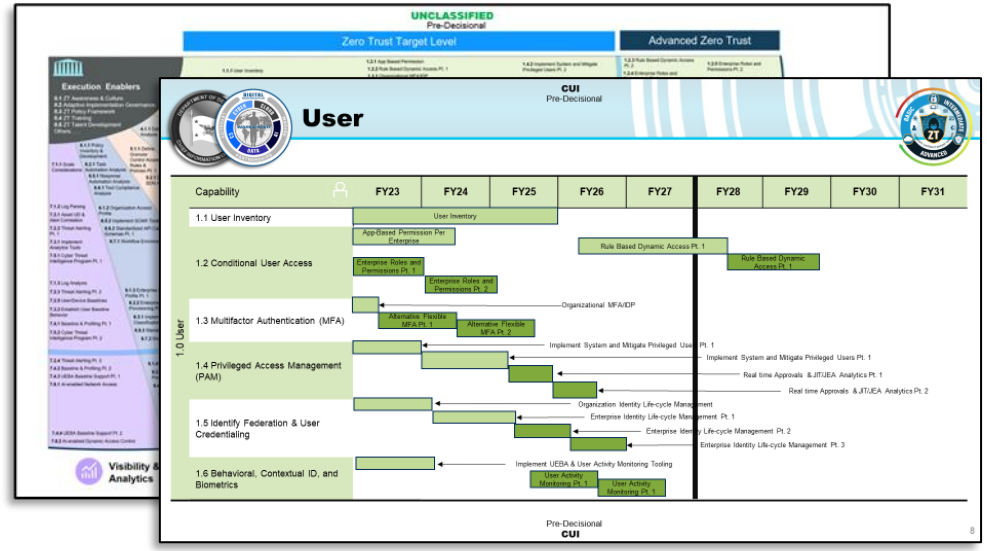
The resulting plan supports the execution of Zero Trust across the DoD to the required level by FY2027

The Concept of COA 1

This stage was primarily about defining "WHAT" the DoD needed to do execute ZT – agnostic of COAs



With this methodology, one iteration emerged as the final timeline



What follows are layers of analysis and explanation to support the detailed execution of the plan over time

*Timelines and activity durations did account for high-level research-based considerations around these critical elements

<u>Other Considerations – More to Come*</u>

Limited development could be done in these areas until ZT capabilities were defined and mapped out

Budget and Acquisition – Capabilities were spread out over time with these concerns in mind, but will require much deeper considerations at the capability and activity level

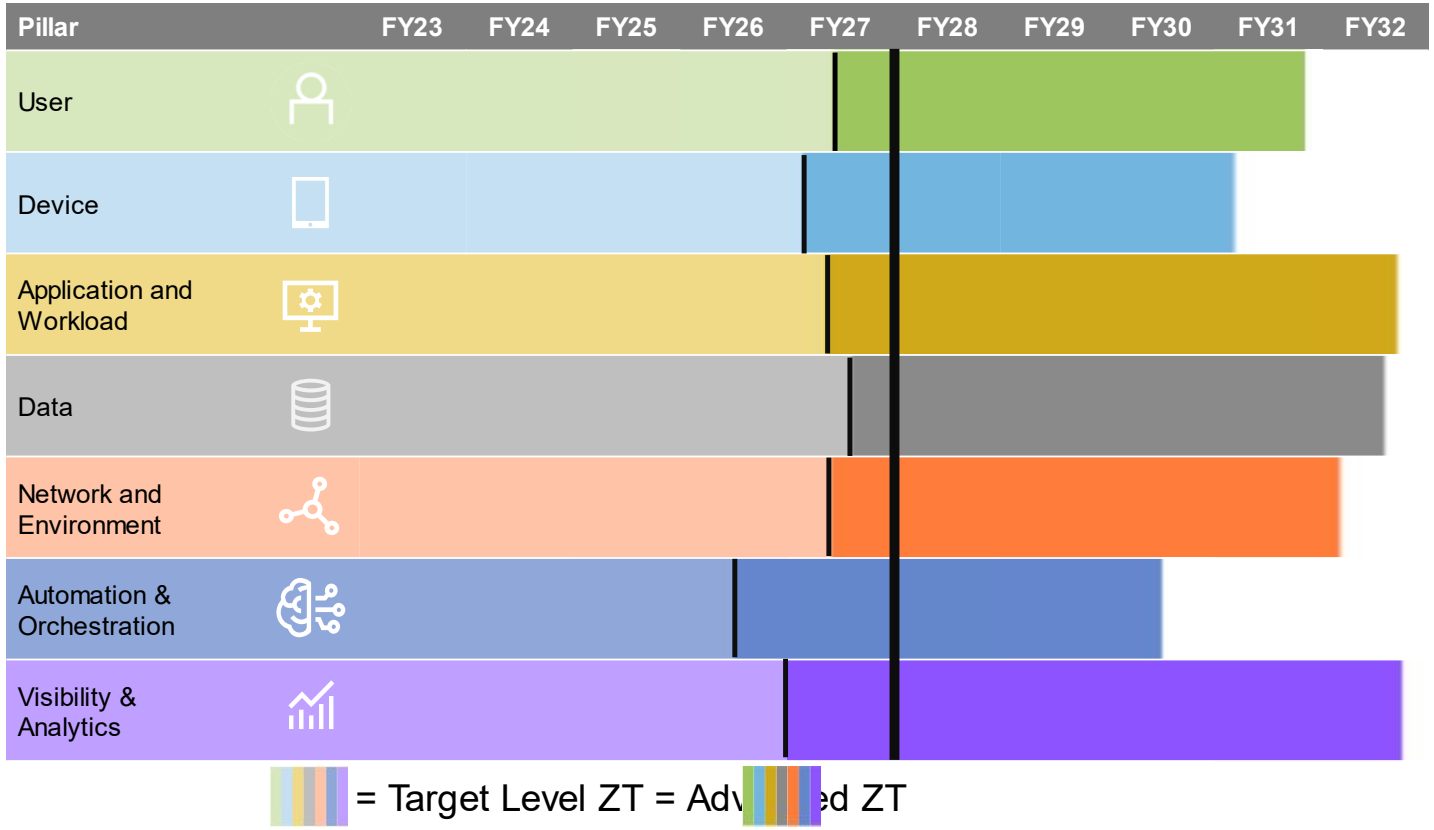
Technical Implementation – Defines "how" to accomplish ZT – COA 1 is about allowing organizations to choose their own methods. COA 2 /3 will better address this. More guidance is coming on controls associated with capabilities, and implementation strategies

Table of Contents

Appendices

COA 1 Recommendations and Other Relevant Timelines

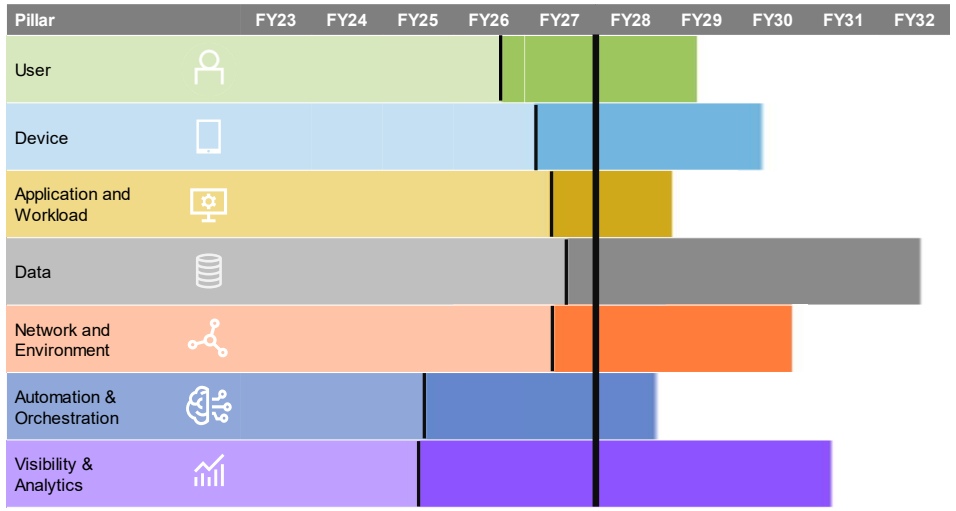
After multiple iterations, this timeline is now “COA 1 (DoD Baseline)”



Balances an aggressive approach to achieving “Target Level ZT” by FY27 with the DoD Budget Cycle by distributing activities over the FYDP and setting Department-Wide expectations

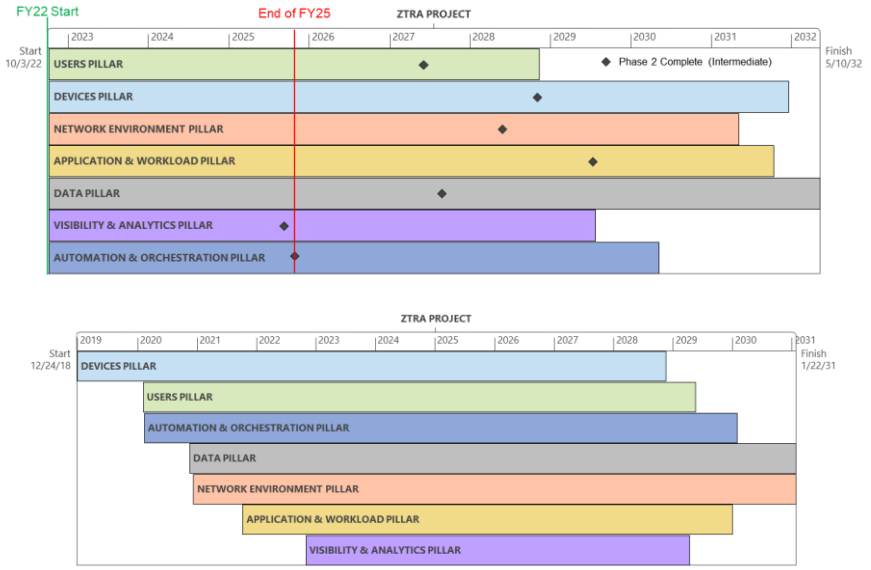
See Appendix A for methodology

Other timelines provide amplifying points and support additional PfMO analysis



<u>DoD Accelerated Baseline</u>:
seeks to achieve "Advanced ZT" more quickly with a more aggressive approach that pushes start dates to the left as much as possible; this accelerated approach is included as an example for organizations seeking to achieve "advanced ZT" more quickly

See Appendix B for methodology



<u>Forward/backward Pass Projections</u>:
assess the likely achievement date of Target and Advanced ZT levels based on risk, duration standard deviations, and cloud employment

Timeline Development and Methodology

Note: “Execution Enablers” as referenced in the following slides are cross-cutting, non-technical capabilities and activities that address culture, governance, and elements of DOTmLPF-P (e.g., ZT Training, etc.) that support the design, development and deployment of the ZT Capabilities required to achieve the DoD Target and Advanced Levels. Details regarding supporting enablers will be further refined and integrated into next versions of the DoD ZT Capability Roadmap and addressed in implementation plans. Enablers identified to-date include: ZT Awareness & Culture, Adaptive Implementation Governance, ZT Policy Framework, ZT Training, and others.

Note: Click on each Capability Title for details

DoD Zero Trust Capabilities

User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
1.1 User Inventory	**2.1** Device Inventory	**3.1** Application Inventory	**4.1** Data Catalog Risk Assessment	**5.1** Data Flow Mapping	**6.1** Policy Decision Point (PDP) & Policy Orchestration	**7.1** Log All Traffic (Network, Data, Apps, Users)
1.2 Conditional User Access	**2.2** Device Detection and Compliance	**3.2** Secure Software Development & Integration	**4.2** DoD Enterprise Data Governance	**5.2** Software Defined Networking (SDN)	**6.2** Critical Process Automation	**7.2** Security Information and Event Management (SIEM)
1.3 Multi-Factor Authentication	**2.3** Device Authorization with Real Time Inspection	**3.3** Software Risk Management	**4.3** Data Labeling and Tagging	**5.3** Macro Segmentation	**6.3** Machine Learning	**7.3** Common Security and Risk Analytics
1.4 Privileged Access Management	**2.4** Remote Access	**3.4** Resource Authorization & Integration	**4.4** Data Monitoring and Sensing	**5.4** Micro Segmentation	**6.4** Artificial Intelligence	**7.4** User and Entity Behavior Analytics
1.5 Identity Federation & User Credentialing	**2.5** Partially & Fully Automated Asset, Vulnerability and Patch Management	**3.5** Continuous Monitoring and Ongoing Authorizations	**4.5** Data Encryption & Rights Management		**6.5** Security Orchestration, Automation & Response (SOAR)	**7.5** Threat Intelligence Integration
1.6 Behavioral, Contextual ID, and Biometrics	**2.6** Unified Endpoint Management (UEM) & Mobile Device Management (MDM)		**4.6** Data Loss Prevention (DLP)		**6.6** API Standardization	**7.6** Automated Dynamic Policies
1.7 Least Privileged Access	**2.7** Endpoint & Extended Detection & Response (EDR & XDR)		**4.7** Data Access Control		**6.7** Security Operations Center (SOC) & Incident Response (IR)	
1.8 Continuous Authentication						
1.9 Integrated ICAM Platform						

EXECUTION ENABLERS — Doctrine | Organization | Training | Material | Leadership & Education | Personnel | Facilities | Policy

Capabilities, Activities, and their dependencies were identified and aligned to ZT Levels

Capabilities

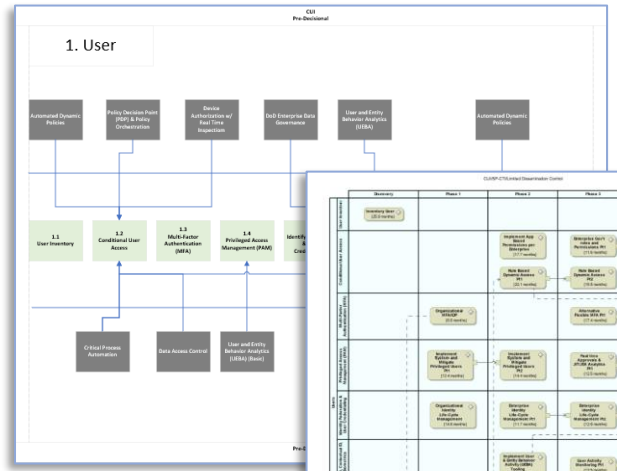
- **1.1** User Inventory
- **1.2** Conditional User Access
- **1.3** Multi-Factor Authentication
- **1.4** Privileged Access Management

Activities and Level

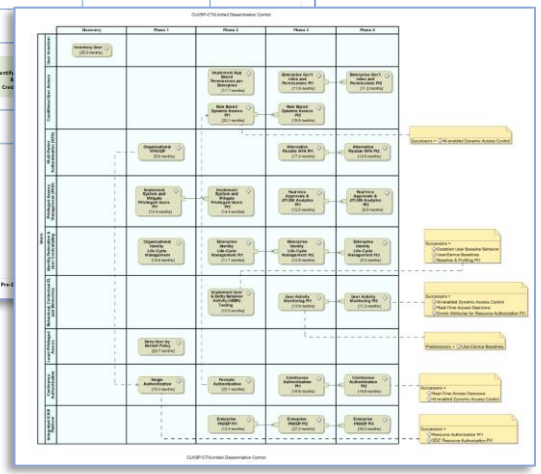
Conditional User Access	
Activity	*Level*
1.2.1 App Based Permissions per Enterprise	ZT Target
1.2.2 Rule Based Dynamic Access Pt1	ZT Target
1.2.3 Rule Based Dynamic Access Pt2	Advanced ZT
1.2.4 Enterprise Gov't roles and Permissions Pt1	Advanced ZT
1.2.5 Enterprise Gov't roles and Permissions Pt2	Advanced ZT

Capabilities break down into activities with associated ZT Levels to better support appropriate sequencing and recognize predecessor, successor relationships

Predecessor and Successor Relationships



Cross-pillar Capability Dependencies

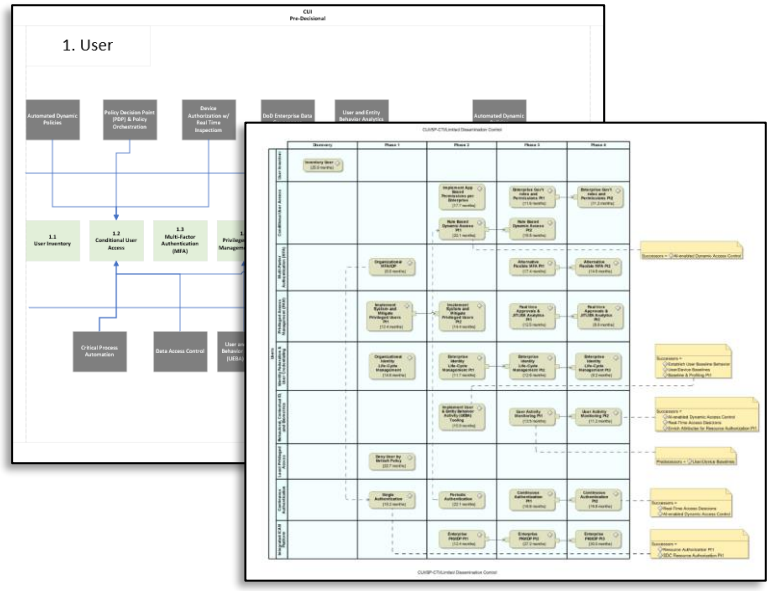


Pillar and Cross-Pillar Activity Dependencies

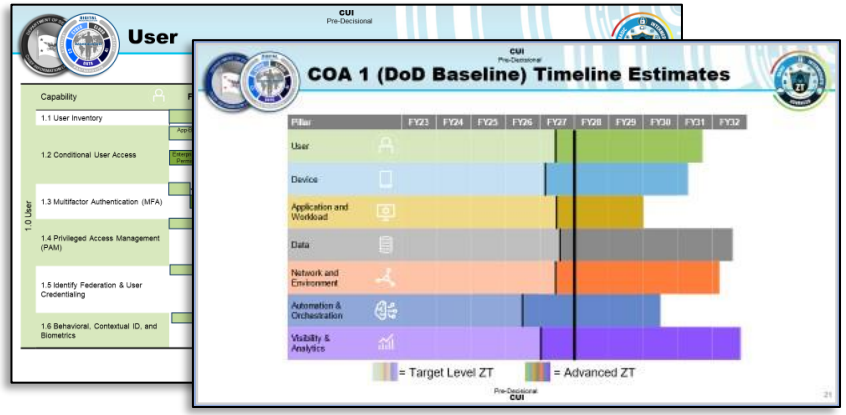
ZT Target Level = All DoD organizations must achieve this level
Advanced ZT = Certain organizations must reach this level based on system and information sensitivity

Timelines were developed by fixing the activities to a set starting point

All DoD organizations are expected to achieve ZT Target Level by 2027



Activities & Durations – Each activity has time duration assigned. Durations were calculated using a DELPHI method employing three teams to determine the required level of effort. The durations were laid out over time based on the dependency relationships established



Set Starting Point – If capabilities are laid out over time starting at 2023 and with all Target levels completed by 2027

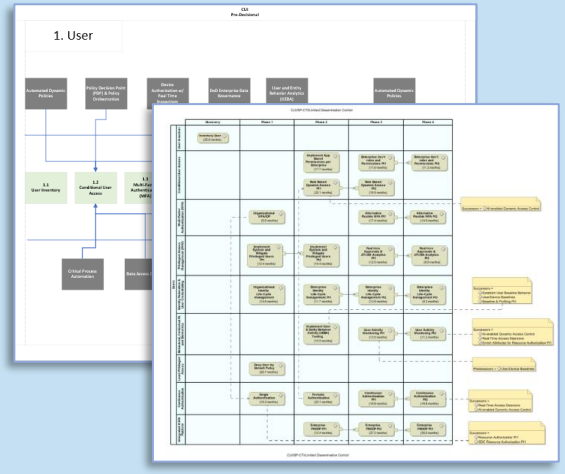
Multiple timelines were generated for analysis

The capabilities and activities, plus their associated durations, ZT Target designations, and sequencing dependencies were entered into an MS Project File (attached)

- **1.1** User Inventory
- **1.2** Conditional User Access
- **1.3** Multi-Factor Authentication
- **1.4** Privileged Access Management

Conditional User Access

Phase Activity	*Phase*	*ZT Target*	*PERT*
1.2.1 App Based Permissions per Enterprise	2	ZT Target	17.7 mons
1.2.2 Rule Based Dynamic Access Pt1	2	ZT Target	22.1 mons
1.2.3 Rule Based Dynamic Access Pt2	3	Advanced ZT	15.5 mons
1.2.4 Enterprise Gov't roles and Permissions Pt1	3	Advanced ZT	11.6 mons
1.2.5 Enterprise Gov't roles and Permissions Pt2	4	Advanced ZT	11.2 mons

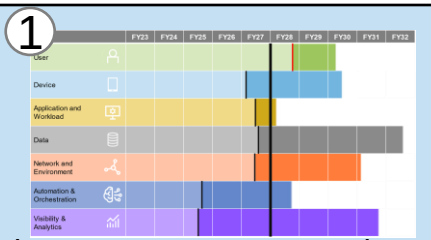


MS Project File

Task Name	Duration	MITRE Phase	ZT Target	Start	Finish
7 Visibility & Analytics	107.85 mons?			Sat 10/1/22	Tue 1/7/31
7.1 Log All Traffic (Network, Data, Apps, Users)	12.6 mons			Sat 10/1/22	Tue 9/19/23
7.1.1 Scale Considerations	353 edays	Discovery	ZT Target	Sat 10/1/22	Tue 9/19/23
7.1.2 Log Parsing	192 edays	Phase 1	ZT Target	Sat 10/1/22	Tue 4/11/23
7.1.3 Log Analysis	313 edays	Phase 2	ZT Target	Sat 10/1/22	Thu 8/10/23
7.2 Security Information and Event Management (SIEM)	40.05 mons			Sat 10/1/22	Mon 10/27/25
7.2.1 Asset ID & Alert Correlation	310 edays	Phase 1	ZT Target	Tue 4/11/23	Thu 2/15/24
7.2.2 Threat Alerting Pt1	228 edays	Phase 1	ZT Target	Sat 10/1/22	Wed 5/17/23
7.2.3 Threat Alerting Pt2	502 edays	Phase 2	ZT Target	Wed 5/17/23	Mon 9/30/24
7.2.4 Threat Alerting Pt3	392 edays	Phase 3	Advanced ZT	Mon 9/30/24	Mon 10/27/25
7.2.5 User/Device Baselines	395 edays	Phase 2	ZT Target	Sun 1/28/24	Wed 2/26/25
7.3 Common Security and Risk Analytics	25.45 mons			Tue 4/11/23	Sun 3/23/25
7.3.1 Implement Analytics Tools	368 edays	Phase 1	ZT Target	Tue 4/11/23	Sat 4/13/24
7.3.2 Establish User Baseline Behavior	420 edays	Phase 2	ZT Target	Sun 1/28/24	Sun 3/23/25
7.4 User and Entity Behavior Analytics (UE	44.85 mons			Sun 1/28/24	Wed 7/7/27
7.4.1 Baseline & Profiling Pt1	374 edays	Phase 2	ZT Target	Sun 1/28/24	Wed 2/5/25
7.4.2 Baseline & Profiling Pt2	690 edays	Phase 3	Advanced ZT	Wed 2/5/25	Sun 12/27/26
7.4.3 UEBA Baseline Support Pt1	192 edays	Phase 3	Advanced ZT	Wed 2/5/25	Sat 8/16/25
7.4.4 UEBA Baseline Support Pt2	192 edays	Phase 4	Advanced ZT	Sun 12/27/26	Wed 7/7/27

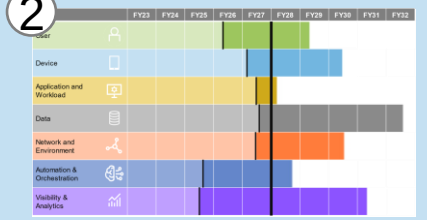
Dates are calculated start and finish from the activity level through the pillar level

1



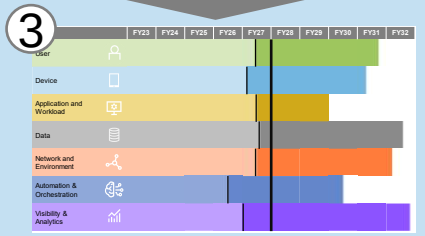
The initial outcomes were mapped to visualize when pillars would achieve the ZT Target levels

2



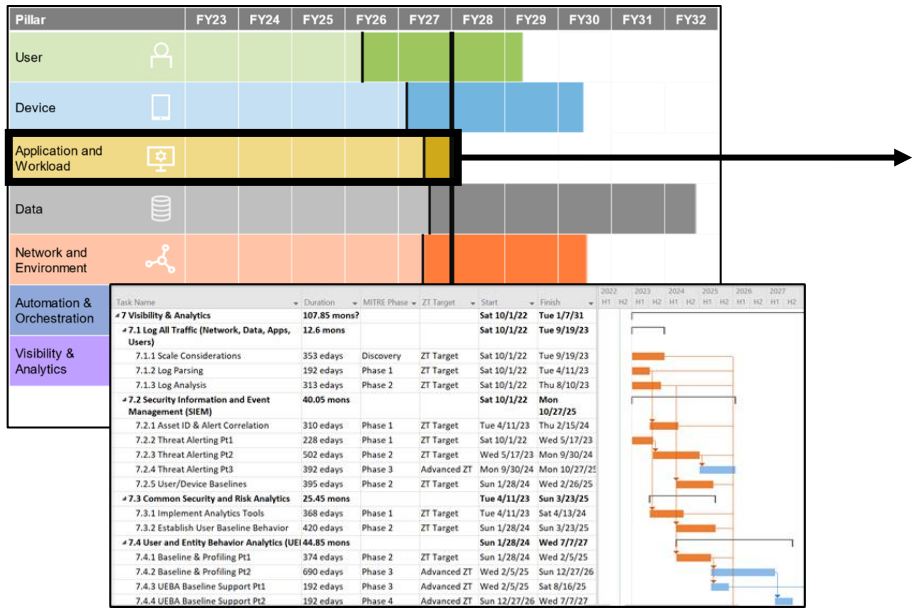
Activity dependencies were re-evaluated, resulting in an updated timeline to achieve ZT Target Levels

3



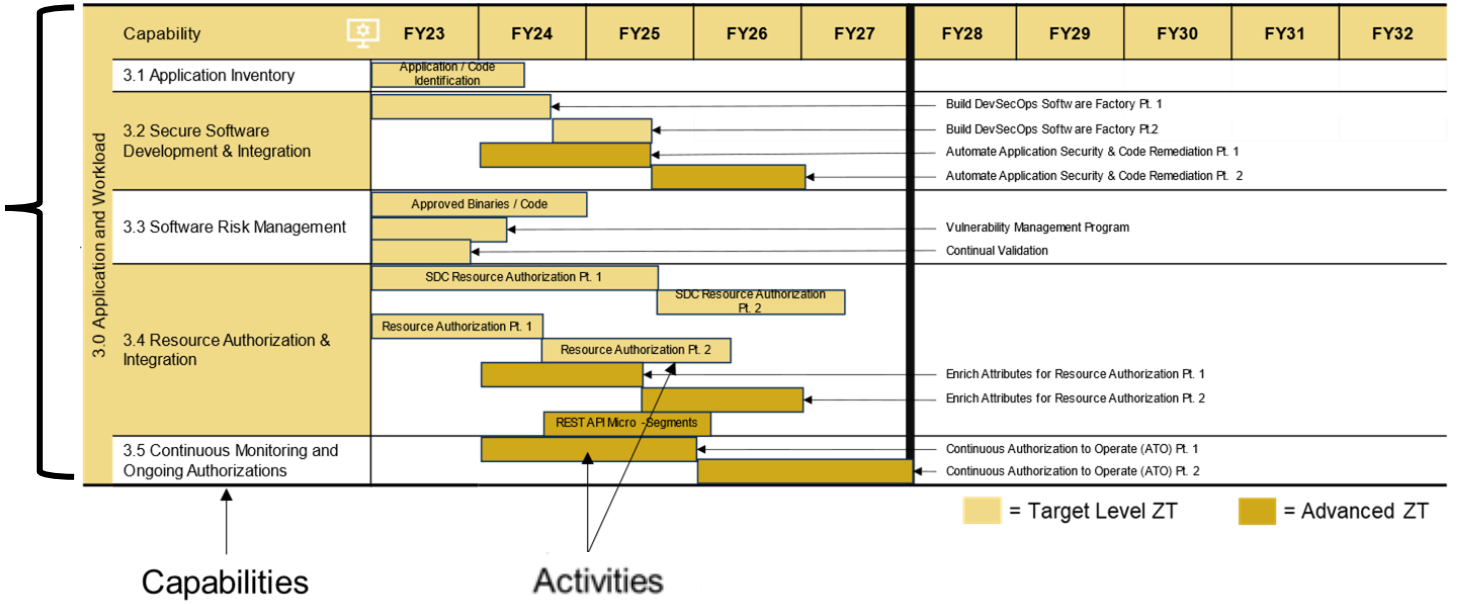
Leveling activity distribution over FYs resulted in COA 1 and supported further acceleration efforts

Each pillar has an associated timeline broken down into activities



MS Project File

Pillar-Capability Timelines



Each Pillar-Capability Timeline is structured based on the dependency relationships (at the activity level) and ZT execution levels as detailed in the attached MS Project document
Activity dates are recommendations and not intended to serve as a formal requirement

Key Communications

Note: Click on each Capability Title for details

DoD Zero Trust Capabilities

User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
1.1 User Inventory	**2.1** Device Inventory	**3.1** Application Inventory	**4.1** Data Catalog Risk Assessment	**5.1** Data Flow Mapping	**6.1** Policy Decision Point (PDP) & Policy Orchestration	**7.1** Log All Traffic (Network, Data, Apps, Users)
1.2 Conditional User Access	**2.2** Device Detection and Compliance	**3.2** Secure Software Development & Integration	**4.2** DoD Enterprise Data Governance	**5.2** Software Defined Networking (SDN)	**6.2** Critical Process Automation	**7.2** Security Information and Event Management (SIEM)
1.3 Multi-Factor Authentication	**2.3** Device Authorization with Real Time Inspection	**3.3** Software Risk Management	**4.3** Data Labeling and Tagging	**5.3** Macro Segmentation	**6.3** Machine Learning	**7.3** Common Security and Risk Analytics
1.4 Privileged Access Management	**2.4** Remote Access	**3.4** Resource Authorization & Integration	**4.4** Data Monitoring and Sensing	**5.4** Micro Segmentation	**6.4** Artificial Intelligence	**7.4** User and Entity Behavior Analytics
1.5 Identity Federation & User Credentialing	**2.5** Partially & Fully Automated Asset, Vulnerability and Patch Management	**3.5** Continuous Monitoring and Ongoing Authorizations	**4.5** Data Encryption & Rights Management		**6.5** Security Orchestration, Automation & Response (SOAR)	**7.5** Threat Intelligence Integration
1.6 Behavioral, Contextual ID, and Biometrics	**2.6** Unified Endpoint Management (UEM) & Mobile Device Management (MDM)		**4.6** Data Loss Prevention (DLP)		**6.6** API Standardization	**7.6** Automated Dynamic Policies
1.7 Least Privileged Access	**2.7** Endpoint & Extended Detection & Response (EDR & XDR)		**4.7** Data Access Control		**6.7** Security Operations Center (SOC) & Incident Response (IR)	
1.8 Continuous Authentication						
1.9 Integrated ICAM Platform						

EXECUTION ENABLERS — Doctrine | Organization | Training | Material | Leadership & Education | Personnel | Facilities | Policy

V1.0 as of 10/04/2022

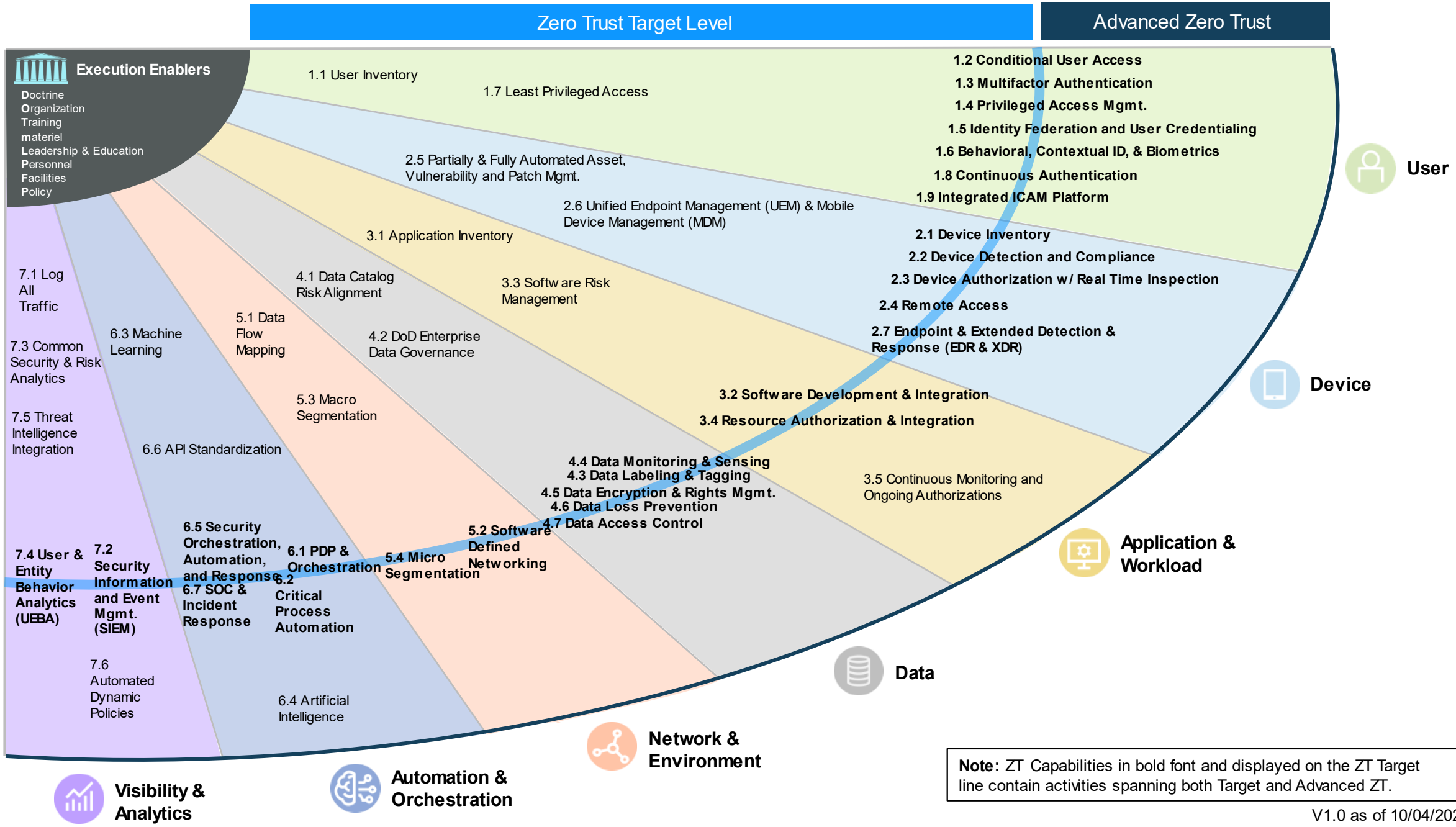
The 45 Capabilities support Target Level and Advanced ZT

	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

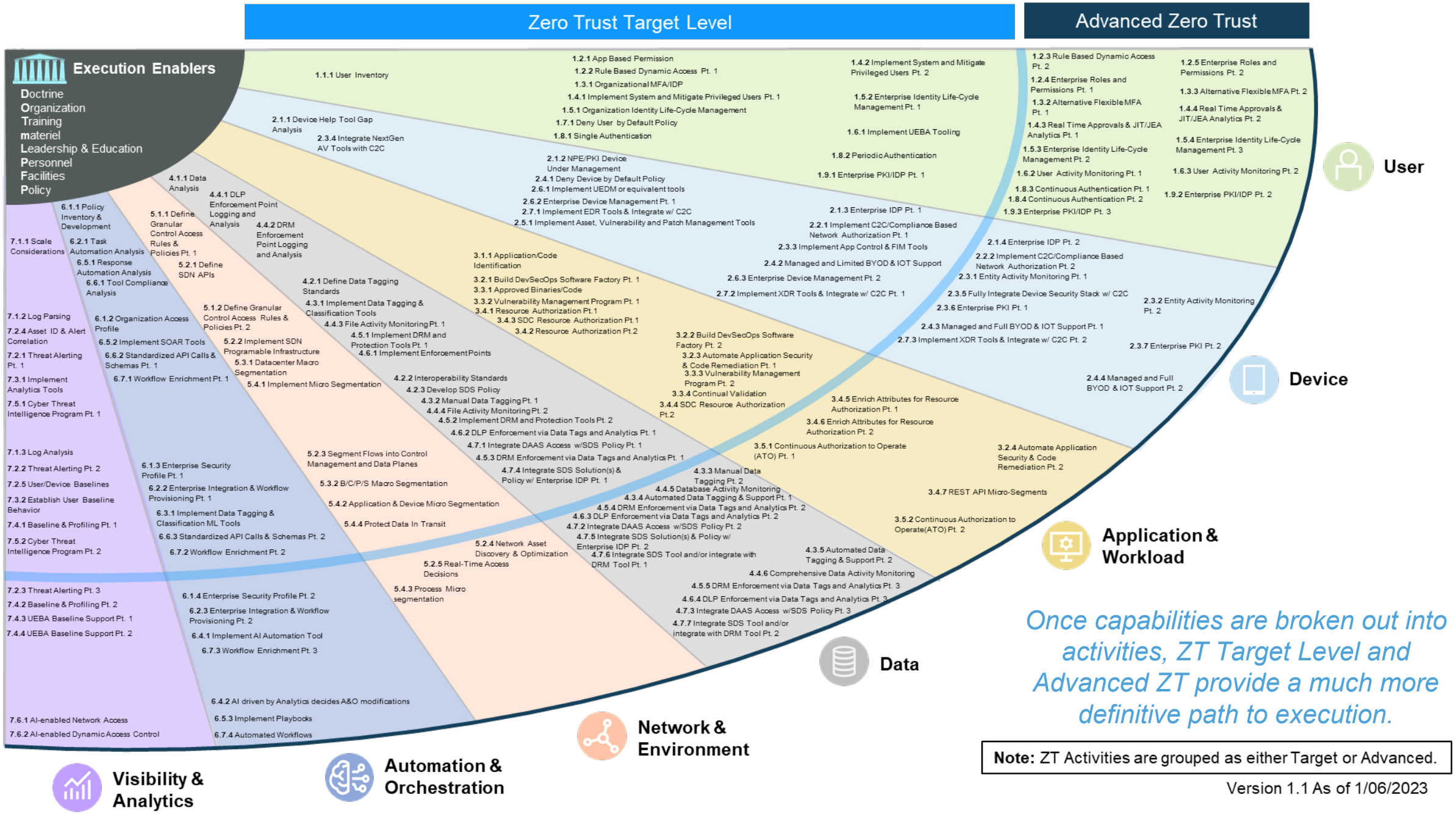
Version 1.0 As of 10/04/2022

Many capabilities have multiple activities that span from target to advanced – Accomplishment of "ZT Target Level" and "Advanced ZT" will be determined at the Activity level



Note: ZT Capabilities in bold font and displayed on the ZT Target line contain activities spanning both Target and Advanced ZT.

V1.0 as of 10/04/2022

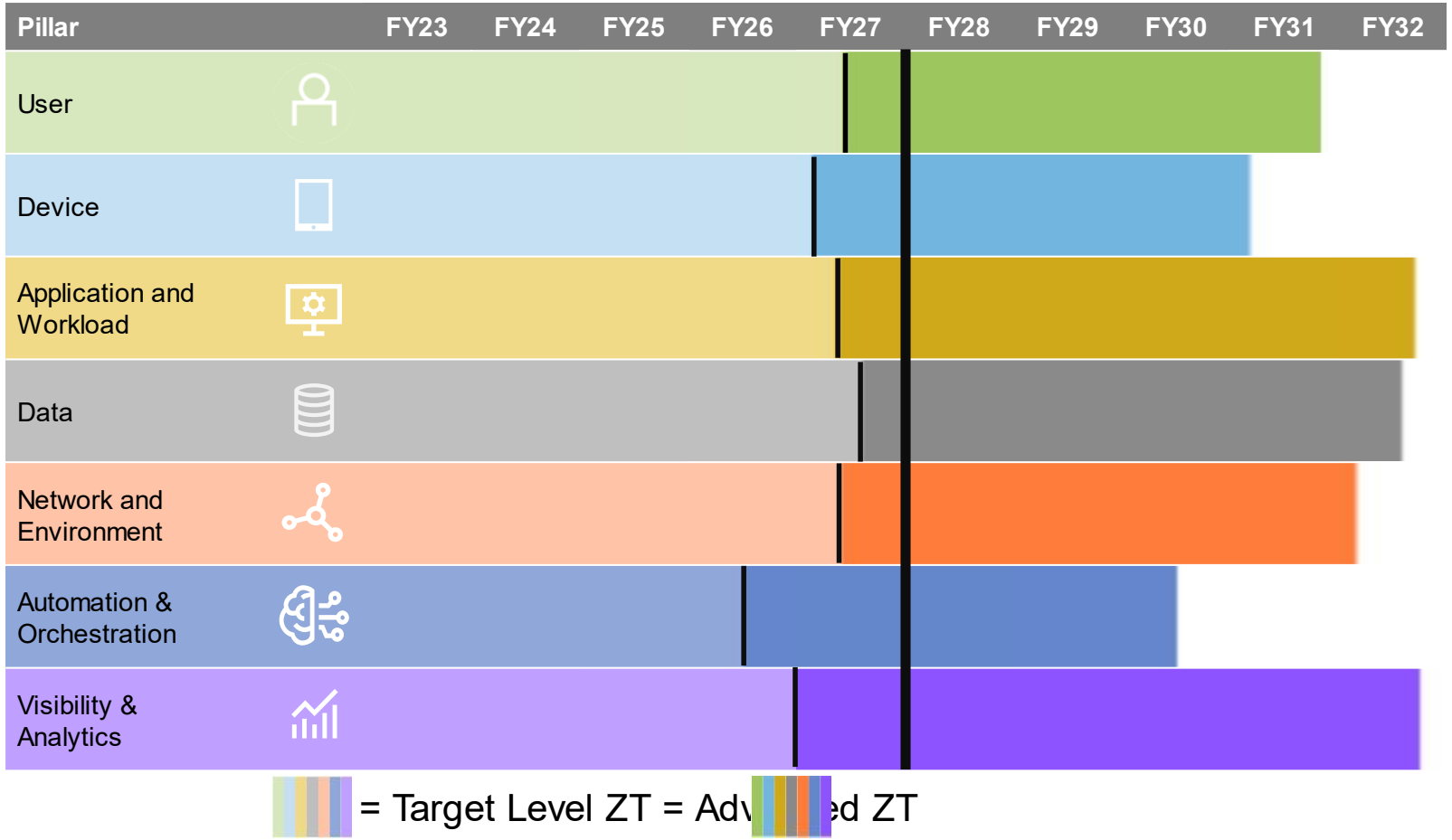


Once capabilities are broken out into activities, ZT Target Level and Advanced ZT provide a much more definitive path to execution.

Note: ZT Activities are grouped as either Target or Advanced.

Version 1.1 As of 1/06/2023

COA 1 (DoD Baseline) achieves Target Level ZT by the end of FY27



- Assumes a start date of FY23;
- It provides a baseline roadmap for a stakeholder who has not yet commenced efforts in developing ZT;
- Stakeholders who have achieved activities on the roadmap can “move ahead”;
- **Does not** proscribe specific solutions to achieving the activities required;
- It allows for some buffer in Target ZT achievement date to the stated goal (end of FY27) if delays occur.

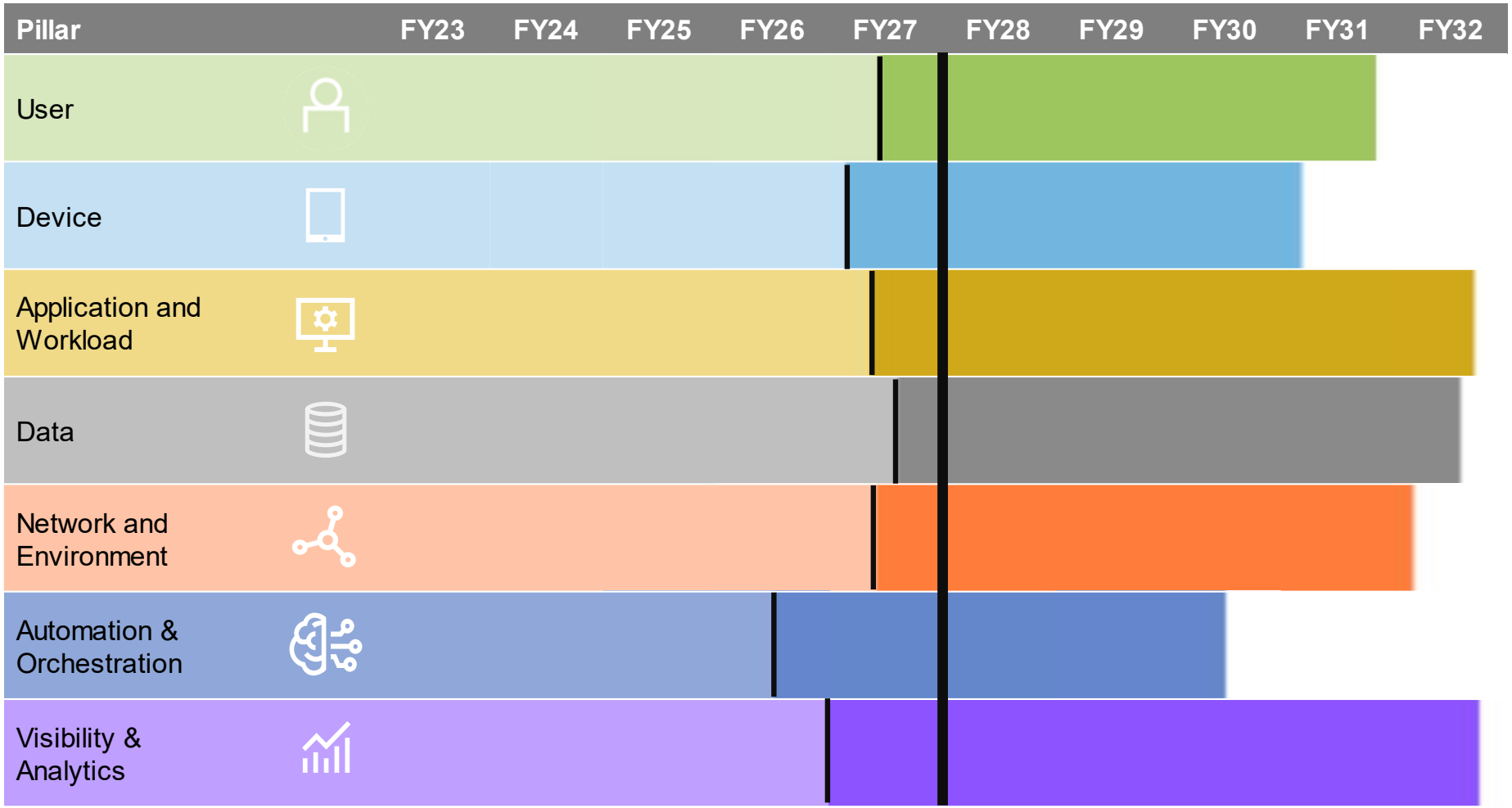
Appendix A: COA 1 Timeline Details (DoD Baseline)

Note 1: The timeline depicted is meant to show *how* activities may be sequenced to achieve Target Level ZT by the end of FY27 as proscribed in the DoD Zero Trust Strategy; these activity durations are meant to serve as estimates for planning purposes only

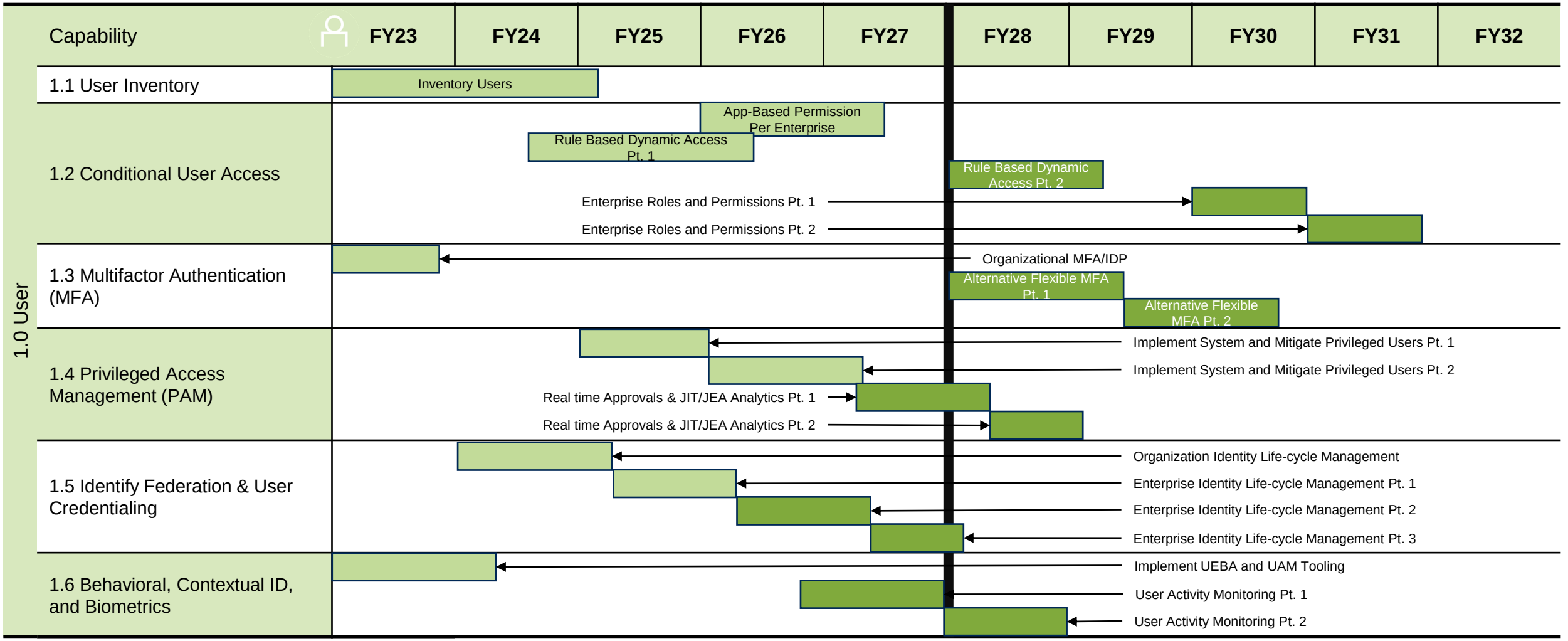
Note 2: The DoD Zero Trust Capability Roadmap described in the High-Level Capability Roadmap section below provides a guide to follow for the DoD baseline course of action (COA). Additionally, to accelerate Zero Trust adoption, the Department is considering several additional complementary COAs including commercial and Government-owned cloud-based enterprise services

Back to Table of Contents

COA 1 (DoD Baseline) Timeline Estimates



User (1 of 2) – COA 1



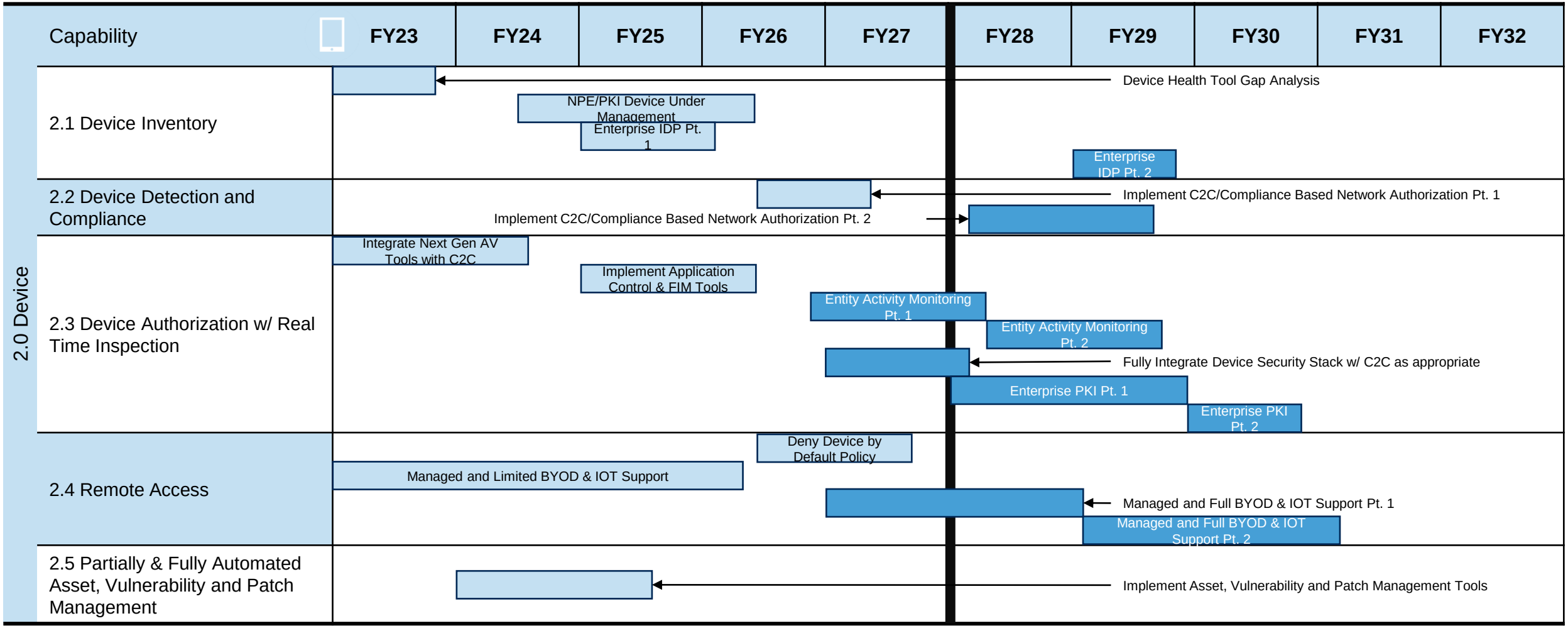
= Target Level ZT = Advanced ZT

User (2 of 2) – COA 1

	Capability	FY23	FY24	FY25	FY26	FY27	FY28	FY29	FY30	FY31	FY32
1.0 User	1.7 Least Privileged Access	Deny User by Default Policy									
	1.8 Continuous Authentication	Single Authentication		Periodic Authentication			Continuous Authentication Pt. 1	Continuous Authentication Pt. 2			
	1.9 Integrated ICAM Platform			Enterprise PKI/IDP Pt. 1	Enterprise PKI/IDP Pt. 2		Enterprise PKI/IDP Pt. 3				

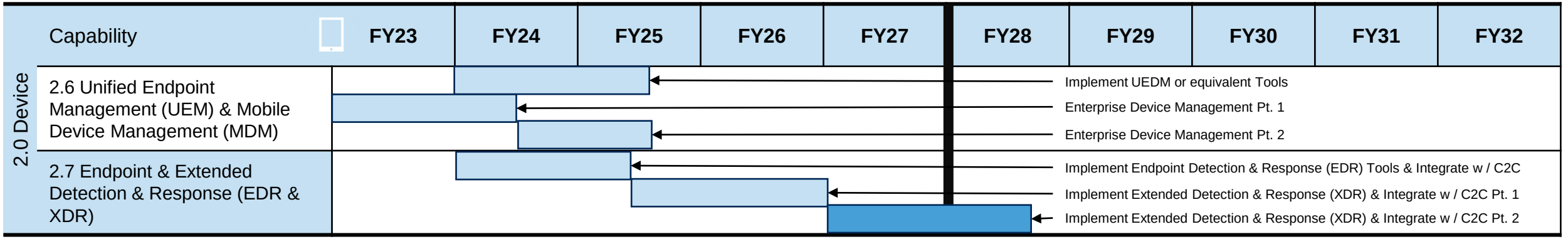
= Target Level ZT = Advanced ZT

Device (1 of 2) – COA 1



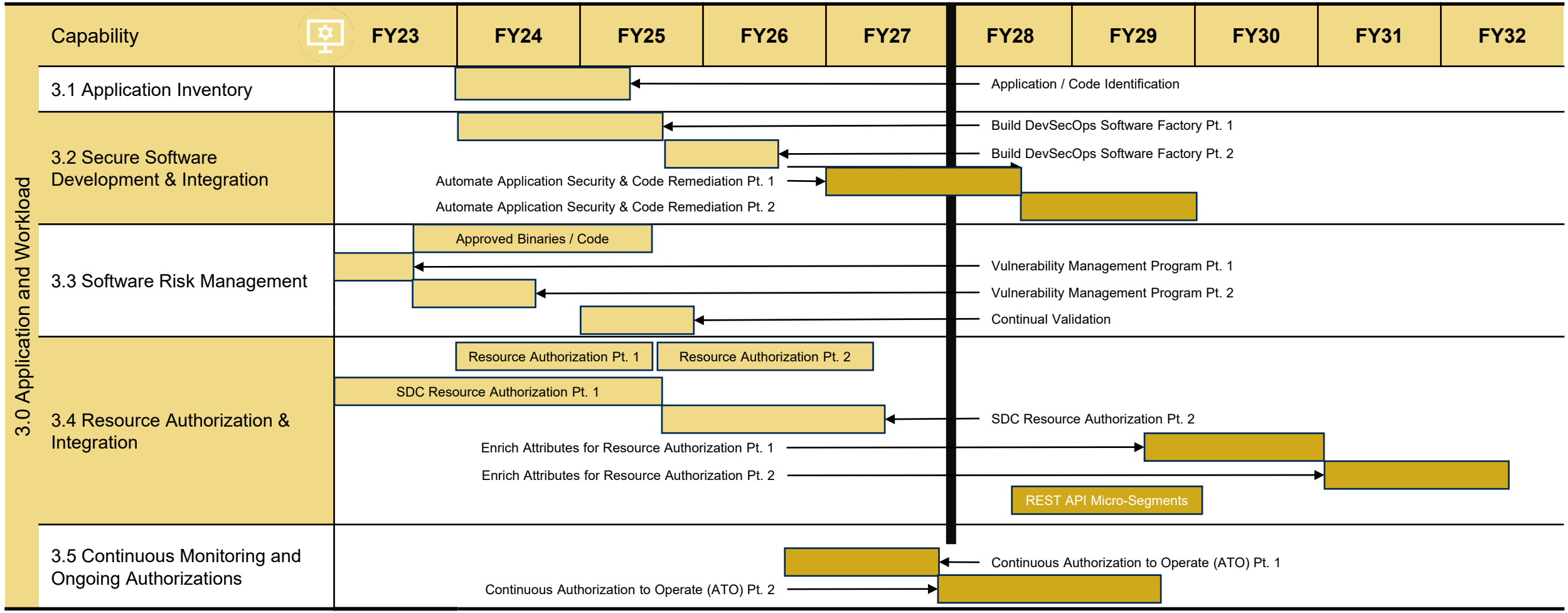
= Target Level ZT = Advanced ZT

Device (2 of 2) – COA 1



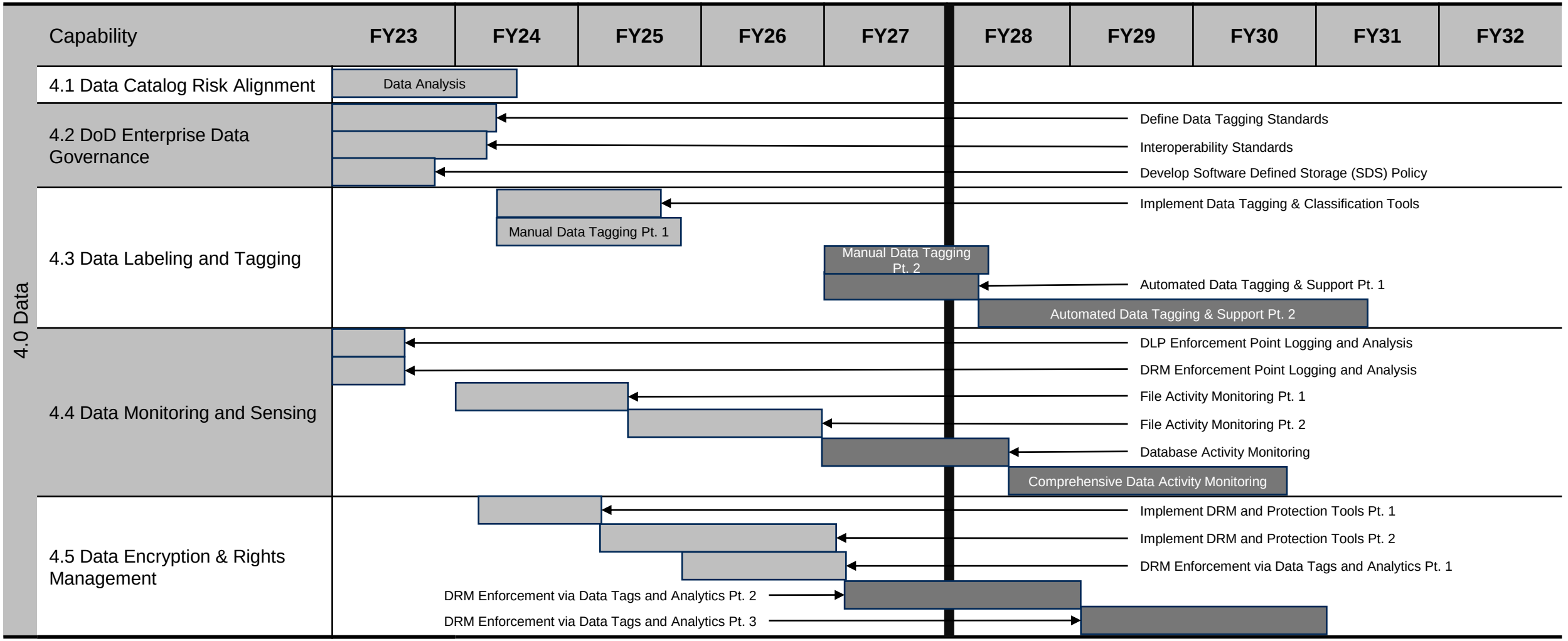
= Target Level ZT = Advanced ZT

Application and Workload – COA 1



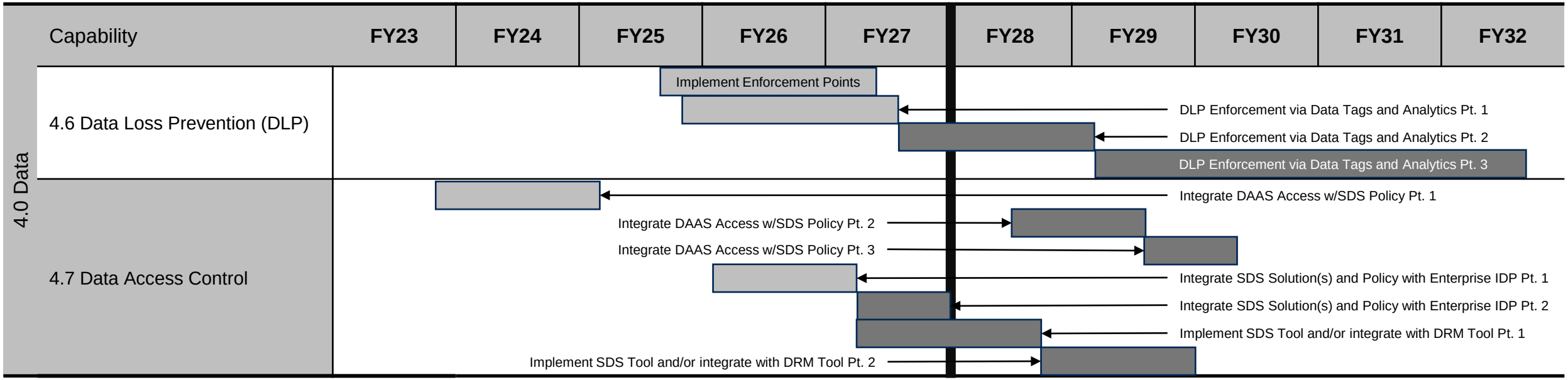
= Target Level ZT = Advanced ZT

Data (1 of 2) – COA 1



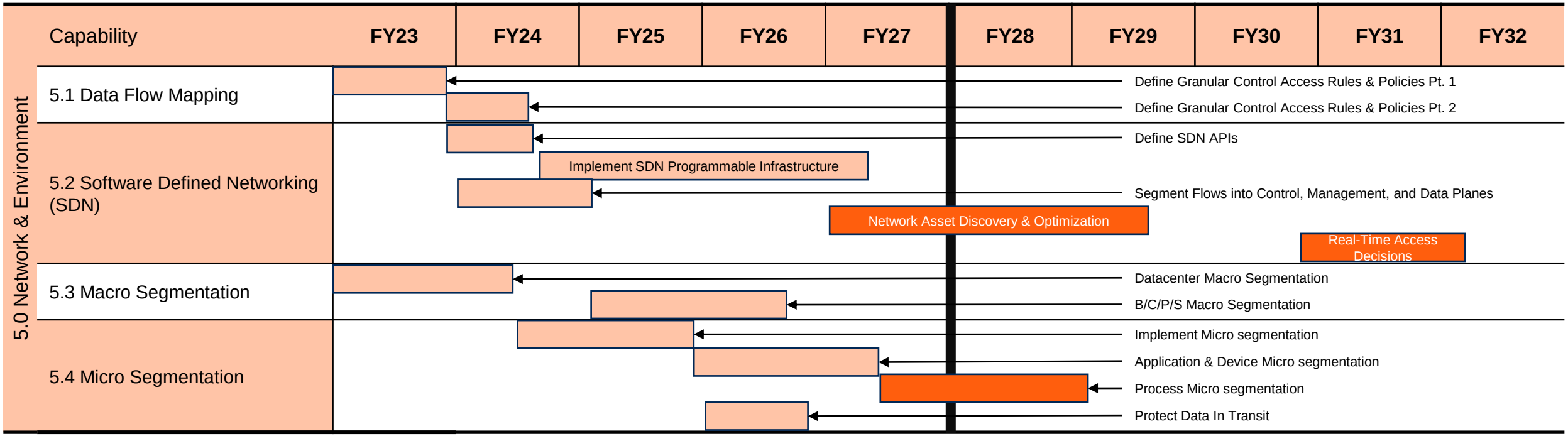
= Target Level ZT = Advanced ZT

Data (2 of 2) – COA 1



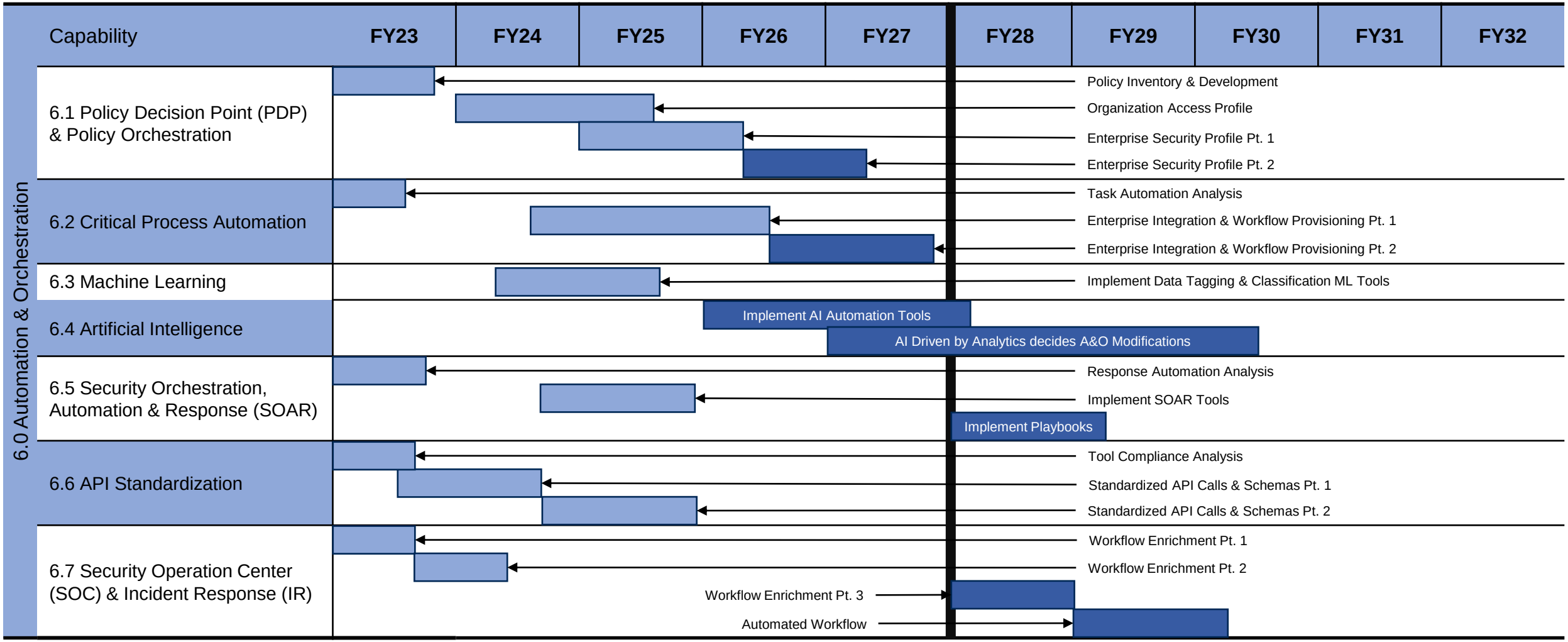
= Target Level ZT = Advanced ZT

Network and Environment – COA 1



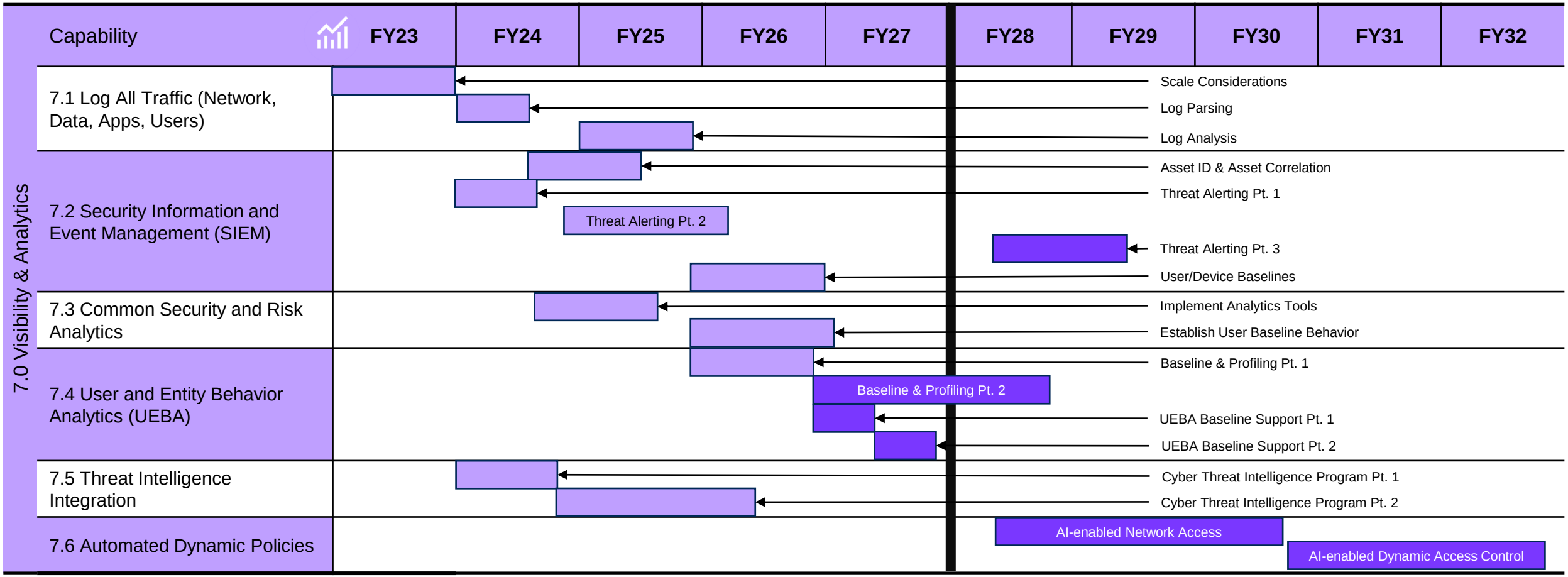
= Target Level ZT = Advanced ZT

Automation & Orchestration – COA 1



= Target Level ZT = Advanced ZT

Visibility & Analytics – COA 1

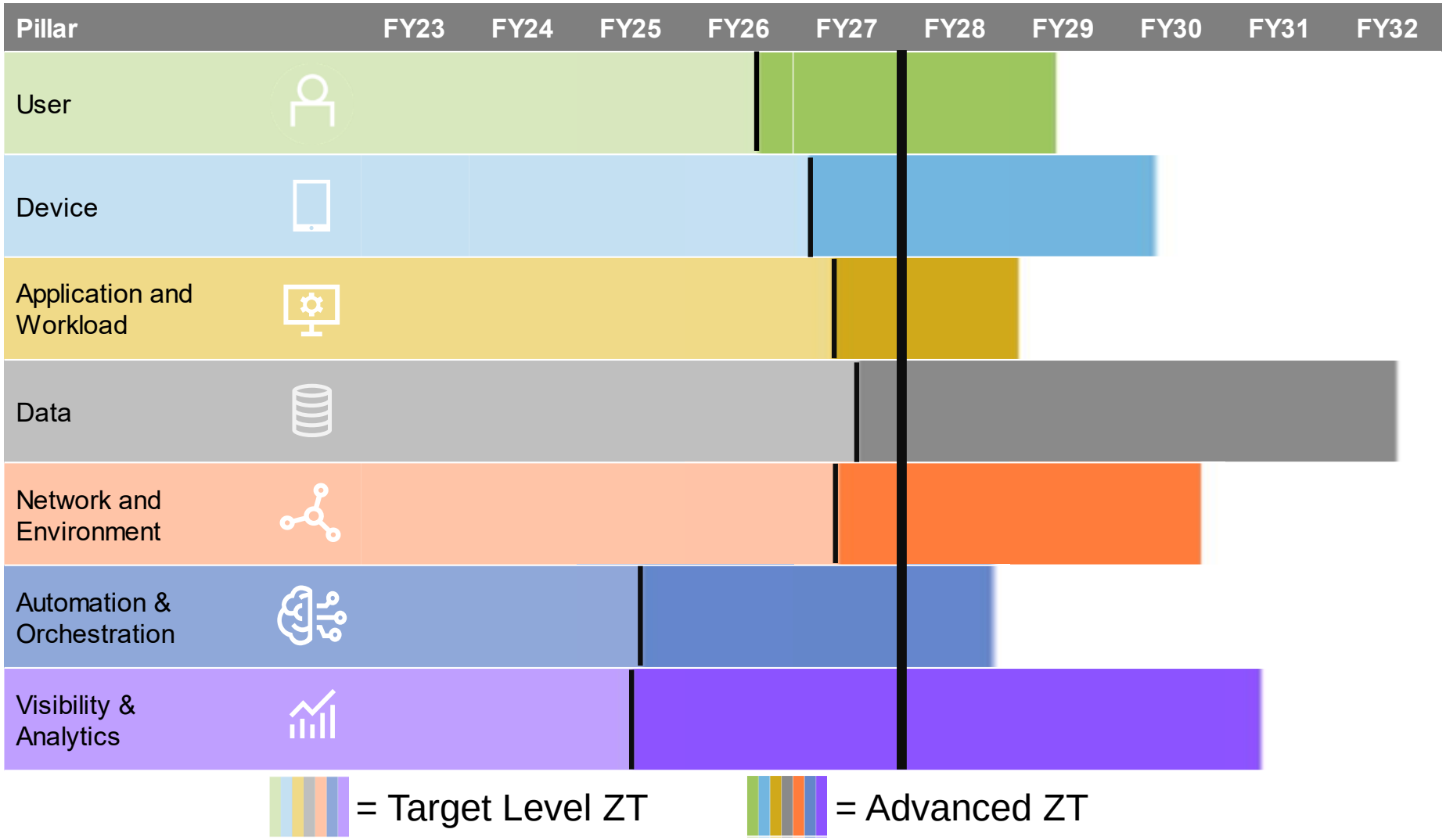


= Target Level ZT = Advanced ZT

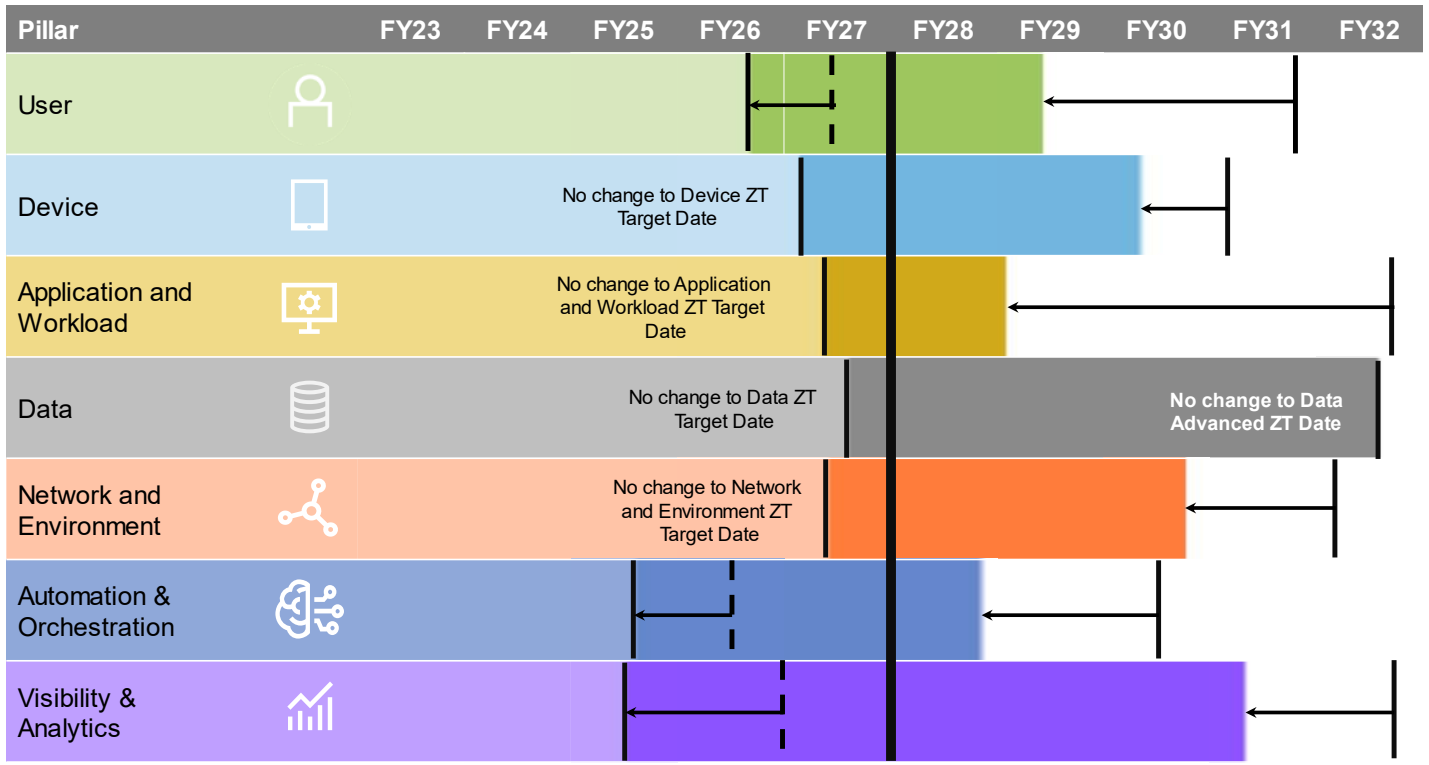
Appendix B: Accelerated DoD Baseline Timeline Details

Back to Table of Contents

Accelerated COA 1 Timeline Estimates



Aggressively shifting activity start dates to FY23 accelerates ZT achievement dates



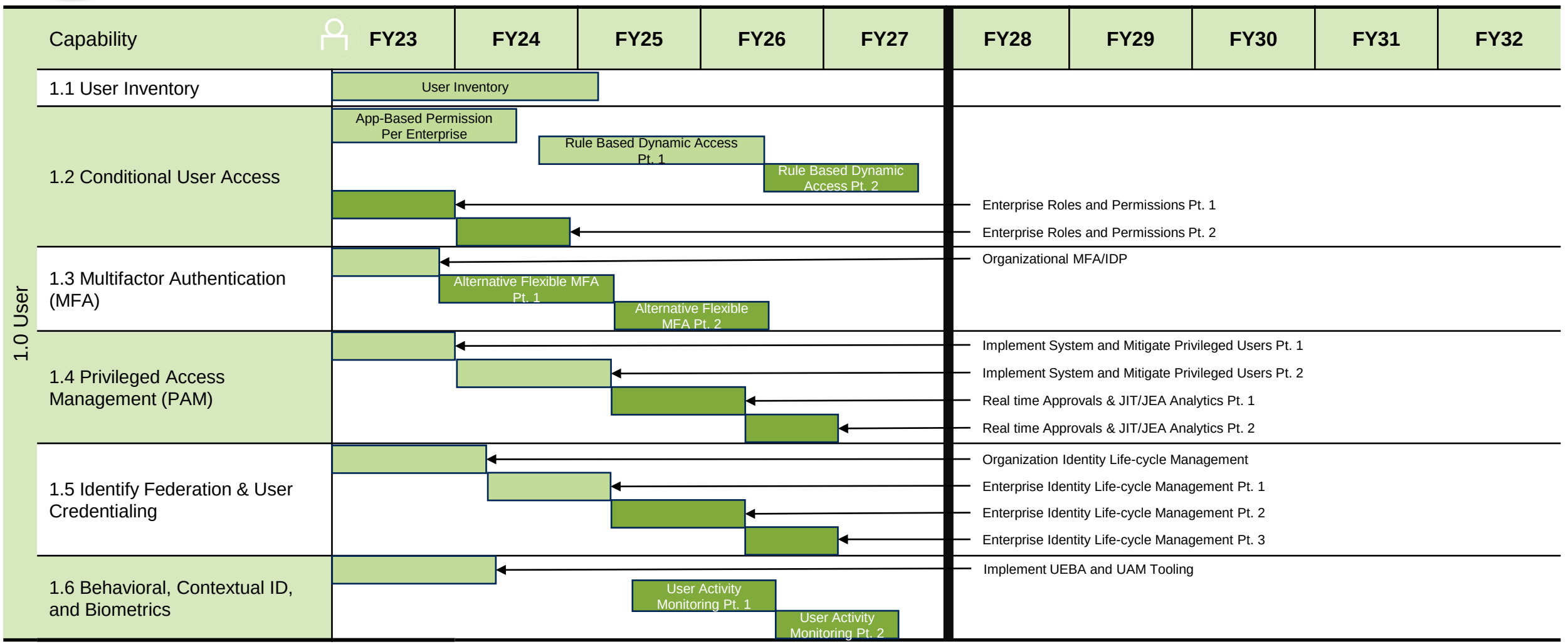
Shifting Target **and** Advanced ZT dates left as much as possible (e.g., when not limited by predecessor activities) significantly reduces the overall timeline to ZT accomplishment

This timeline serves as a model for those stakeholders who have the desire (and capacity) to achieve Advanced ZT more quickly than the recommended baseline COA 1

Left-shifting Activities:

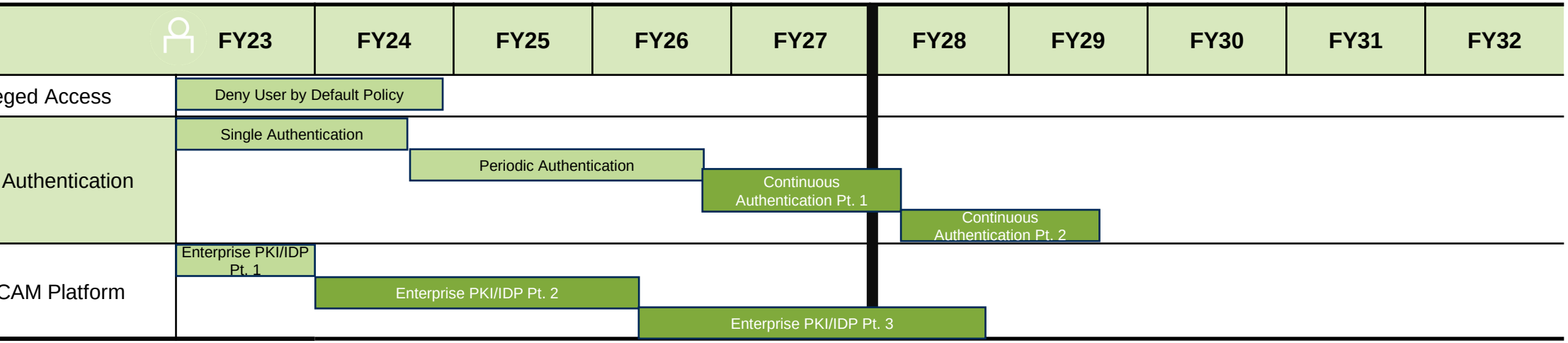
- ✔ Reduces the time to achieving Target Level ZT
- ✔ May result in increased financial and personnel resourcing in the near term due to increased requirements
- ✔ Due to shifting priorities to the left, reduces the risk that other priorities supersede Zero Trust in future years
- X Stakeholders may view this timeline as unrealistic
- X May result in misprioritization of activity accomplishment (e.g., by focusing on advanced activities too soon)

User (1 of 2) - Accelerated



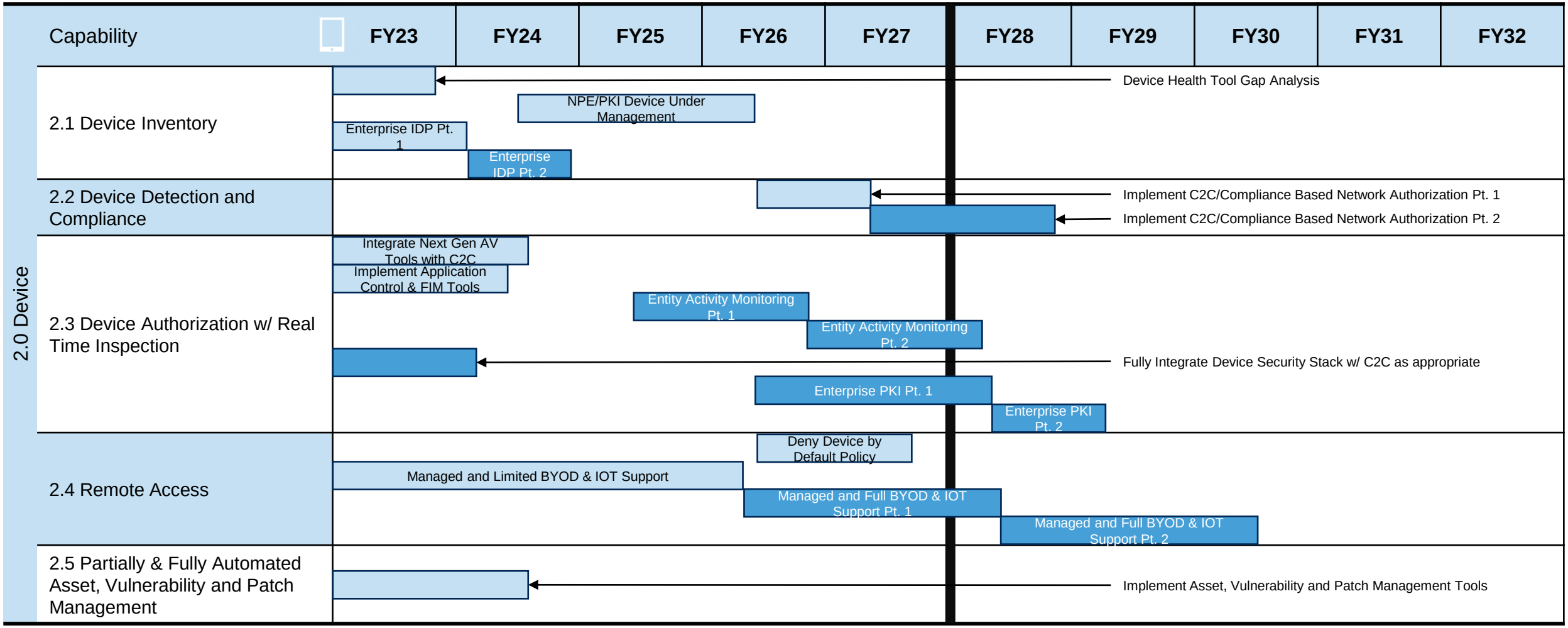
= Target Level ZT = Advanced ZT

User (2 of 2) - Accelerated



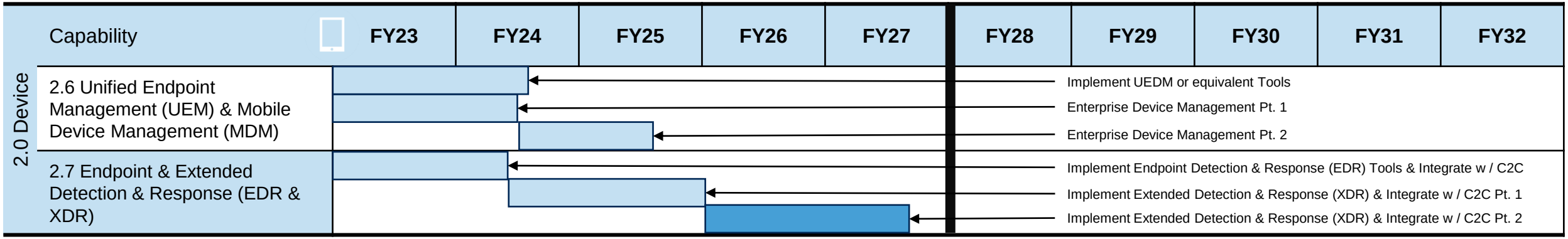
= Target Level ZT = Advanced ZT

Device (1 of 2) - Accelerated



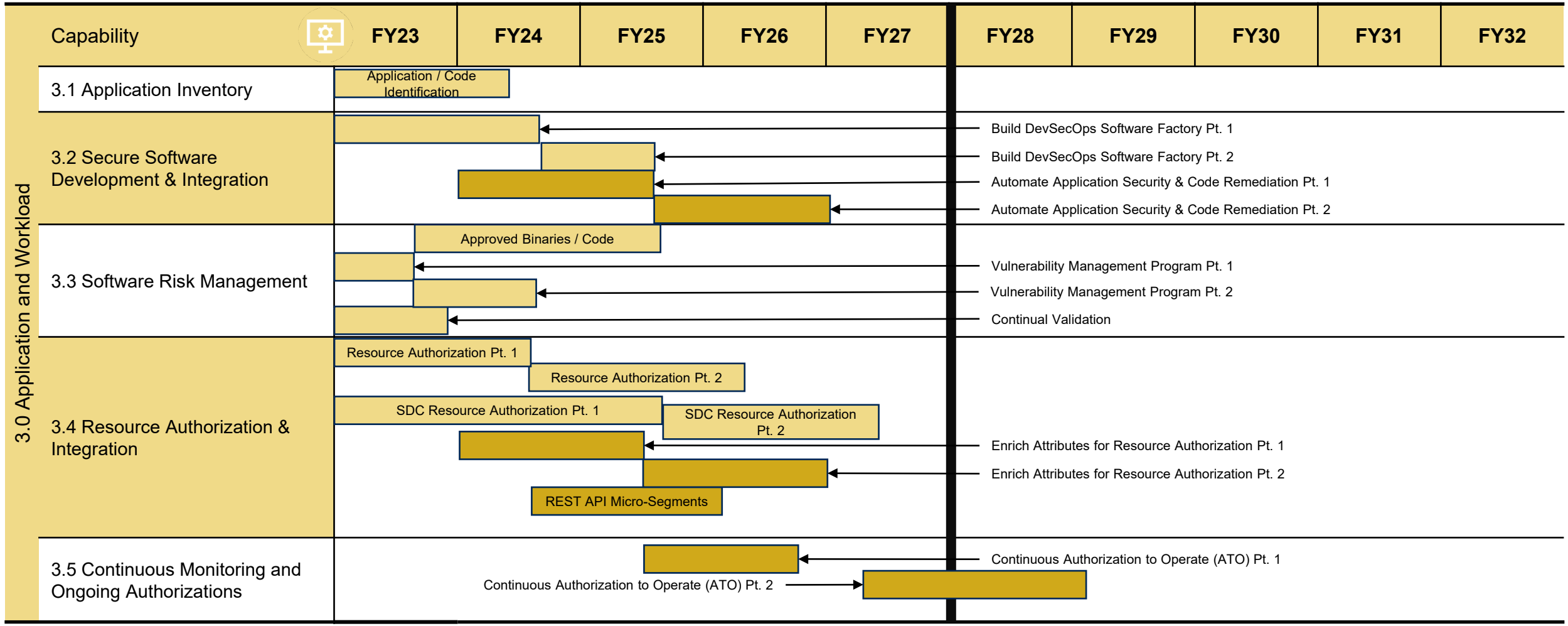
= Target Level ZT = Advanced ZT

Device (2 of 2) - Accelerated



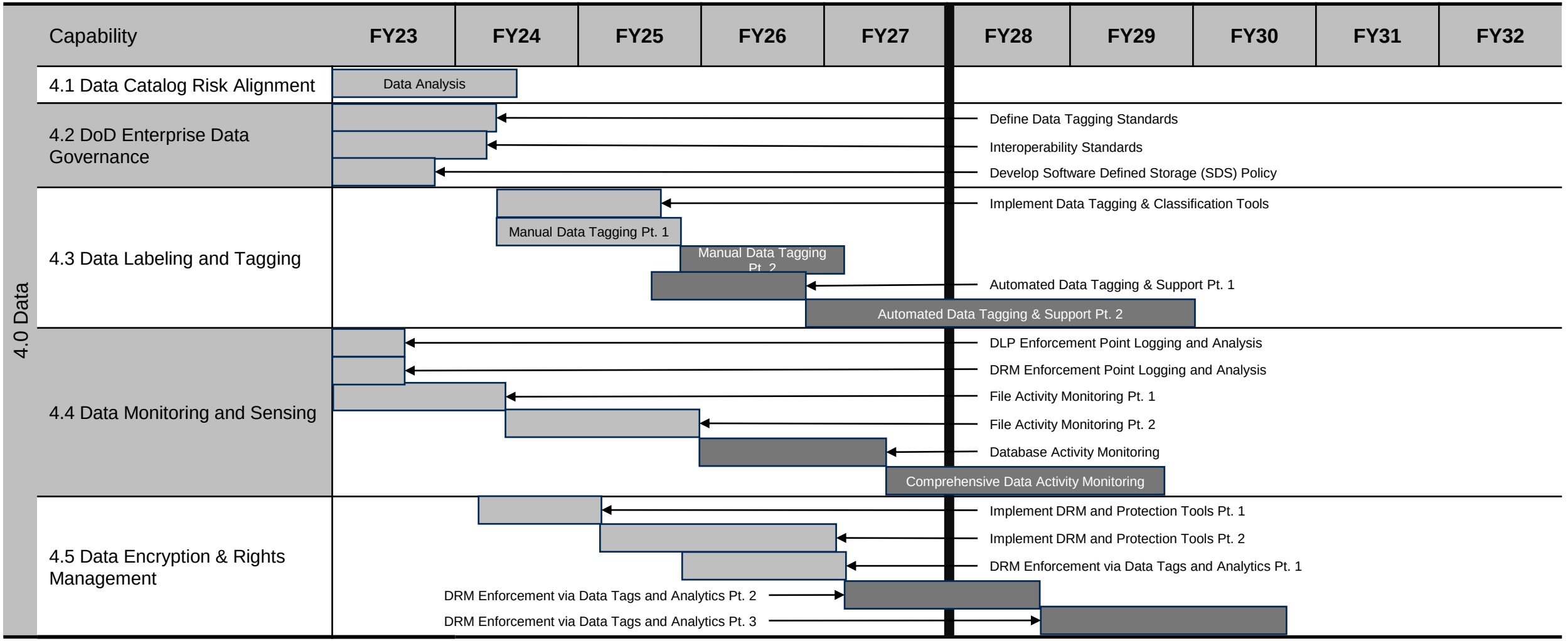
= Target Level ZT = Advanced ZT

Application and Workload - Accelerated



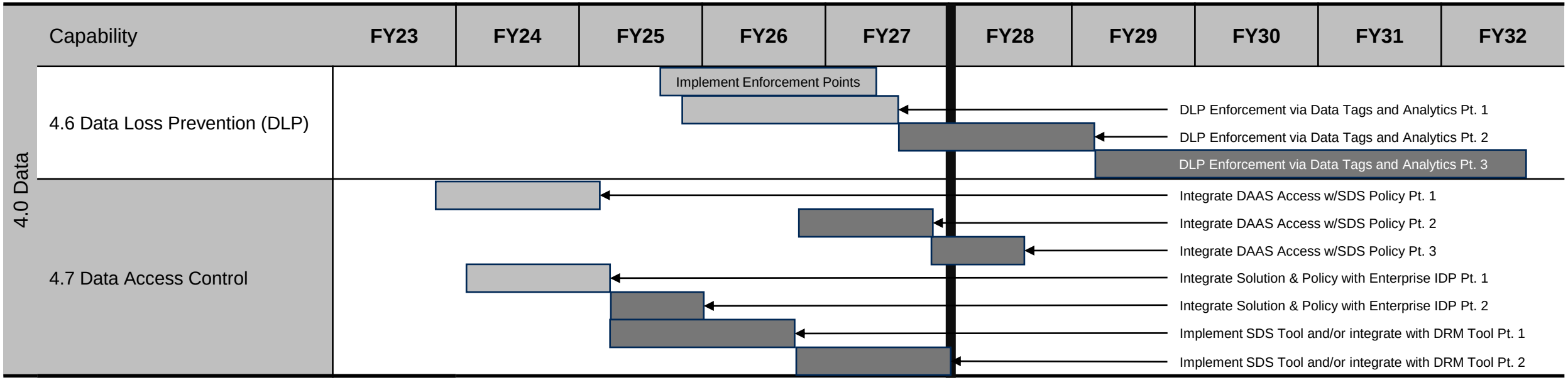
= Target Level ZT = Advanced ZT

Data (1 of 2) - Accelerated



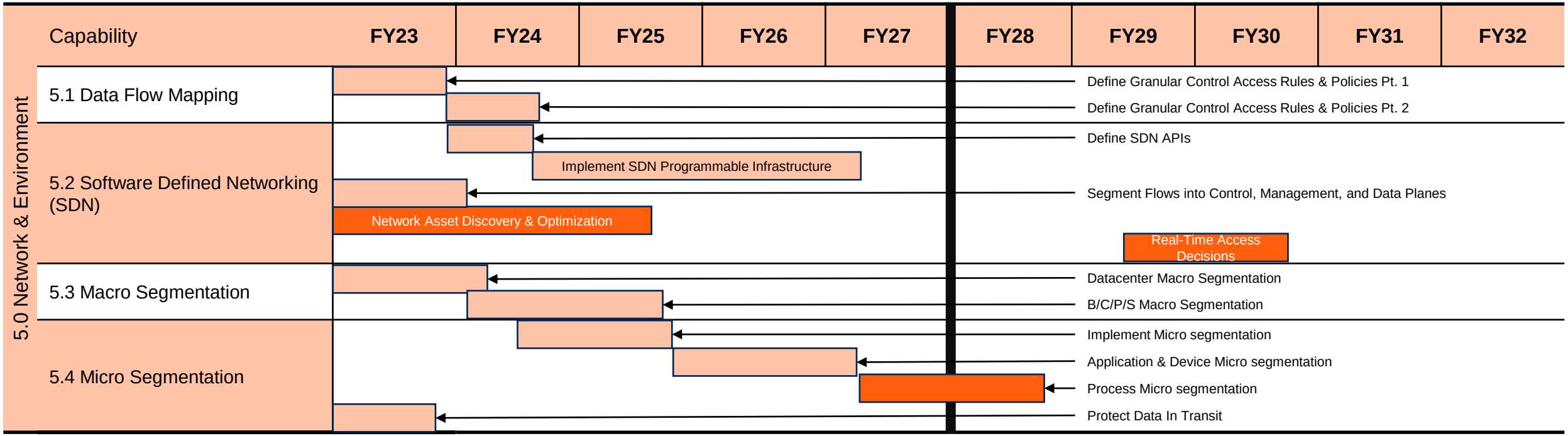
= Target Level ZT = Advanced ZT

Data (2 of 2) - Accelerated



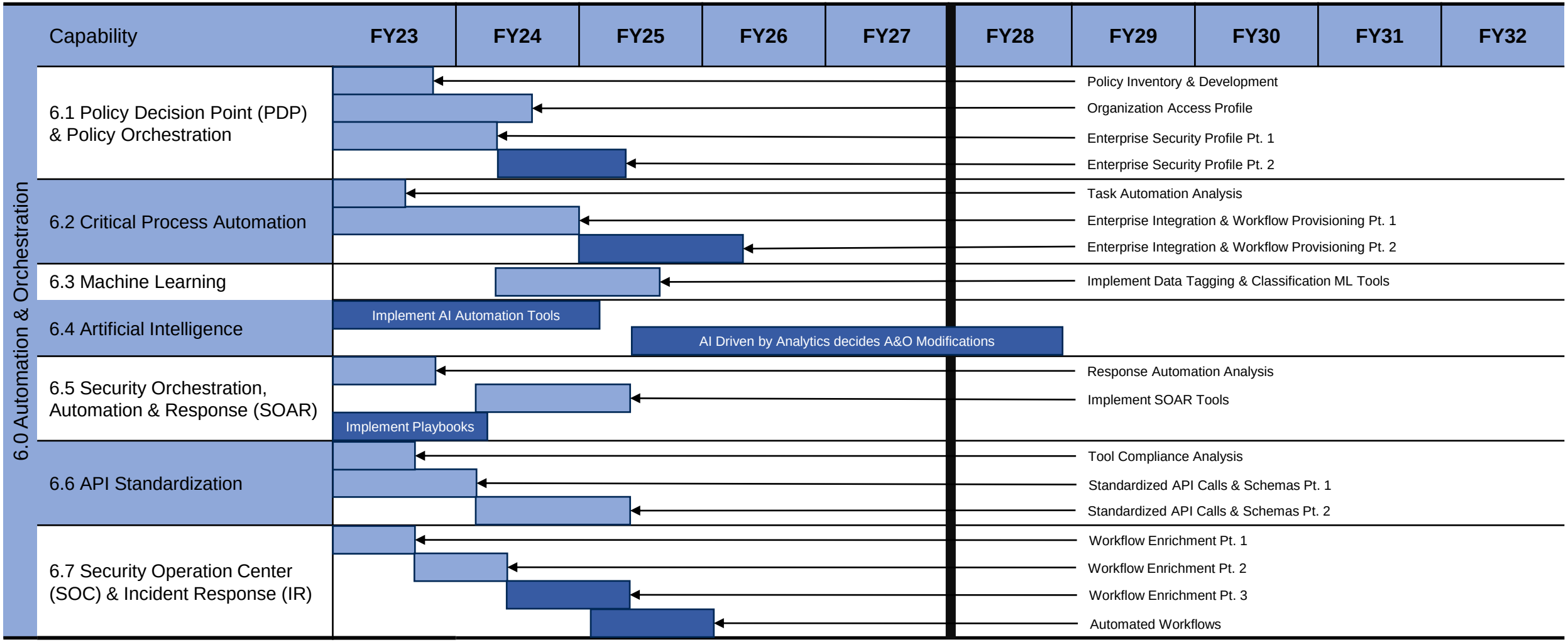
= Target Level ZT = Advanced ZT

Network and Environment - Accelerated



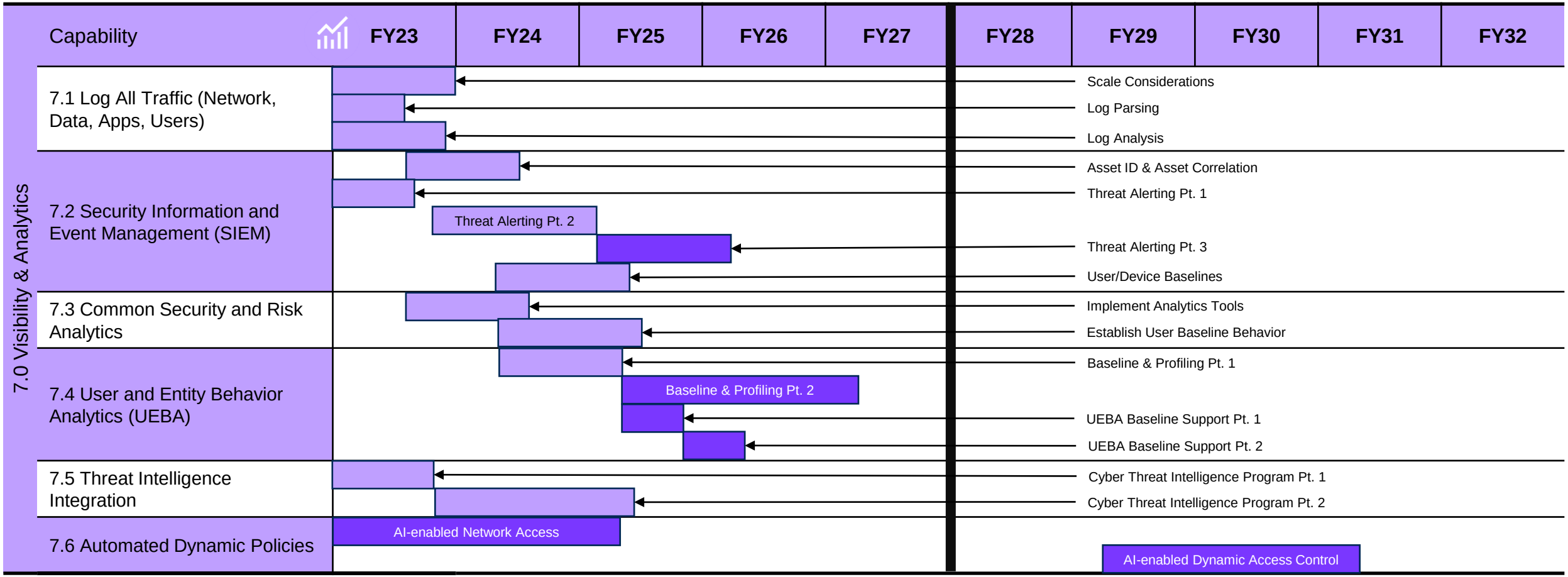
= Target Level ZT = Advanced ZT

Automation & Orchestration - Accelerated



= Target Level ZT = Advanced ZT

Visibility & Analytics - Accelerated



= Target Level ZT = Advanced ZT

Appendix C: Capability Definitions

Note: There are 45 capabilities and 152 activities. Each capability is defined in the subsequent slides and aligned with activities. Activity Outcome descriptions are provided in the excel spreadsheet titled “() DoD ZT Capabilities and Activities”

Back to Table of Contents

Capability Definitions

ID #	Capability	Pillar	Capability Description	Capability Outcome	Impact to ZT	Activities
1.1	User Inventory	1 - User	Regular and Privileged users are identified and integrated into an inventory supporting regular modifications. Applications, software and services that have local users are all part of the inventory and highlighted.	System owners have control (visibility and administrative rights) of all authorized and authenticated users on the network	Users not on the authorized user list will be denied access by policy	* Inventory User
1.2	Conditional User Access	1 - User	Through maturity levels Conditional Access works to create a dynamic level of access for users in the environment. This starts with traditional role-based access controls across a federate ICAM, expands to be application focused roles and ultimately utilizes enterprise attributes to provide dynamic access rules.	Eventually, organizations control user, device, and non-user entity DAAS access through dynamically changing user risk profiles and fine-grained access control to include the use of user risk assessments	Users not known to the system and users who present an unacceptable degree of risk will be denied access with greater accuracy	* Implement App Based Permissions per Enterprise * Rule Based Dynamic Access Pt1 * Rule Based Dynamic Access Pt2 * Enterprise Gov't roles and Permissions Pt1 * Enterprise Gov't roles and Permissions Pt2
1.3	Multi-Factor Authentication (MFA)	1 - User	This capability initially focuses on developing an organization focused MFA provider and Identity Provider to enable the centralization of users. Retirement of local and/or built-in accounts and groups is a critical piece to this capability. At the later maturity levels alternative and flexible MFA tokens can be used to provide access for standard and external users.	DoD organizations require users and non-user entities to authenticate using at least two of the following three attributes: knowledge (user ID/password), possession (CAC/token), or something you are (inherence, e.g., iris/fingerprints), in order to access DAAS	Users not presenting multiple forms of authentication will be denied access to DAAS system and resources	* Organizational MFA/IDP * Alternative Flexible MFA Pt1 * Alternative Flexible MFA Pt2
1.4	Privileged Access Management (PAM)	1 - User	The capability focuses on removal of permanent administrator/elevated privileges by first creating a Privileged Account Management (PAM) system and migrating privileged users to it. The capability is then expanded upon by using automation with privilege escalation approvals and feeding analytics into the system for anomaly detection.	DoD organizations control, monitor, secure, and audit privileged identities (e.g., through password vaulting, JIT/JEA with PAWS) across their IT environments	Critical assets and applications secured, controlled, monitored and managed through limits on admin access	* Implement System and Migrate Privileged Users Pt1 * Implement System and Migrate Privileged Users Pt2 * Real time Approvals & JIT/JEA Analytics Pt1 * Real time Approvals & JIT/JEA Analytics Pt2

Return to Capability Overview

Capability Definitions

ID #	Capability	Pillar	Capability Description	Capability Outcome	Impact to ZT	Activities
1.5	Identity Federation & User Credentialing	1 - User	The initial scope of this capability focuses on standardizing the Identity Lifecycle Management (ILM) processes and integrating with the standard organizational IDP/IDM solution. Once completed the capability shifts to establishing an Enterprise ILM process/solution either through a single solution or identity federation.	DoD organizations manually issue, manage, and revoke credentials bound to DoD person, device, and NPE identities. Identity information is developed and shared across entitles and trust domains providing "single sign-on" convenience and efficiencies to identified (authenticated and authorized) users and devices.	Visibility and accuracy of user authentication information is increased, to include DoD users and users managed by other agencies. Users lacking sufficient credentials are denied access according to established policies.	* Organizational Identity Life-Cycle Management * Enterprise Identity Life-Cycle Management Pt1 * Enterprise Identity Life-Cycle Management Pt2 * Enterprise Identity Life-Cycle Management Pt3
1.6	Behavioral, Contextual ID, and Biometrics	1 - User	Utilizing the Enterprise IDP, user and entity behavioral analytics (UEBA) are enabled with basic user attributes. Once completed this is expanded into Organizational specific attributes using Organizational IDPs as available. Finally UEBA are integrated with the PAM and JIT/JEA systems to better detect anomalous and malicious activities.	DoD organizations utilize behavioral, contextual, and biometric telemetry to enhance risk-based authentication and access controls	Behavioral, contextual, and biometric telemetry enhances MFA with	* Implement User & Entity Behavior Activity (UEBA) and User Activity Monitoring (UAM) Tooling * User Activity Monitoring Pt1 * User Activity Monitoring Pt2
1.7	Least Privileged Access	1 - User	DoD organizations govern access to DAAS using the absolute minimum access required to perform routine, legitimate tasks or activities. DoD Application Owners identify the necessary roles and attributes for standard and privileged user access. Privileged access for all DoD organization DAAS is audited and removed when unneeded.	DoD organizations govern access to DAAS using the absolute minimum access required to perform routine, legitimate tasks or activities	Users on the network only have access to the DAAS for which they are authorized and authenticated over a specific timeframe	* Deny User by Default Policy
1.8	Continuous Authentication	1 - User	The DoD organizations and overall enterprise will methodically move towards continuous attribute based authentication. Initially the capability focuses on standardizing legacy single authentication to a organizationally approved IDP with users and groups. The second stages adds in based rule based (time) authentication and ultimately matures to Continuous Authentication based on the application/software activities and privileges requested.	DoD organizations continuously authenticate and authorize users' access to DAAS within and across sessions using MFA	Users not continuously presenting multiple forms of authentication will be denied access to DAAS system and resources	* Single Authentication * Periodic Authentication * Continuous Authentication Pt1 * Continuous Authentication Pt2

Return to Capability Overview

Capability Definitions

ID #	Capability	Pillar	Capability Description	Capability Outcome	Impact to ZT	Activities
1.9	Integrated ICAM Platform	1 - User	DoD organizations and overall enterprise employ enterprise-level identity management and public key infrastructure (PKI) systems to track user, administrator and NPE identities across the network and ensure access is limited to only those who have the need and the right to know. Organizations can verify they need and have the right to access via credential management systems, identity governance and administration tools, and an access management tool. PKI systems can be federated but must either trust a central root certificate authority (CA) and/or cross-sign standardized organizational CA's.	DoD organizations employ enterprise-level identity management systems to track user and NPE identities across the network and ensure access is limited to only those who have the need and the right to know; organizations can verify they need and have the right to access via credential management systems, identity governance and administration tools, and an access management tool	Identities of users and NPE are centrally managed to ensure authorized and authenticated access to DAAS resources across platforms	* Enterprise PKI/IDP Pt1 * Enterprise PKI/IDP Pt2 * Enterprise PKI/IDP Pt3
2.1	Device Inventory	2 - Device	DoD organizations establish and maintain an approved inventory list of all devices authorized to access the network and enroll all devices on the network prior to network connection. Device attributes will include technical details such as the PKI (802.1x) machine certificate, device object, patch/vulnerability status and others to enable successor activities.	DoD organizations establish and maintain a trusted inventory list of all devices authorized to access the network and enroll all devices on the network prior to network connection	By default policy, devices will be denied network access; the only devices permitted access to the network shall be known, authorized, and listed in the device inventory	* Device Health Tool Gap Analysis * NPE/PKI, Device under Management * Enterprise IDP Pt1 * Enterprise IDP Pt2
2.2	Device Detection and Compliance	2 - Device	DoD organizations employ asset management systems for user devices to maintain and report on IT and Cybersecurity compliance. Managed devices (enterprise and mobile) attempting to connect to a DoD network or access a DAAS resource is detected and has its compliance status confirmed (via C2C)	DoD organizations employ asset management systems for user devices to maintain and report on IT compliance. Any device (including mobile, IOT, managed, and unmanaged) attempting to connect to a DoD network or access a DAAS resource is detected and has its compliance status confirmed (via C2C)	Any device attempting to connect to the network will be detected; only those devices that are compliant (e.g., anti-virus is up to date, approved configuration) will receive access to requested DAAS	* Implement C2C/Compliance Based Network Authorization Pt1 * Implement C2C/Compliance Based Network Authorization Pt2

Return to Capability Overview

Capability Definitions

ID #	Capability	Pillar	Capability Description	Capability Outcome	Impact to ZT	Activities
2.3	Device Authorization w/ Real Time Inspection	2 - Device	DoD Organizations conduct foundational and extended device tooling (NextGen AV, AppControl, File Integrity Monitoring (FIM), etc.) integration to better understand the risk posture. Organizational PKI systems are integrated to expand the existing Enterprise PKI to devices as well. Lastly Entity Activity Monitoring is also integrated to identify anomalous activities.	DoD organizations establish processes (e.g., Enterprise PKI) and utilize tools to identify any device (including unmanaged devices, infrastructure devices, and endpoint devices) attempting to access the network, and make a determination if the device should be authorized to access the network. Maturation of this capability monitoring and detection of this activity on endpoints and IT infrastructure in real time	Components can use policies to deny devices by default and explicitly allow access to DAAS resources only by devices that meet mandated configuration standards. Security threats identified are remediated faster through continuous activity inspection enables faster remediation of security threats	* Entity Activity Monitoring Pt1 * Entity Activity Monitoring Pt2 * Implement Application Control & File Integrity Monitoring (FIM) Tools * Integrate NextGen AV Tools with C2C * Fully Integrate Device Security stack with C2C as appropriate * Enterprise PKI Pt1 * Enterprise PKI Pt2
2.4	Remote Access	2 - Device	DoD organizations audit existing device access processes and tooling to set a least privilege baseline. In phase 2 this access is expanded to cover basic BYOD and IOT support using the Enterprise IDP for approved applications. The final phases expand coverage to include all BYOD and IOT devices for services using the approved set of device attributes.	DoD organizations establish policies to allow authorized users and devices access to the network or a device from a geographical distance through a network connection	Enables properly authorized and authenticated users and NPEs to access DAAS from remote locations	* Deny Device by Default Policy * Managed and Limited BYOD & IOT Support * Managed and Full BYOD & IOT Support Pt1 * Managed and Full BYOD & IOT Support Pt2
2.5	Partially & Fully Automated Asset, Vulnerability and Patch Management	2 - Device	DoD organizations establish processes to automatically test and deploy vendor patches for connected devices; hybrid patch management (both human and automated) is employed	DoD organizations establish processes to automatically test and deploy vendor patches for connected devices; hybrid patch management (both human and automated) is employed	Risk is minimized by automatically deploying vendor patches to all network devices	* Implement Asset, Vulnerability and Patch Management Tools
2.6	Unified Endpoint Management (UEM) & Mobile Device Management (MDM)	2 - Device	DoD organizations establish a centralized UEM solution that provides the choices of agent and/or agentless management of computer and mobile devices to a single console regardless of device location. DoD-issued devices can be remotely managed and security policies are enforced.	DoD organizations establish a centralized UEM tool that provides the choices of agent and/or agentless management of computer and mobile devices to a single console. DoD-issued mobile devices are remotely managed and security policies are enforced.	DAAS resources are protected through agent and agentless management, IT is able to manage, secure, and deploy resources and applications on any device from a single console to provide redress of cybersecurity threats. Security vulnerabilities are mitigated, and policy enforcement measures are received through IT remote management of DoD-issued mobile devices	* Implement UEDM or equivalent Tools * Enterprise Device Management Pt1 * Enterprise Device Management Pt2

Return to Capability Overview

Capability Definitions

ID #	Capability	Pillar	Capability Description	Capability Outcome	Impact to ZT	Activities
2.7	Endpoint & Extended Detection & Response (EDR & XDR)	2 - Device	DoD organizations use endpoint detection and response (EDR) tooling to monitor, detect, and remediate malicious activity on endpoints. Expanding the capability to include XDR tooling allows organizations to account for activity beyond the endpoints such as cloud and network as well.	DoD organizations use EDR tools to monitor, detect, and remediate malicious activity on endpoints as a baseline. Upgrading to XDR tools allows organizations to account for activity beyond the endpoints.	Threats originating from network-connected endpoints are initially reduced through active investigation and response. Maturation focuses on forensics and faster threat detection and remediation are enabled by correlating data across multiple security layers (e.g., email, cloud, endpoint)	* Implement Endpoint Detection & Response (EDR) Tools and Integrate with C2C * Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt1 * Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt2
3.1	Application Inventory	3 - Applications and Workloads	System owners ensure that all applications and application components are identified and inventoried; only applications and application components that have been authorized by the appropriate authorizing official/CISO/CIO shall be utilized within the system owner's purview	System owners ensure that all applications and application components are identified and inventoried; only applications and application components that have been authorized by the appropriate authorizing official/CISO/CIO shall be utilized within the system owner's purview	Unauthorized applications and application components are not used on or within the system	* Application/Code Identification
3.2	Secure Software Development & Integration	3 - Applications and Workloads	Foundational software and application security processes and infrastructure are established following Zero Trust principles and best practices. Controls such as code review, runtime protection, secure API gateways, container and serverless security are integrated and automated.	Organization-defined security controls and practices are integrated, to include Zero Trust security controls and virtualization, into the software development lifecycle and DevOps toolchain. Custom software development teams use DevSecOps to integrate static and dynamic application security testing into software delivery workflows in accordance with the organization's requirements (policies, technologies, and processes).	Zero Trust security concepts, processes, and capabilities are accepted and integrated across the DevOps toolchain, to include static and dynamic application security testing necessary for the discovery of weaknesses and vulnerabilities during application development	* Build DevSecOps Software Factory Pt1 * Build DevSecOps Software Factory Pt2 * Automate Application Security & Code Remediation Pt1 * Automate Application Security & Code Remediation Pt2
3.3	Software Risk Management	3 - Applications and Workloads	DoD organizations establish software/application risk management program. Foundational controls include Bill of Materials risk management, Supplier Risk Management, approved repositories and update channels, and vulnerability management program. Additional controls include Continual validation within the CI/CD pipelines and vulnerability maturation with external sources.	DoD establishes policies and procedures to secure supply chain cybersecurity for code components within DoD and DIB systems by evaluating and identifying supplier sourcing risk for approved sources, creating repositories and update channels for use by development teams, creating Bill of Materials for applications to identify source, supportability and risk posture, and establishing industry standard (DIB) and approved vulnerability databases for use in DevSecOps	Code used in DAAS and associated components of the supply chain is secure, vulnerabilities are reduced, and DoD is aware of potential risks	* Approved Binaries/Code * Vulnerability Management Program Pt1 * Vulnerability Management Program Pt2 * Continual Validation

Return to Capability Overview

Capability Definitions

ID #	Capability	Pillar	Capability Description	Capability Outcome	Impact to ZT	Activities
3.4	Resource Authorization & Integration	3 - Applications and Workloads	DoD establishes a standardized resource authorization gateway for authorizations via the CI/CD pipelines in a risk approach that reviews the User, Device and Data security posture. Authorizations utilize a programmatic (e.g., Software Defined) approach in a live/production environment. Attributes are enriched utilizing other pillar activities and the API and Authorization gateway. Approved enterprise APIs are micro-segmented using authorizations.	DoD establishes a standard approach managing the authorizations of resources in a risk approach that reviews the User, Device and Data security posture.	Resource authorization enables the ability for limited access to those resources and in a programmatic way in later stages. This improvise the ability to remove access when it is not needed.	* Resource Authorization Pt1 * Resource Authorization Pt2 * SDC Resource Authorization Pt1 * SDC Resource Authorization Pt2 * Enrich Attributes for Resource Authorization Pt1 * Enrich Attributes for Resource Authorization Pt2 * REST API Micro-Segments
3.5	Continuous Monitoring and Ongoing Authorizations	3 - Applications and Workloads	DoD organizations employ automated tools and processes to continuously monitor applications and assess their authorization to operate	DoD organizations employ automated tools and processes to continuously monitor applications and assess their authorization to operate	Near real time visibility into the effectiveness of deployed security controls	* Continuous Authorization to Operate (cATO) Pt1 * Continuous Authorization to Operate (cATO) Pt2
4.1	Data Catalog Risk Alignment	4 - Data	Data owners ensure that data is identified and inventoried and any changes to the data landscape are automatically detected and included within the catalog. The data landscape must then be reviewed to identify potential risks related to data loss, attack, or any other unauthorized alteration and/or access	Data owners ensure that data is identified and inventoried and any changes to the data landscape are automatically detected and included within the catalog. The data landscape must then be reviewed to identify potential risks related to data loss, attack, or any other unauthorized alteration and/or access	Data assets are known and can therefore be collected, tagged, and protected according to risk levels in alignment with a prioritization framework, and encrypted for protection	* Data Analysis
4.2	DoD Enterprise Data Governance	4 - Data	DoD establishes enterprise data labeling/tagging and DAAS access control/sharing policies (e.g., SDS policy) that are enforceable. Developed enterprise standards ensure an appropriate level of interoperability between DoD Organizations.	DoD establishes enterprise data labeling/tagging and DAAS access control/sharing policies (e.g., SDS policy) that are enforceable at the field level	Decision rights and accountability framework ensure appropriate behavior in the valuation, creation, consumption, and control of data and analytics	* Define Data Tagging Standards * Interoperability Standards * Develop Software Defined Storage (SDS) Policy
4.3	Data Labeling and Tagging	4 - Data	Data owners label and tag data in compliance with DoD enterprise governance on labeling/tagging policy. As phases advance automation is used to meet scaling demands and provide better accuracy.	Data owners label and tag data in compliance with DoD enterprise governance on labeling/tagging policy	Establishing machine enforceable data access controls, risk assessment, and situational awareness require consistently and correctly labeled and tagged data	* Implement Data Tagging & Classification Tools * Manual Data Tagging Pt1 * Manual Data Tagging Pt2 * Automated Data Tagging & Support Pt1 * Automated Data Tagging & Support Pt2

Return to Capability Overview

Capability Definitions

ID #	Capability	Pillar	Capability Description	Capability Outcome	Impact to ZT	Activities
4.4	Data Monitoring and Sensing	4 - Data	Data owners will capture active metadata that includes information about the access, sharing, transformation, and use of their data assets. Data Loss Prevention (DLP) and Data Rights Management (DRM) enforcement point analysis is conducted to determine where tooling will be deployed. Data outside of DLP and DRM scope such as File Shares and Databases is actively monitored for anomalous and malicious activity using alternative tooling.	Data owners will capture active metadata that includes information about the access, sharing, transformation, and use of their data assets	Data in all states are detectable and observable	* DLP Enforcement Point Logging and Analysis * DRM Enforcement Point Logging and Analysis * File Activity Monitoring Pt1 * File Activity Monitoring Pt2 * Database Activity Monitoring * Comprehensive Data Activity Monitoring
4.5	Data Encryption & Rights Management	4 - Data	DoD organizations establish and implement a strategy for encrypting data at rest and in transit using Data Rights Management (DRM) tooling. The DRM solution utilizes data tags to determine protection and lastly integrates with ML and AI to automate protection	DoD organizations establish and implement a strategy for encrypting data at rest and in transit	Encrypting data in all states reduces the risk of unauthorized data access and improves data security	* Implement DRM and Protection Tools Pt1 * Implement DRM and Protection Tools Pt2 * DRM Enforcement via Data Tags and Analytics Pt1 * DRM Enforcement via Data Tags and Analytics Pt2 * DRM Enforcement via Data Tags and Analytics Pt3
4.6	Data Loss Prevention (DLP)	4 - Data	DoD organizations utilize the identified enforcement points to deploy approved DLP tools and integrate tagged data attributes with DLP. Initially the DLP solution is put into a "monitor-only" mode to limit business impact and later using analytics is put into a "prevent" mode. Extended data tag attributes are used to feed the DLP solution and lastly integrate with ML and AI.	DoD organizations have identified enforcement points, deployed approved DLP tools at those enforcement points, and integrate tagged data attributes with DLP	Data breaches and data exfiltration transmissions are detected and mitigated	* Implement Enforcement Points * DLP Enforcement via Data Tags and Analytics Pt1 * DLP Enforcement via Data Tags and Analytics Pt2 * DLP Enforcement via Data Tags and Analytics Pt3
4.7	Data Access Control	4 - Data	DoD organizations ensure appropriate access to and use of data based on the data and user/NPE/device properties. Software Defined Storage (SDS) is utilized to scale manage permissions to DAAS. Lastly the SDS solution(s) is integrated with DRM tooling improving protections.	DoD organizations ensure appropriate access to and use of data based on the data and user/NPE/device properties	Unauthorized entities, or any entity on an unauthorized device cannot access data; Zero Trust cybersecurity will be sufficiently strong to separate community of interest data access for data in the same classification	* Integrate DAAS Access w/ SDS Policy Pt1 * Integrate DAAS Access w/ SDS Policy Pt2 * Integrate DAAS Access w/ SDS Policy Pt3 * Integrate Solution(s) and Policy with Enterprise IDP Pt1 * Integrate Solution(s) and Policy with Enterprise IDP Pt2 * Implement SDS Tool and/or integrate with DRM Tool Pt1 * Implement SDS Tool and/or integrate with DRM Tool Pt2

Return to Capability Overview

Capability Definitions

ID #	Capability	Pillar	Capability Description	Capability Outcome	Impact to ZT	Activities
5.1	Data Flow Mapping	5 - Network and Environment	DoD organizations reconcile data flows by gathering, mapping, and visualizing network traffic data flows and patterns to ensure authorized access and protection for network and DAAS resources specifically tagging programmatic (e.g., API) access when possible.	DoD organizations reconcile data flows by gathering, mapping, and visualizing network traffic data flows and patterns to ensure authorized access and protection for network and DAAS resources	Sets the foundation for network segmentation and tighter access control by understanding data traffic on the network	* Define Granular Control Access Rules & Policies Pt1 * Define Granular Control Access Rules & Policies Pt2
5.2	Software Defined Networking (SDN)	5 - Network and Environment	DoD organizations define API decision points and implement SDN programmable infrastructure to separate the control and data planes and centrally manage and control the elements in the data plane. Integrations are conducted with decision points and segmentation gateway to accomplish the plane separation. Analytics are then integrated to real time decision making for access to resources.	DoD organizations define API decision points and implement SDN programmable infrastructure to separate the control and data planes and centrally manage and control the elements in the data plane	Enables the control of packets to a centralized server, provides additional visibility into the network, and enables integration requirements	* Define SDN APIs* Implement SDN Programable Infrastructure * Segment Flows into Control, Management, and Data Planes * Network Asset Discovery & Optimization * Real-Time Access Decisions
5.3	Macro Segmentation	5 - Network and Environment	DoD organizations establish network boundaries and provide security against networked assets located within an environment by validating the device, user, or NPE on each attempt of accessing a remote resource prior to connection.	DoD organizations establish network perimeters and provide security against devices located within an environment by validating the device, user, or NPE on each attempt of accessing a remote resource prior to connection	Network segmentation is defined by a large perimeter to enable resource segmentation by function and user type	* Datacenter Macro segmentation * B/C/P/S Macro segmentation
5.4	Micro Segmentation	5 - Network and Environment	DoD organizations define and document network segmentation based on identity and / or application access in their virtualized and/or cloud environments. Automation is used to apply policy changes through programmatic (e.g., API) approaches. Lastly where possible organizations will utilize host-level process micro segmentation.	DoD organizations define and document network segmentation based on identity and / or application access in their virtualized cloud environments	Network segmentation enabled by narrower and specific segmentation in a virtualized environment via identity and / or application access, allowing for improved protection of data in transit as it crosses system boundaries (e.g., in a coalition environment, system high boundaries) and supported dynamic, real-time access decisions and policy changes	* Implement Micro segmentation * Application & Device Micro segmentation * Process Micro segmentation * Protect Data In Transit

Return to Capability Overview

Capability Definitions

ID #	Capability	Pillar	Capability Description	Capability Outcome	Impact to ZT	Activities
6.1	Policy Decision Point (PDP) & Policy Orchestration	6 - Automation and Orchestration	DoD organizations initially collect and document all rule-based policies to orchestrate across the security stack for effective automation; DAAS access procedures and policies will be defined, implemented, and updated. Organizations mature this capability by establishing PDPs and PEPs (including the Next Generation Firewall) to make DAAS resource determinations and enable, monitor, and terminate connections between a user/device and DAAS resources according to predefined policy.	DoD organizations initially collect and document all rule-based policies to orchestrate across the security stack for effective automation; DAAS access procedures and policies will be defined, implemented, and updated. Organizations mature this capability by establishing PDPs and PEPs (including the Next Generation Firewall) to make DAAS resource determinations and enable, monitor, and terminate connections between a user/device and DAAS resources according to predefined policy	PDPs and PEPs ensure proper implementation of DAAS access policies to users or endpoints that are properly connected (or denied access) to requested resources	* Policy Inventory & Development * Organization Access Profile * Enterprise Security Profile Pt1 * Enterprise Security Profile Pt2
6.2	Critical Process Automation	6 - Automation and Orchestration	DoD organizations employ automation methods, such as RPA, to address repetitive, predictable tasks for critical functions such as data enrichment, security controls, and incident response workflows according to system security engineering principles.	DoD organizations employ automation methods, such as RPA, to address repetitive, predictable tasks for critical functions such as data enrichment, security controls, and incident response workflows according to system security engineering principles	Response time and capability is increased with orchestrated workflows and risk management processes	* Task Automation Analysis * Enterprise Integration & Workflow Provisioning Pt1 * Enterprise Integration & Workflow Provisioning Pt2
6.3	Machine Learning	6 - Automation and Orchestration	DoD organizations employ ML to execute (and enhance execution of) critical functions such as incident response, anomaly detection, user baselining, and data tagging.	DoD organizations employ ML to execute (and enhance execution of) critical functions such as incident response, anomaly detection, user baselining, and data tagging	Response time and capability is increased with orchestrated workflows and risk management processes	* Implement Data Tagging & Classification ML Tools
6.4	Artificial Intelligence	6 - Automation and Orchestration	DoD organizations employ AI to execute (and enhance execution of) critical functions - particularly risk and access determinations and environmental analysis.	DoD organizations employ AI to execute (and enhance execution of) critical functions - particularly risk and access determinations and environmental analysis	Response time and capability is increased with orchestrated workflows and risk management processes	* Implement AI automation tools * AI Driven by Analytics decides A&O modifications

Return to Capability Overview

Capability Definitions

ID #	Capability	Pillar	Capability Description	Capability Outcome	Impact to ZT	Activities
6.5	Security Orchestration, Automation & Response (SOAR)	6 - Automation and Orchestration	DoD organizations achieve initial operational capability of security technologies to orchestrate and automate policies (e.g., PEPs and PDPs) and rulesets to improve security operations, threat and vulnerability management, and security incident response by ingesting alert data, triggering playbooks for automated response and remediation.	DoD organizations achieve IOC of security technologies to orchestrate and automate policies (e.g., PEPs and PDPs) and rulesets to improve security operations, threat and vulnerability management, and security incident response by ingesting alert data, triggering playbooks for automated response and remediation	Pre-defined playbooks from collection to incident response and triage enables initial process automation that accelerates a security team's decision and response speed	* Response Automation Analysis * Implement SOAR Tools * Implement Playbooks
6.6	API Standardization	6 - Applications and Workloads	DoD establishes and enforces enterprise-wide programmatic interface (e.g., API) standards; all non-compliant APIs are identified and replaced.	DoD establishes and enforces enterprise-wide API standards; all non-compliant APIs are identified and replaced	Standardizing APIs across the department improves application interfaces, enabling orchestration, and enhancing interoperability	* Tool Compliance Analysis * Standardized API Calls & Schemas Pt1 * Standardized API Calls & Schemas Pt2
6.7	Security Operations Center (SOC) & Incident Response (IR)	7 - Visibility and Analytics 6 - Automation and Orchestration	In the event a computer network defense service provider (CNDSP) does not exist, DoD organizations define and stand up security operations centers (SOC) to deploy, operate, and maintain security monitoring, protections and response for DAAS; SOCs provide security management visibility for status (upward visibility) and tactical implementation (downward visibility). Workflows within the SOC are automated using automation tooling and enrichment occurs between service providers and technologies.	In the event a CNDSP does not exist, DoD organizations define and stand up SOCs to deploy, operate, and maintain security monitoring, protections and response for DAAS; SOCs provide security management visibility for status (upward visibility) and tactical implementation (downward visibility)	Standardized, coordinated, and accelerated incident response and investigative efforts	* Workflow Enrichment Pt1 * Workflow Enrichment Pt2 * Workflow Enrichment Pt3 * Automated Workflow
7.1	Log All Traffic (Network, Data, Apps, Users)	7 - Visibility and Analytics	DoD organizations collect and process all logs including network, data, application, device, and user logs and make those logs available to the appropriate Computer Network Defense Service Provider (CNDSP) or security operations center (SOC). Logs and events follow a standardized format and rules/analytics are developed as needed.	DoD organizations collect and process all logs including network, data, application, device, and user logs and make those logs available to the appropriate Computer Network Defense Service Provider (CNDSP) or SOC	Foundational to the development of automated hunt and incident response playbooks	* Scale Considerations * Log Parsing * Log Analysis

Return to Capability Overview

Capability Definitions

ID #	Capability	Pillar	Capability Description	Capability Outcome	Impact to ZT	Activities
7.2	Security Information and Event Management (SIEM)	7 - Visibility and Analytics	Computer Network Defense Service Provider (CNDSP) or security operations centers (SOC) monitor, detect, and analyze data logged into a security information and event management (SIEM) tool. User and device baselines are created using security controls and integrated with the SIEM. Alerting within the SIEM is matured over the phases to support more advanced data points (e.g., Cyber Threat Intel, Baselines, etc.)	CNDSPs/SOCs monitor, detect, and analyze data logged into a security information and event management (SIEM) tool	Processing and exploiting data in the SIEM enables effective security analysis of anomalous user behavior, alerting, and automation of relevant incident response to common threat events	* Threat Alerting Pt1 * Threat Alerting Pt2 * Threat Alerting Pt3 * Asset ID & Alert Correlation * User/Device Baselines
7.3	Common Security and Risk Analytics	7 - Visibility and Analytics	Computer Network Defense Service Provider (CNDSP) or security operations centers (SOC) employ data tools across their enterprises for multiple data types to unify data collection and examine events, activities, and behaviors.	CNDSPs/SOCs employ big data tools across their enterprises for multiple data types to unify data collection and examine events, activities, and behaviors	Analysis integrated across multiple data types to examine event, activities, and behaviors	* Implement Analytics Tools * Establish User Baseline Behavior
7.4	User and Entity Behavior Analytics	7 - Visibility and Analytics	DoD organizations initially employ analytics to profile and baseline activity of users and entities and to correlate user activities and behaviors and detect anomalies. Computer Network Defense Service Provider (CNDSP) or security operations centers (SOC) mature this capability through the employment of advanced analytics to profile and baseline activity of users and entities and to correlate user activities and behaviors, and detect anomalies.	DoD organizations initially employ analytics to profile and baseline activity of users and entities and to correlate user activities and behaviors and detect anomalies. CNDSPs/SOCs mature this capability through the employment of advanced analytics to profile and baseline activity of users and entities and to correlate user activities and behaviors, and detect anomalies	Advanced analytics support detection of anomalous users, devices, and NPE actions and advanced threats	* Baseline & Profiling Pt1 * Baseline & Profiling Pt2 * UEBA Baseline Support Pt1 * UEBA Baseline Support Pt2
7.5	Threat Intelligence Integration	7 - Visibility and Analytics	Computer Network Defense Service Provider (CNDSP) or security operations centers (SOC) integrate threat intelligence information and streams about identities, motivations, characteristics, and tactics, techniques and procedures (TTPs) with data collected in the SIEM.	CNDSPs/SOCs integrate threat intelligence information and streams about identities, motivations, characteristics, and tactics, techniques and procedures (TTPs) with data collected in the SIEM	Integrating threat intelligence into other SIEM data enhances monitoring efforts and incident response	* Cyber Threat Intelligence Program Pt1 * Cyber Threat Intelligence Program Pt2

Return to Capability Overview

Capability Definitions

ID #	Capability	Pillar	Capability Description	Capability Outcome	Impact to ZT	Activities
7.6	Automated Dynamic Policies	7 - Visibility and Analytics	DoD Organization ML & AI solutions dynamically and automatically update security profiles and device configuration through continuous security posture monitoring, risk and confidence scoring, and automated patch management.	CNDSPs/SOCs dynamically and automatically update security profiles and device configuration through continuous security posture monitoring, risk and confidence scoring, and automated patch management	Users and NPEs are denied access based on automated, real-time security profiles based on external conditions and evolving risk and confidence scores	* AI-enabled Network Access * AI-enabled Dynamic Access Control

Return to Capability Overview