

UNCLASSIFIED



CLEARED
For Open Publication

Dec 09, 2024

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

SLIDES ONLY
NO SCRIPT PROVIDED



Zero Trust Execution Roadmap v1.1

22 November 2024

UNCLASSIFIED

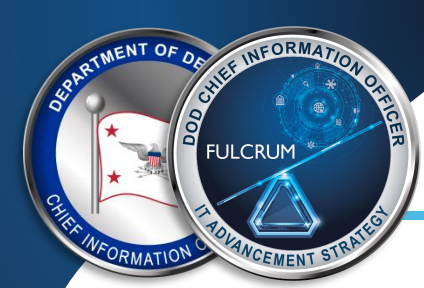


Table Of Contents

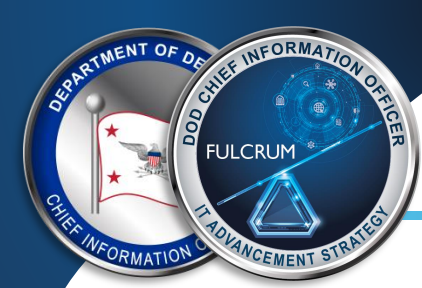
- 1 Introduction
- 2 Zero Trust Courses of Action
- 3 Key Considerations for Courses of Action
- 4 Courses of Action Use Cases
- 4 ZT Assessment Process for Courses of Action
- 5 Hybrid Courses of Action Approach

Appendices

Appendix A: COA 1 Timeline Details (Uplifting Legacy)

Appendix B: Capability Definitions

ZT Execution Roadmap Update

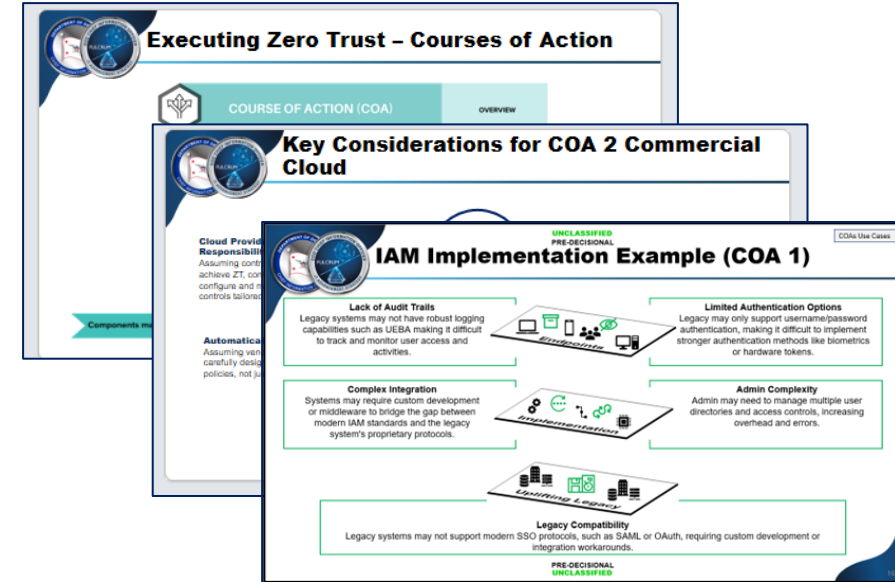


Define, Understand, and Contextualize*

ID#	Activity Name	Associated Capability	Phase	Duration (months)	Descriptions	Outcomes	Predecessor(s)	Successor(s)
1.1.1	Inventory User	1.1 User Inventory	Target Level ZT	25.9	DoD Organizations establish and update a user inventory manually if needed, preparing for automated approach in later stages. Accounts both centrally managed by an IdP/ICAM and locally on systems will be identified and inventoried. Privileged accounts will be identified for future audit and both standard and privileged user accounts local to applications and systems will be identified for future migration and/or decommission.	Identified Managed Regular Users; Identified Managed Privileged Users; Identified applications using their own user account management for non-administrative and administrative accounts		
1.2.1	Implement App Based Permissions per Enterprise	1.2 Conditional User Access	Target Level ZT	17.7	The DoD enterprise working with the Organizations establishes a basic set of user attributes for authentication and authorization. These are integrated with the "Enterprise Identity Life-Cycle Management P11" activity process for a complete enterprise standard. The enterprise Identity, Credential and Access Management (ICAM) solution is enabled for self-service functionality for adding/updating attributes within the solution. Remaining Privileged Access Management (PAM) activities are fully migrated to PAM solution.	Enterprise roles/attributes needed for user authorization to application functions and/or data have been registered with enterprise ICAM. DoD Enterprise ICAM has self-service attribute/role registration service that enables application owners to add attributes or use existing enterprise attributes. Privileged activities are fully migrated to PAM.		
1.2.2	Rule Based Dynamic Access P12	1.2 Conditional User Access	Target Level ZT	22.1	DoD Organizations utilize the rules from the "Periodic Authentication" activity to build basic rules enabling and disabling privileges dynamically. High-risk user accounts utilize the PAM solution to move to dynamic privileged access using Just-in-Time access and Just-Enough-Administration methods.	Access to application's/service's functions and/or data are limited to users with appropriate enterprise attributes. All possible applications use JIT/JEA permissions for administrative users	Single Authentication	Rule Based Dynamic Access P12; AI-enabled Network Access
1.2.3	Rule Based Dynamic Access P12	1.2 Conditional User Access	Advanced ZT	15.5	DoD Organizations expand the development of rules for dynamic access decision making accounting for risk. Solutions used for dynamic access are integrated with cross pillar Machine Learning and Artificial Intelligence functionality enabling automated rule management.	Components and services are fully utilizing rules to enable dynamic access to applications and services; Technology utilized for Rule Based Dynamic Access supports integration with AI/ML tooling	Rule Based Dynamic Access P12; File Activity Monitoring P12	

Producing a common lexicon on activity descriptions, dependencies, outcomes, and end state were the first steps

Develop and Refine



Continuing to develop and refine COAs for achieving Zero Trust will enable implementation and strengthen security posture

This update to the DoD Capability Execution Roadmap provides key considerations and implementation example use cases for each of three Courses of Action (COAs)

* Note: Refinements to a select number of Target Level Activity descriptions and outcomes are detailed in a complementary .xls file published separately

DoD Zero Trust by Fiscal Year 2027

Zero Trust is a security model that provisions access to data, applications, assets, and services only after strict authentication and authorization of a user's identity, infrastructure resources, and rule/policy context of each access request is affirmed

MISSION

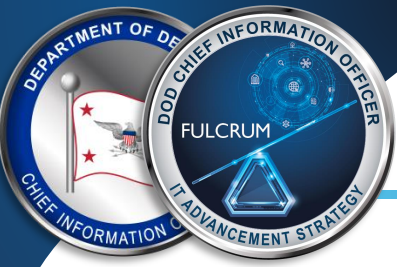
Lead and synchronize the Department's effort to accelerate Zero Trust adoption across the DoD & achieve *Target Level ZT* before the end of FY27.



VISION

Convert the DoD Information Enterprise into a fully implemented, Zero Trust framework which prevents adversary freedom of movement & exploitation of DoD data.

The DoD Zero Trust Strategy



Vision

A DoD Information Enterprise secured by a fully implemented, Department-wide Zero Trust cybersecurity framework

Goals

What We Understand & Agree To

1. Zero Trust Cultural Adoption

A Zero Trust security framework and mindset guide the design, development, integration, and deployment of information technology across the DoD Zero Trust Ecosystem

What to "Do"

2. DoD Information Systems Secured & Defended

DoD cybersecurity practices incorporate and operationalize Zero Trust to achieve enterprise resilience in DoD information systems

How to "Do" Zero Trust

3. Technology Acceleration

Zero Trust-based technologies deploy at a pace equal to or exceeding industry advancements





What Support is Needed

4. Zero Trust Enablement

DoD Zero Trust execution integrates with Department- and Component-level processes

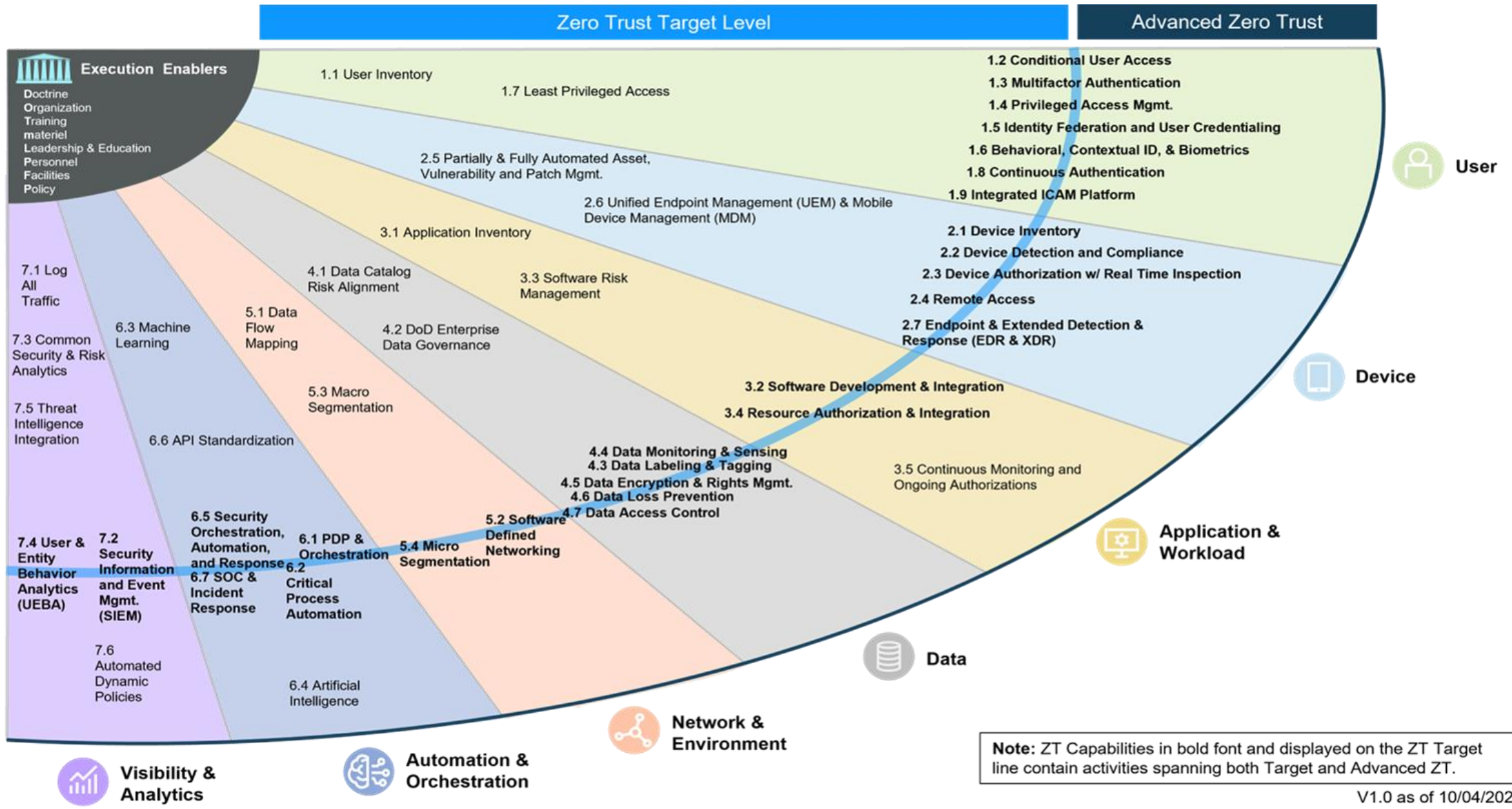
Focus of Courses of Action (COAs)

Executing Zero Trust – Courses of Action

	COURSE OF ACTION (COA)	OVERVIEW
	COA 1: Uplifting Legacy	Components augment existing and/or new infrastructure integration to meet Target and/or Advanced level ZT.
	COA 2: Commercial Cloud	Components leverage Cloud Service offerings from Cloud Service Providers if they meet Target and/or Advanced level ZT.
	COA 3: Purpose-Built On-Premise Cloud	An on-premise cloud owned, controlled and operated by a single organization (i.e.: DoD) or a Component to meet Target and/or Advanced level ZT.

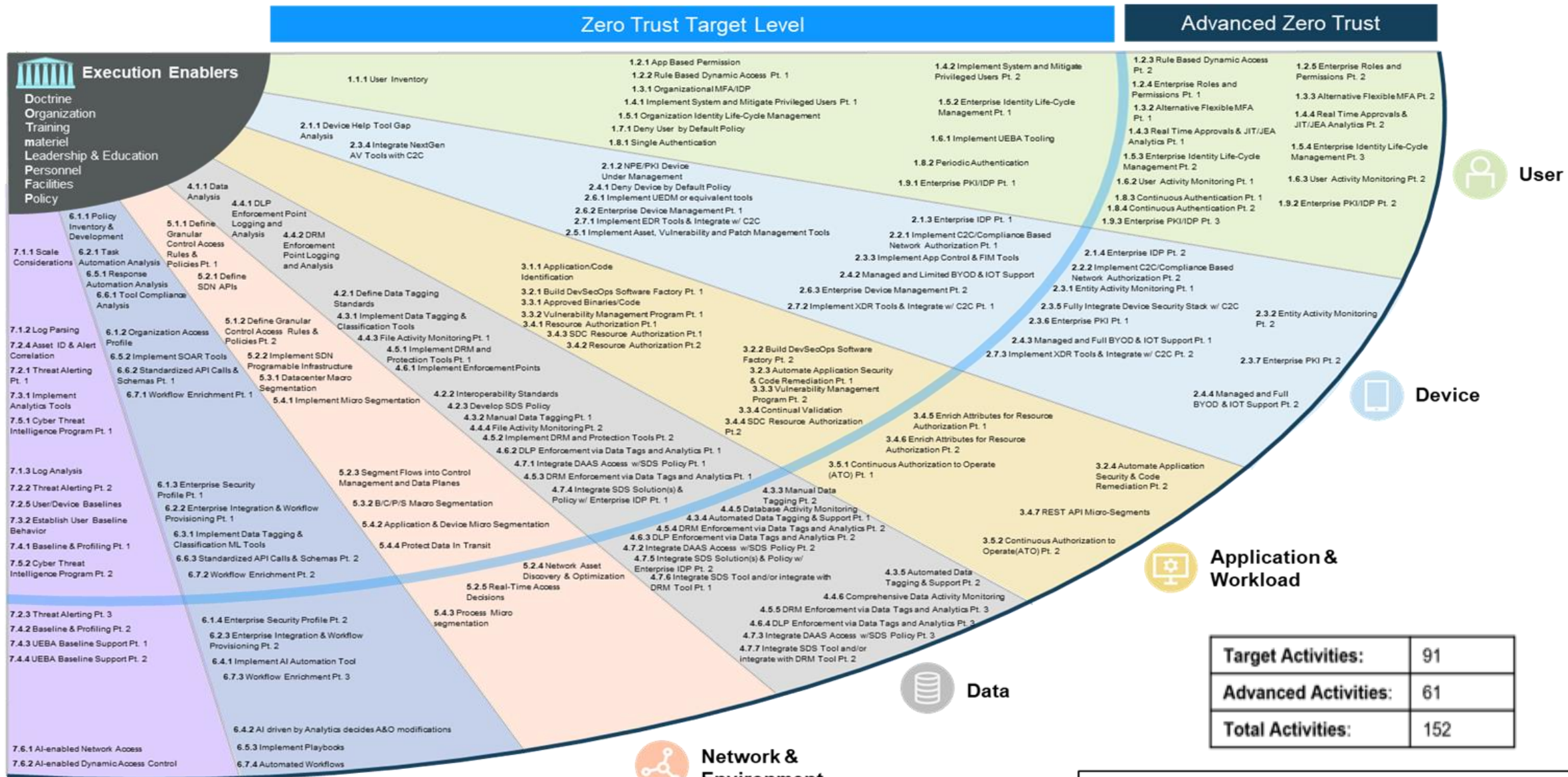
Components may choose to leverage any or all of the COAs in their hybrid approach to meet their unique mission requirements

42 ZT Capabilities within TARGET + 3 ZT Capabilities within ADVANCED = 45 ZT Capabilities for Maximum Level ZT (full achievement of ADVANCED Level ZT within DoD)



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

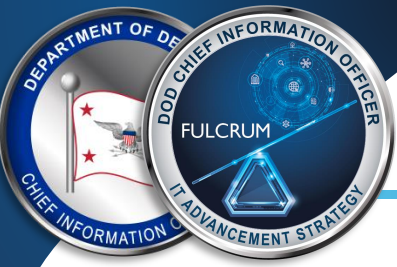
91 ZT Activities within TARGET + 61 ZT Activities within ADVANCED = 152 ZT Activities for Maximum Level ZT (full achievement of ADVANCED Level)



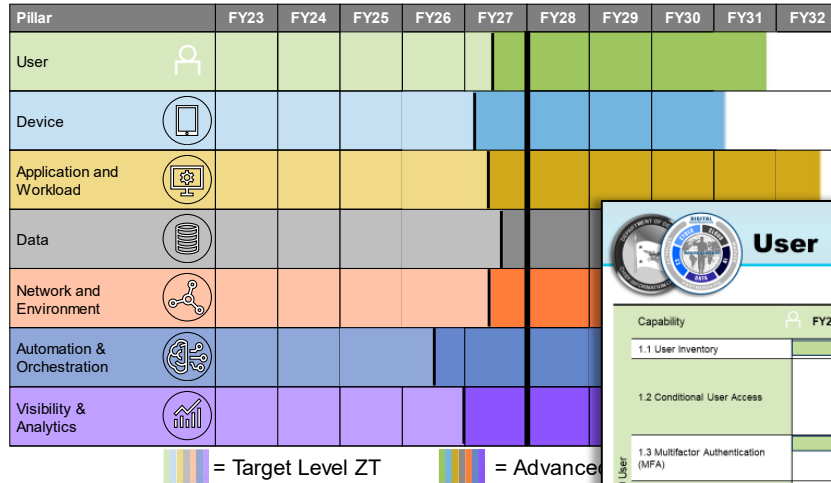
Target Activities:	91
Advanced Activities:	61
Total Activities:	152

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

ZT Implementation Timeline Example

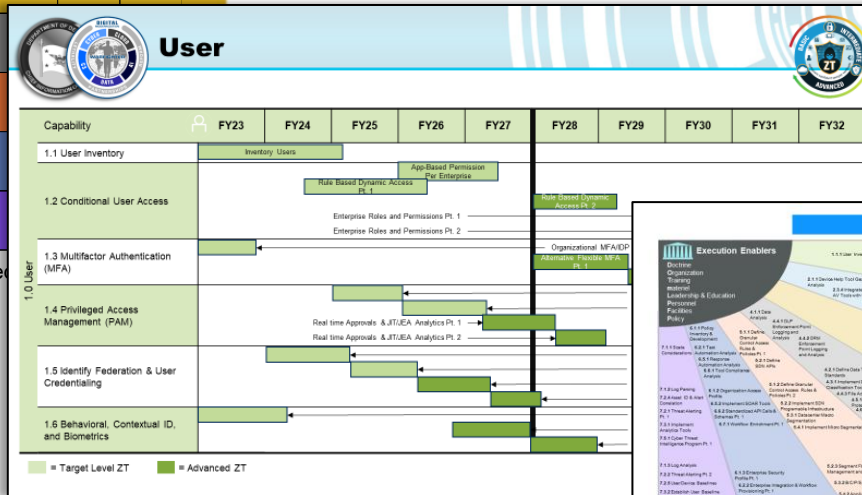


COA 1 Uplifting Legacy



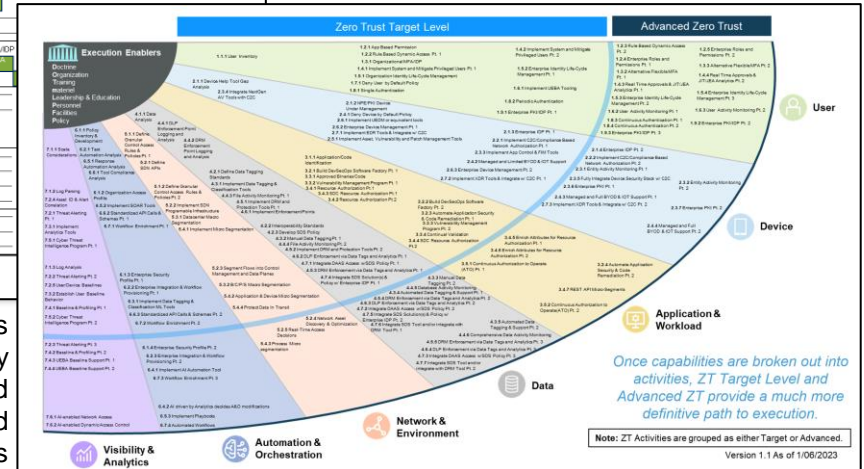
Seven pillar view of the timeline

Note: All durations are notional, based on COA 1



Activities & timeline at the individual pillar level

All activities to achieve by Target and Advanced Levels



The goal was to establish a notional timeline with clear sequencing for each activity at the individual pillar level agnostic of a solution with a COA 1 approach

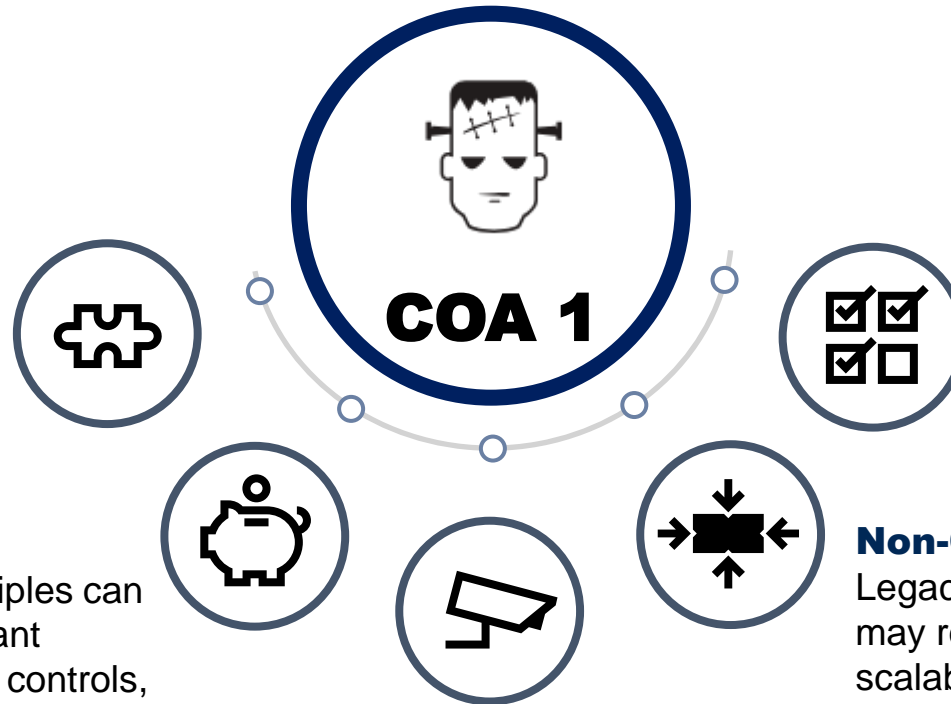
Key Considerations: Uplifting Legacy

Legacy System Compatibility

Legacy system compatibility in brownfield approaches can be challenging, requiring additional resources, time, and expertise to ensure interoperability.

Complexity and Costs

Retrofitting existing systems for ZT principles can be complex and costly, requiring significant changes to network architecture, access controls, and security mechanisms.



Self-Operated Challenges

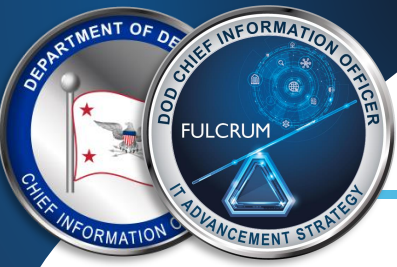
Often requires self operation and management for all aspects of the system including security controls, monitoring, and access management.

Non-Cloud Native and Limited Scalability

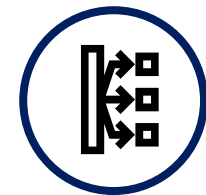
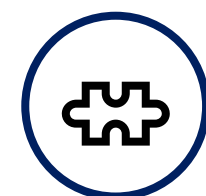
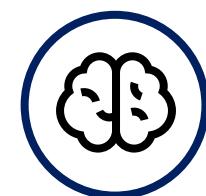
Legacy applications may not be designed for cloud. It may rely on traditional perimeter security and have scalability limitations.

Limited Visibility and Control

Limited visibility and control in brownfield environments can hinder identification and resolution of security gaps.



Key Considerations: Commercial Cloud



Cloud Provider Security Responsibility

Should not assume security responsibility is transferred to the commercial cloud provider, ZT is a shared responsibility.

Learning and Development

May require comprehensive training on the new security protocols and technologies involved in ZT architecture with commercial cloud

Automatically Achieve Zero Trust

Should not assume that controls will automatically achieve ZT, still required to carefully design and implement enforcement policies, not just lift and shift.

Network Segmentation

Cloud offers isolating features; but true network segmentation requires careful design, configuration, and enforcement within the cloud, regardless of the underlying infrastructure.

Legacy Application Compatibility

Need to assess status of legacy apps and modernization strategy to understand dependencies that may not easily be compatible with commercial cloud.

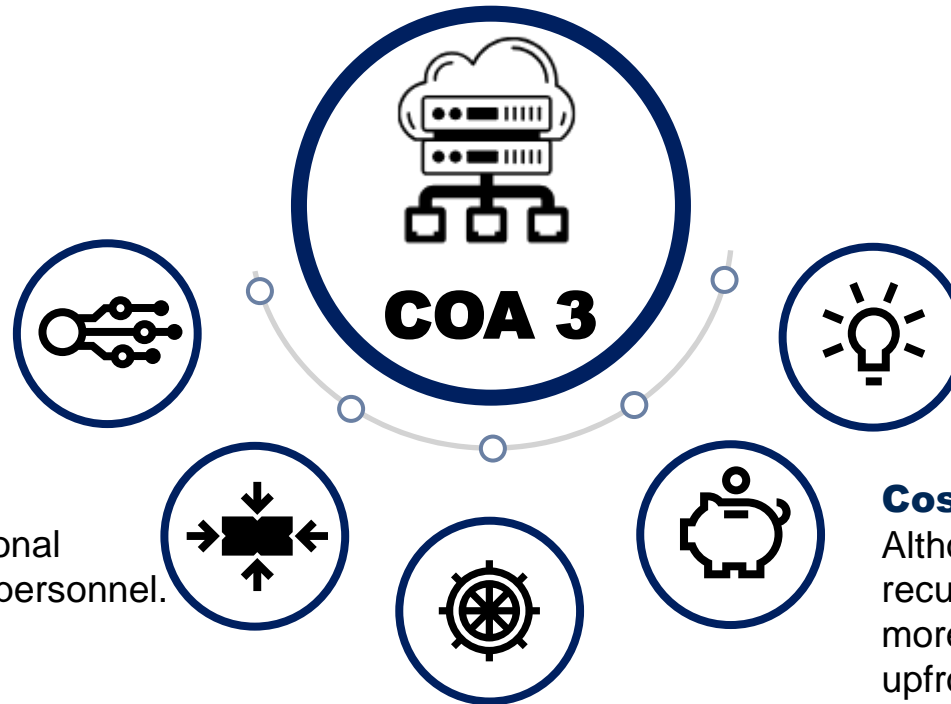
Key Considerations: Purpose-Built On-Prem Cloud

Infrastructure and Design

Unique environments require implementing controls, authentication, and network segmentation tailored to specific on-prem infrastructure needs.

Scalability and Flexibility

Scaling and adapting may require additional investments in hardware, software, and personnel.



Rapid Innovation

Commercial cloud providers may offer a wider range of cutting-edge services, features that may not be easily replicated to on-prem; must consider the trade-offs.

Cost Efficiency

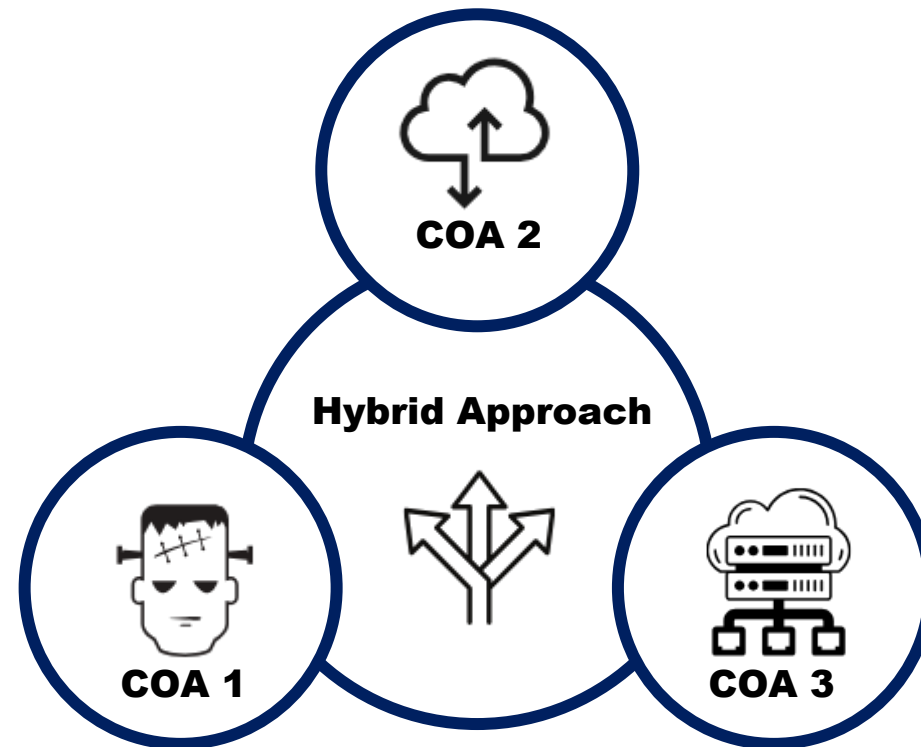
Although commercial cloud may entail more recurring costs, should not assume COA 3 is more cost effective; COA 3 may require more upfront investments on infrastructure, skilled personnel, and maintenance.

Level of Control

On prem-cloud may offer more direct control over infrastructure and data with direct oversight and custom security measures.

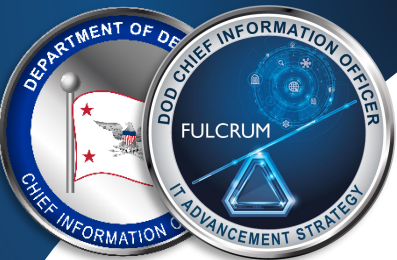
COAs Reinforce & Augment Each Other

Selecting any single COA does not prohibit the employment of any other COA – they can all be employed together to achieve ZT



Certain COAs may optimize efforts to reach Target or Advanced ZT Level for specific systems, resulting in a more effective and accelerated ZT adoption across the DoD Information Environment

ZT Assessment and Risk Management For All COAs



ZT Readiness Assessment Tool (ZRAT)

Get a baseline understanding of your environment for ZT compliance and map ZT activities to the corresponding security controls.

Automated Threat Based Cyber Assessment (TBCA)

Simulate Tactics, Techniques, and Procedures (TTPs) for ZT efficacy.

Advanced Persistent Threat (APT) Exercises

Conduct APT purple team exercises.

ZT Overlays

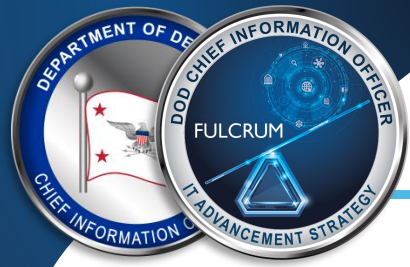
Utilize ZT Overlays as part of the Risk Management Framework Process (RMF) to attain accreditation.

Operational & Continuous Assessment

Continue to assess environment for breach, lateral movement, and ZT drift from assessed baseline.

Validate solutions meet ZT activities & outcomes & ensure ZT principles are integrated and upheld over time.

Implementation Example Use Cases



The following examples demonstrate how each COA can be deployed independently or in a hybrid approach when implementing specific ZT activities (e.g., IAM, EDR, and SIEM)*

IAM Implementation Example (COA 1)

- Lack of Audit Trails**: Legacy systems may not have robust logging capabilities such as UEBA making it difficult to track and monitor user access and activities.
- Limited Authentication Options**: Legacy may only support username/password authentication, making it difficult to implement stronger authentication methods like biometrics or hardware tokens.

IAM Implementation Example (COA 2)

- Complex Integration**: Systems may require custom development or middleware to bridge the gap between modern IAM standards and the legacy system's proprietary protocols.
- Admin Complexity**: Admin may need to manage multiple user directories and access controls, increasing overhead and errors.

IAM Implementation Example (COA 3)

- Data Sovereignty**: On-prem IAM solutions may have data residency requirements that conflict with cloud-based IAM services.
- Integration with Legacy Systems**: On-prem IAM solutions may require custom development or integration workarounds.

IAM Implementation Example (COA 1)

- Lack of Audit Trails**: Legacy systems may not have robust logging capabilities such as UEBA making it difficult to track and monitor user access and activities.
- Limited Authentication Options**: Legacy may only support username/password authentication, making it difficult to implement stronger authentication methods like biometrics or hardware tokens.
- Complex Integration**: Systems may require custom development or middleware to bridge the gap between modern IAM standards and the legacy system's proprietary protocols.
- Admin Complexity**: Admin may need to manage multiple user directories and access controls, increasing overhead and errors.
- Legacy Compatibility**: Legacy systems may not support modern SSO protocols, such as SAML or OAuth, requiring custom development or integration workarounds.

EDR Implementation Example (COA 1)

- Enhanced Visibility and Coverage**: Cloud-based EDR solutions offer broader visibility and coverage than on-premises systems, allowing for better threat detection and faster incident response across all endpoints, regardless of location or environment.
- Advanced Analytics and AI Capabilities**: Analyze data in real-time, detect anomalies, and identify threats more effectively using cloud resources and AI-driven analytics.

EDR Implementation Example (COA 2)

- Rapid Deployment**: Components can quickly implement and secure endpoints using pre-configured templates, automated provisioning, and streamlined deployment processes.
- Scalable and Flexible**: Cloud-based EDR solutions can dynamically scale resources and handle large data volumes for optimal performance.

EDR Implementation Example (COA 3)

- Reduced Infrastructure and Maintenance Costs**: Cloud-based EDR solutions minimize upfront hardware and software costs and ongoing maintenance expenses. Scale resources as needed, optimizing costs through a pay-as-you-go model of cloud services.
- Continuous Updates and Maintenance**: Cloud-based EDR solutions receive regular updates, patches, and new features automatically, ensuring up-to-date protection against emerging threats.

EDR Implementation Example (COA 2)

- Enhanced Visibility and Coverage**: Cloud-based EDR solutions offer broader visibility and coverage than on-premises systems, allowing for better threat detection and faster incident response across all endpoints, regardless of location or environment.
- Advanced Analytics and AI Capabilities**: Analyze data in real-time, detect anomalies, and identify threats more effectively using cloud resources and AI-driven analytics.
- Rapid Deployment**: Components can quickly implement and secure endpoints using pre-configured templates, automated provisioning, and streamlined deployment processes.
- Scalable and Flexible**: Cloud-based EDR solutions can dynamically scale resources and handle large data volumes for optimal performance.
- Reduced Infrastructure and Maintenance Costs**: Cloud-based EDR solutions minimize upfront hardware and software costs and ongoing maintenance expenses. Scale resources as needed, optimizing costs through a pay-as-you-go model of cloud services.
- Continuous Updates and Maintenance**: Cloud-based EDR solutions receive regular updates, patches, and new features automatically, ensuring up-to-date protection against emerging threats.

SIEM Implementation Example (COA 1)

- Complete Visibility**: On-prem SIEM solutions can provide stringent security measures and have complete visibility over infrastructure.
- Strict Data Controls**: On-prem SIEM allows the choice for specific storage infrastructure, such as dedicated servers or can implement longer retention/storing without relying on third-party cloud.
- Low Dependency On Connectivity**: On-prem SIEM solutions operate within the network infrastructure, ensuring continuous monitoring and analysis of security events, even during internet outages or disruptions.

SIEM Implementation Example (COA 2)

- Complete Visibility**: On-prem SIEM solutions can provide stringent security measures and have complete visibility over infrastructure.
- Strict Data Controls**: On-prem SIEM allows the choice for specific storage infrastructure, such as dedicated servers or can implement longer retention/storing without relying on third-party cloud.
- Low Dependency On Connectivity**: On-prem SIEM solutions operate within the network infrastructure, ensuring continuous monitoring and analysis of security events, even during internet outages or disruptions.

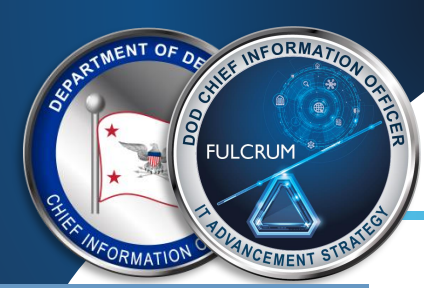
SIEM Implementation Example (COA 3)

- Complete Visibility**: On-prem SIEM solutions can provide stringent security measures and have complete visibility over infrastructure.
- Strict Data Controls**: On-prem SIEM allows the choice for specific storage infrastructure, such as dedicated servers or can implement longer retention/storing without relying on third-party cloud.
- Low Dependency On Connectivity**: On-prem SIEM solutions operate within the network infrastructure, ensuring continuous monitoring and analysis of security events, even during internet outages or disruptions.

SIEM Implementation Example (COA 3)

- Complete Visibility**: On-prem SIEM solutions can provide stringent security measures and have complete visibility over infrastructure.
- Strict Data Controls**: On-prem SIEM allows the choice for specific storage infrastructure, such as dedicated servers or can implement longer retention/storing without relying on third-party cloud.
- Low Dependency On Connectivity**: On-prem SIEM solutions operate within the network infrastructure, ensuring continuous monitoring and analysis of security events, even during internet outages or disruptions.

* Note: Identity and Access Management (IAM); Endpoint Detection & Response (EDR); and Security Information and Event Management (SIEM)



IAM Use Cases

- IAM Implementation – COA 1
- IAM Implementation – COA 2
- IAM Implementation – COA 3

IAM Implementation Example (COA 1)

Lack of Audit Trails

Legacy systems may not have robust logging capabilities such as UEBA making it difficult to track and monitor user access and activities.



Limited Authentication Options

Legacy may only support username/password authentication, making it difficult to implement stronger authentication methods like biometrics or hardware tokens.

Complex Integration

Systems may require custom development or middleware to bridge the gap between modern IAM standards and the legacy system's proprietary protocols.



Admin Complexity

Admin may need to manage multiple user directories and access controls, increasing overhead and errors.



Legacy Compatibility

Legacy systems may not support modern SSO protocols, such as SAML or OAuth, requiring custom development or integration workarounds.

IAM Implementation Example (COA 2)

Single Sign On

Commercial cloud often provides SSO capabilities allowing users to authenticate and access without repeated log ins.

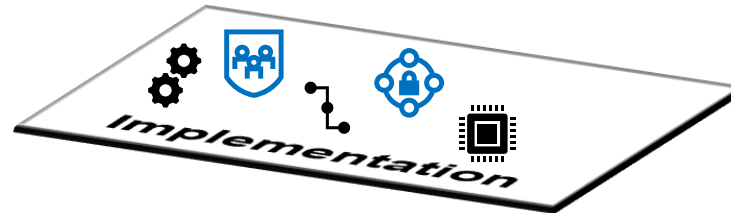


MFA

Typically offer built-in MFA with options like SMS-based codes, hardware token, biometric authentication.

RBAC and Conditional access

Offers RBAC mechanisms that enable granular access policies based on roles and permissions.



API Access Management

Cloud typically provides API access management capabilities, allowing secure access to APIs using authentication and authorization mechanisms.

Integration with Existing Systems

Commercial cloud can integrate with existing IAM such as Active Directory to assist with provisioning, deprovisioning, and synchronization.



Centralized Identity Management

Cloud IAM services offer centralized identity management capabilities, manage user identities, roles, and permissions in a unified manner.

IAM Implementation Example (COA 3)

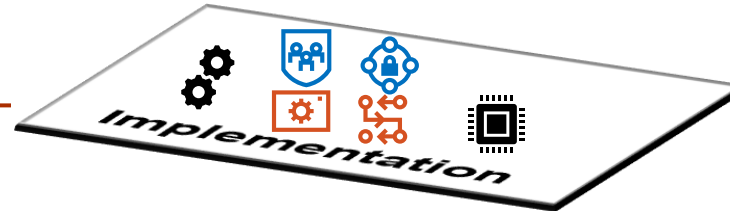
Data Sovereignty

Data remains within physical boundaries reducing the risk of unauthorized access or data breaches.



Latency

In certain environments, an on prem cloud keeps the infrastructure close to the users, security teams can provide faster response times and improved performance.

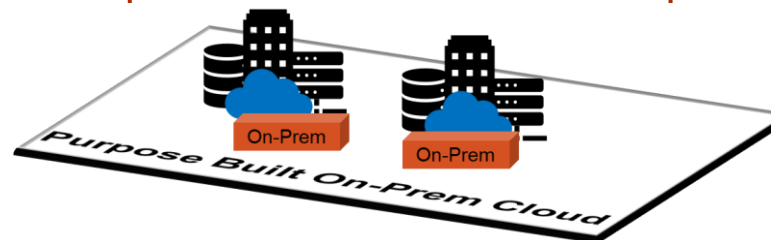


Customization and Flexibility

Tailor IAM to specific needs to meet requirements and seamless integration with existing infrastructure, apps, and workflow.

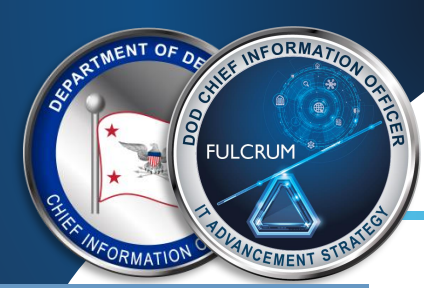
Integration with Legacy Systems

On-prem IAM approaches can enable integrations with existing complex legacy applications and systems.



Centralized Control

On-Prem cloud the organization has complete control of the IAM system, allowing customization and flexibility.



EDR Use Cases

- EDR Implementation – COA 1
- EDR Implementation – COA 2
- EDR Implementation – COA 3

EDR Implementation Example (COA 1)

Disruption and Downtime

EDR in place may require manual maintenance, updates, and monitoring potentially leading to more servers, upgrading software, and training staff increasing possible downtime.

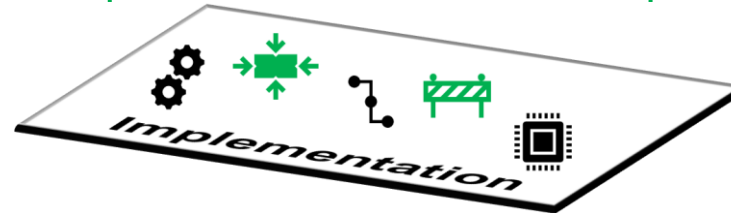


Legacy Systems Limitations

Limitations with modern security capabilities such as threat intel, UEBA, SOAR, automation, can hinder the overall effectiveness and efficiency of an EDR.

Integration Challenges

If an environment has been using a variety of legacy systems (On-Prem, Multiple OS, and custom-built apps) they have built a significant amount of tech debt over time.



Scalability Concerns

Deploying and managing EDR agents on each endpoint across the network or setting up on EDR server can present challenges as the environment evolves.



Cost and Resource Allocation

Implementing an EDR solution in an environment with multiple legacy systems, on-prem servers, and endpoints may necessitate hardware upgrades, software installations, and configuration changes. This could involve purchasing new servers, upgrading existing ones, and managing the infrastructure through tasks like patching, monitoring, and troubleshooting.

EDR Implementation Example (COA 2)

Enhanced Visibility and Coverage

Cloud-based EDR solutions offer broader visibility and coverage than on-premises systems, allowing for better threat detection and faster incident response across all endpoints, regardless of location or environment.

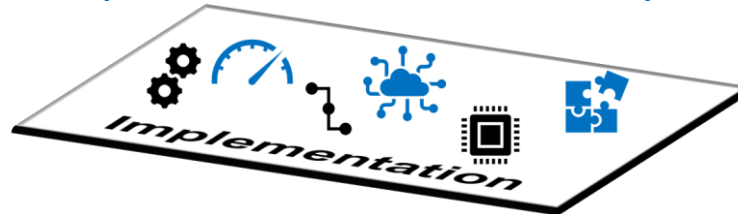


Advanced Analytics and AI Capabilities

Analyze data in real-time, detect anomalies, and identify threats more effectively using cloud resources and AI-driven analytics.

Rapid Deployment

Components can quickly implement and secure endpoints using pre-configured templates, automated provisioning, and streamlined deployment processes.



Scalable and Flexible

Cloud-based EDR solutions can dynamically scale resources and handle large data volumes for optimal performance.

Reduced Infrastructure and Maintenance Costs

Cloud-based EDR solutions minimize upfront hardware and software costs and ongoing maintenance expenses. Scale resources as needed, optimizing costs through a pay-as-you-go model of cloud services.



Continuous Updates and Maintenance

Cloud-based EDR solutions receive regular updates, patches, and new features automatically, ensuring up-to-date protection against emerging threats.

EDR Implementation Example (COA 3)

Compliance and Regulatory Requirements

Environments may require hosting and protecting data within their own premises and infrastructure.

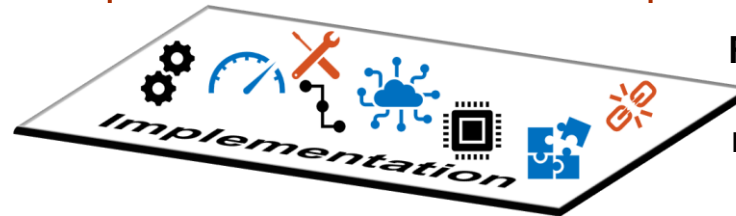


Control and Security

Full control over infrastructure and security, allowing for customization and tailored security policies.

Customization and Integration

Flexibility for customization and integration with existing infrastructure.

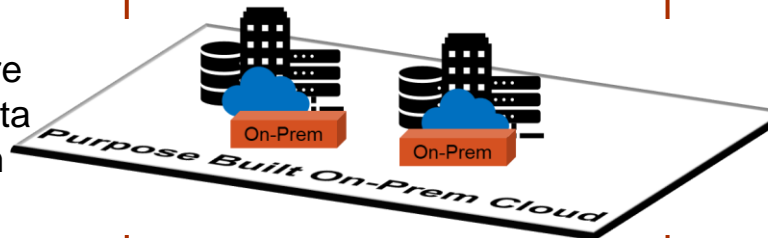


Reduced Dependency on Third Party Providers

Minimizes the potential risks associated with relying on solely on third party providers for critical security functions.

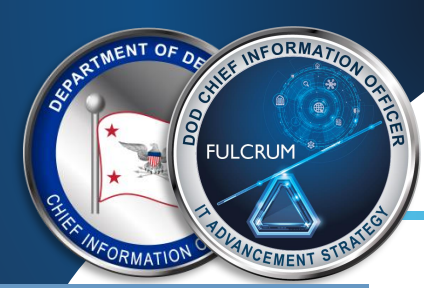
Lower Latency and Local Data Processing

Real time threat detection and response, where minimizing latency is crucial. By keeping the data and processing closer to the network-on prem may provide a faster response and better performance.



Cost Considerations

Potentially avoid ongoing subscription fees associated with commercial clouds and have more predictable cost structures.



SIEM Use Cases

- SIEM Implementation – COA 1
- SIEM Implementation – COA 2
- SIEM Implementation – COA 3

SIEM Implementation Example (COA 1)

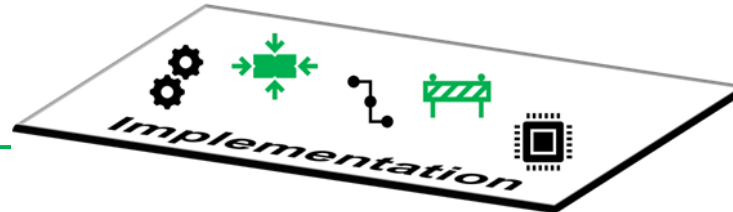
Limited Incident Response Capabilities

Implementing a SIEM to Legacy systems may lack the necessary integration and automation capabilities to support efficient incident response processes.



Limited Log Aggregation

Legacy systems may generate logs in different formats or lack standardized logging practices.



Integration with Security Tools

Legacy systems may not integrate seamlessly with modern security tools and technologies. This can hinder the effectiveness of a SIEM solution, as it may not be able to gather comprehensive security event data from all relevant systems and applications.

Scalability & Performance

Legacy systems may have limited processing power or storage capacity, which can impact the scalability and performance.



Integration with Legacy Systems

Legacy systems may not have the necessary log sources or event collection capabilities required for effective SIEM implementation. May also require custom APIs, connectors, or log forwarding.

SIEM Implementation Example (COA 2)

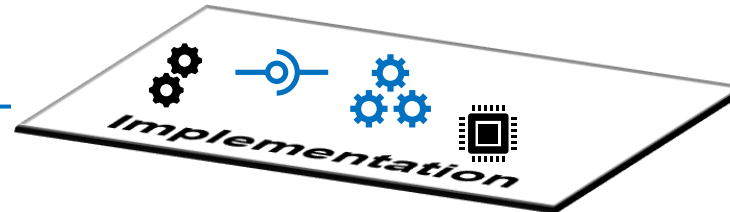
Simplified management and maintenance

User-friendly interfaces and management tools that simplify the provisioning, configuration, and management of the SIEM infrastructure.



Enhanced performance

Cloud environments provide high-performance infrastructure with robust computing power and storage capabilities.



Built In Capabilities

Cloud environments often have built-in integration capabilities with various services and applications. This makes it easier to integrate the SIEM solution with other security tools, log sources, and cloud-based services.

Scalability

Offer virtually unlimited scalability for their SIEM infrastructure. Scalability ensures that the SIEM solution can handle large volumes of logs and events from various sources without performance degradation.



Cost Effectiveness

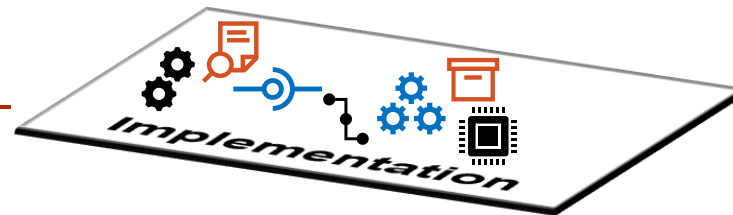
Follow a pay-as-you-go model, eliminating the need for upfront hardware and infrastructure investments.

SIEM Implementation Example (COA 3)



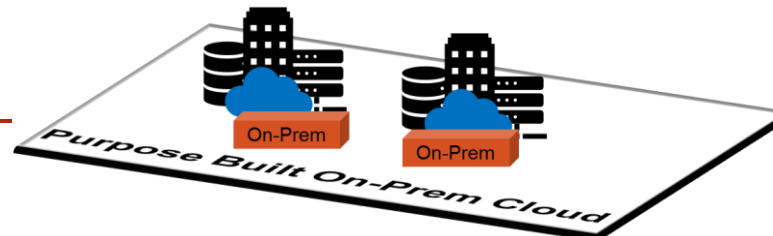
Complete Visibility

On-prem SIEM solutions can provide stringent security measures and have complete visibility over infrastructure.



Strict Data Controls

On-prem SIEM allows the choice for specific storage infrastructure, such as dedicated servers or can implement longer retention/storing without relying on third-party cloud.



Low Dependency On Connectivity

On-prem SIEM solutions operate within the network infrastructure, ensuring continuous monitoring and analysis of security events, even during internet outages or disruptions.

Summary: Hybrid Approach

Most Components will leverage a Hybrid COA approach based on their unique environments

Data Privacy & Compliance

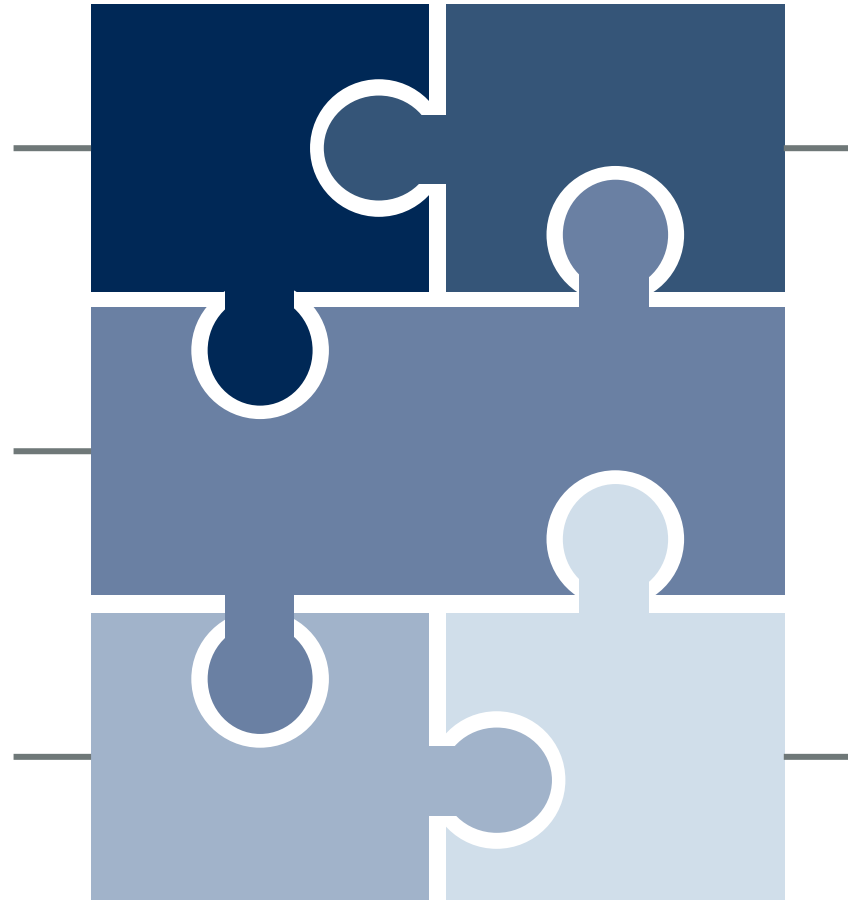
Sensitive data can be stored and processed on-prem or in a private cloud, while non-sensitive data or compute intensive tasks can be offloaded to a commercial cloud for scale and efficiency.

Scaling/Bursting

On-Prem (COA 3) can be used normally, and if dealing with a spike or sudden increase in endpoints, commercial cloud (COA 2) can be leveraged.

Geographical Distribution

On-Prem and Private Cloud approaches can be deployed locally for low latency detection, with data collected from all locations and centralized to a commercial cloud for analysis/reporting.

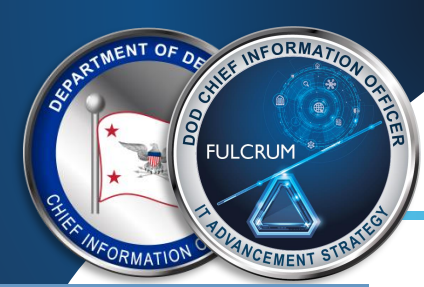


Legacy

Legacy systems may be critical in environments. Additional security can be implemented to protect, without completely replacing legacy. Data can possibly be analyzed and proceeded in cloud.

Cost Optimization

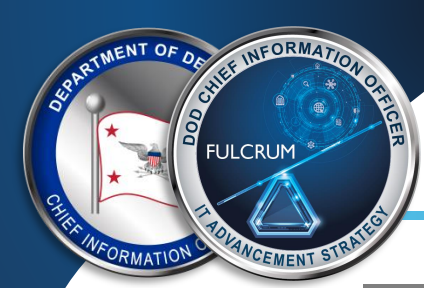
A hybrid approach may optimize costs by leveraging both on-prem and commercial cloud environments.



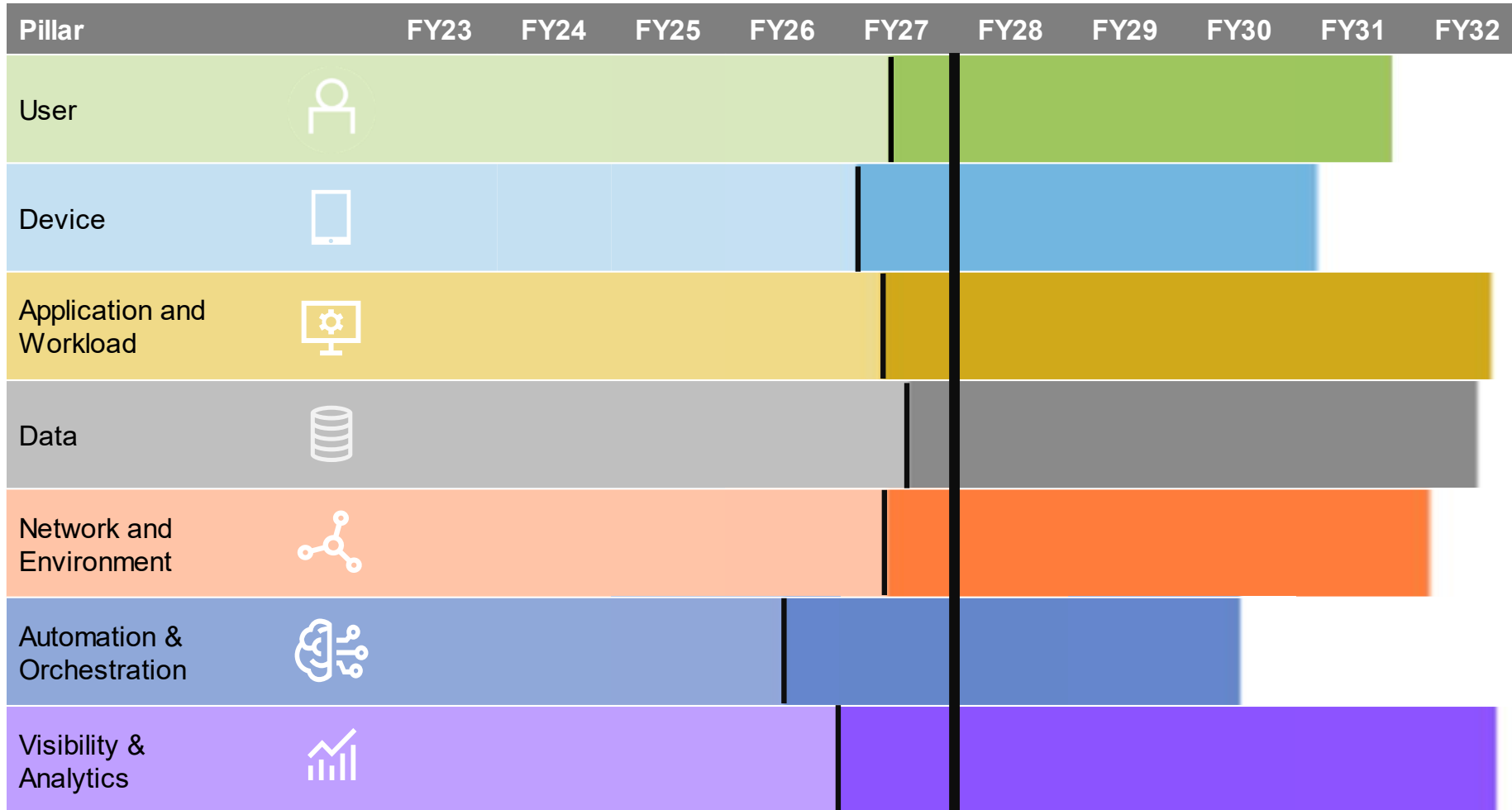
Appendix A: COA 1 Timeline Details (Uplifting Legacy)

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 prescribed 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



COA 1 (DoD Baseline) Timeline Estimates



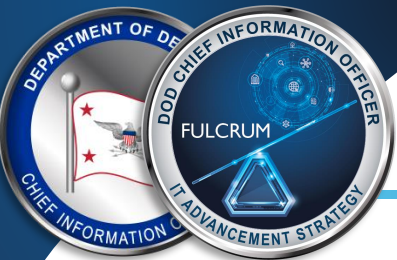
V1.0 as of 10/04/2022



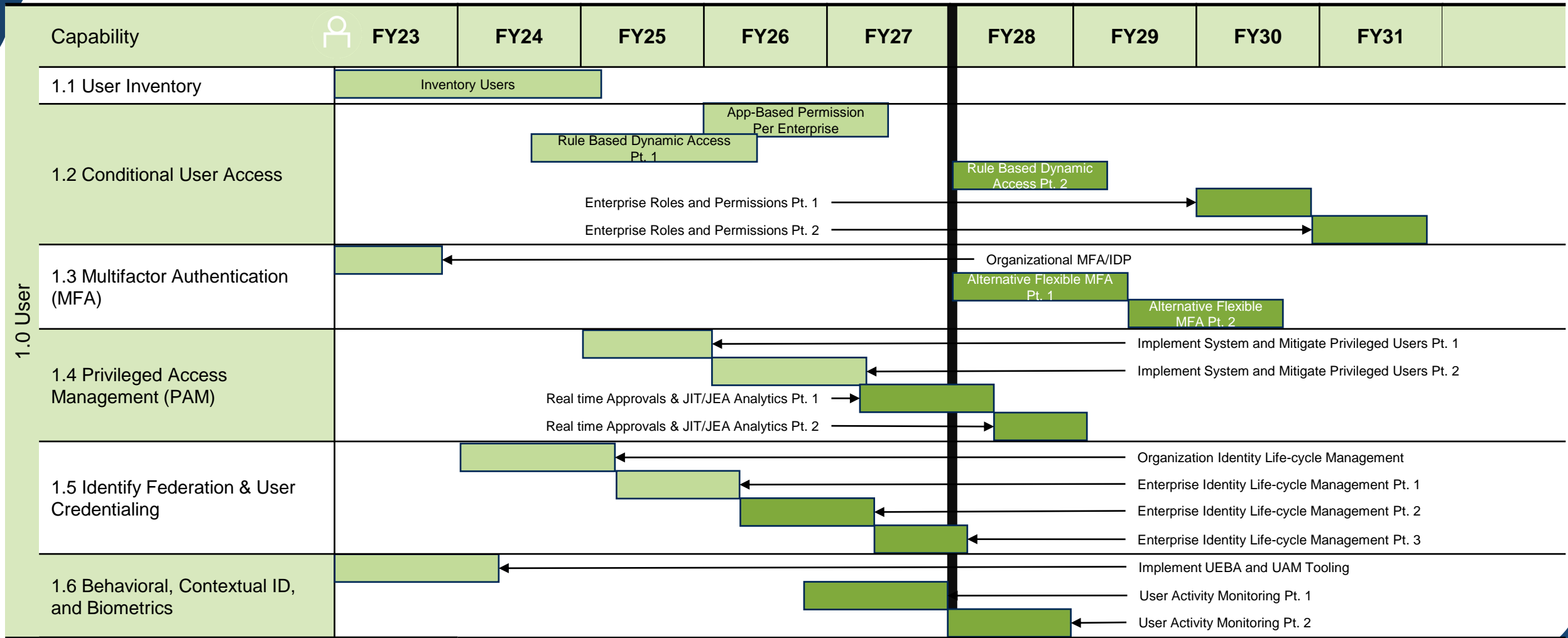
= Target Level ZT



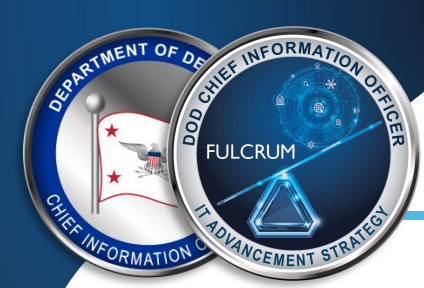
= Advanced ZT



User (1 of 2) – COA 1



Light Green = Target Level ZT Dark Green = Advanced ZT

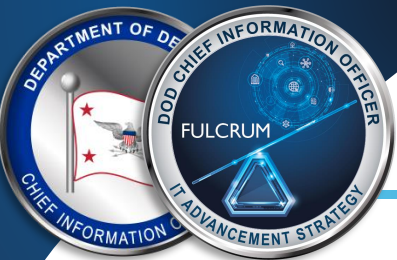


User (2 of 2) – COA 1

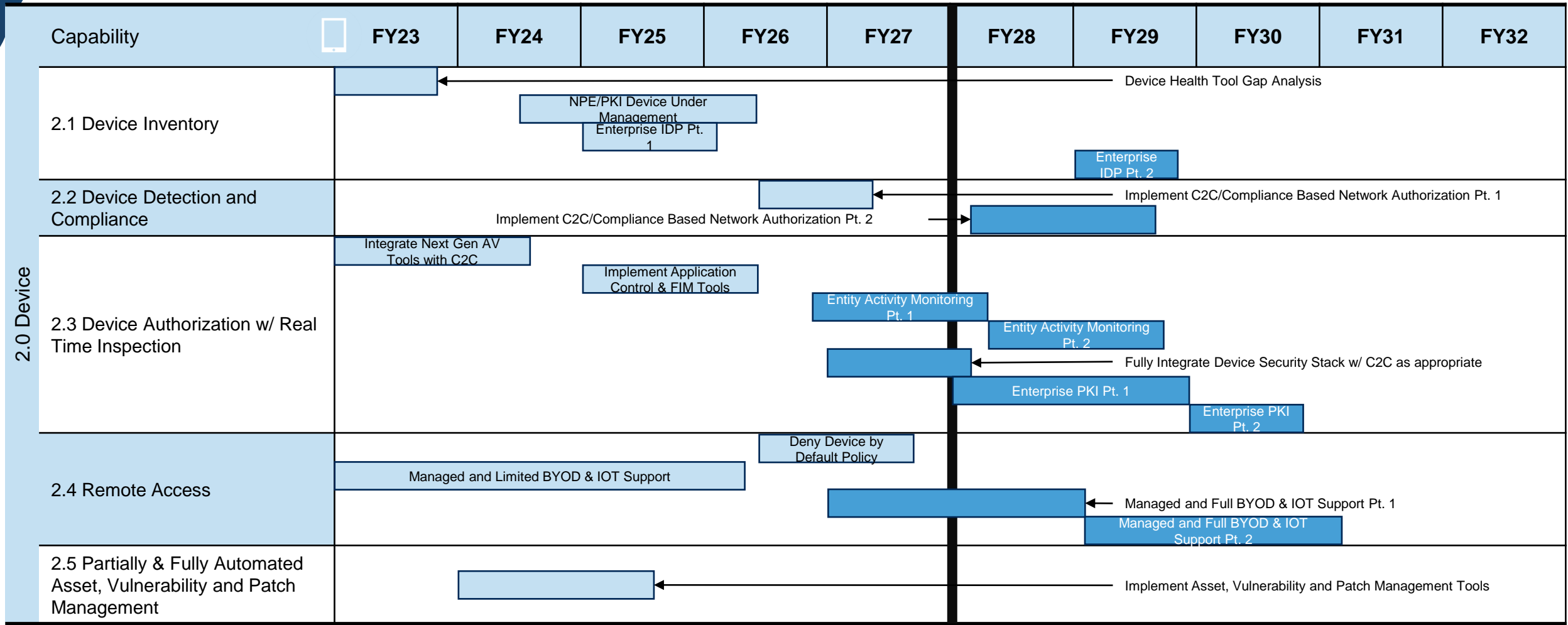
Capability		FY23	FY24	FY25	FY26	FY27	FY28	FY29	FY30	FY31	FY32
1.0 User	1.7 Least Privileged Access		Deny User by Default Policy								
	1.8 Continuous Authentication		Single Authentication		Periodic Authentication			Continuous Authentication Pt. 1		Continuous Authentication Pt. 2	
	1.9 Integrated ICAM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

Light Green = Target Level ZT

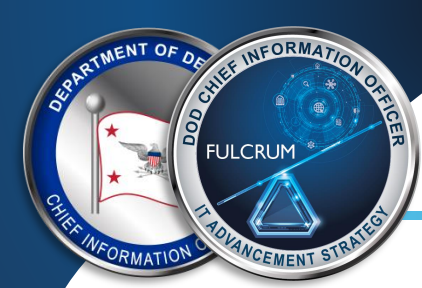
Dark Green = Advanced ZT



Device (1 of 2) – COA 1



Light Blue = Target Level ZT Dark Blue = Advanced ZT



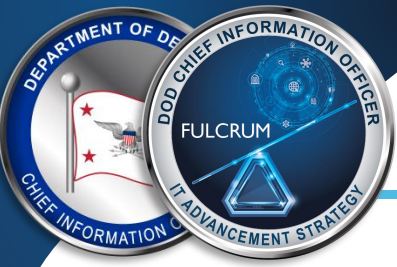
Device (2 of 2) – COA 1

Capability	FY23	FY24	FY25	FY26	FY27	FY28	FY29	FY30	FY31	FY32
2.6 Unified Endpoint Management (UEM) & Mobile Device Management (MDM)										
2.7 Endpoint & Extended Detection & Response (EDR & XDR)										

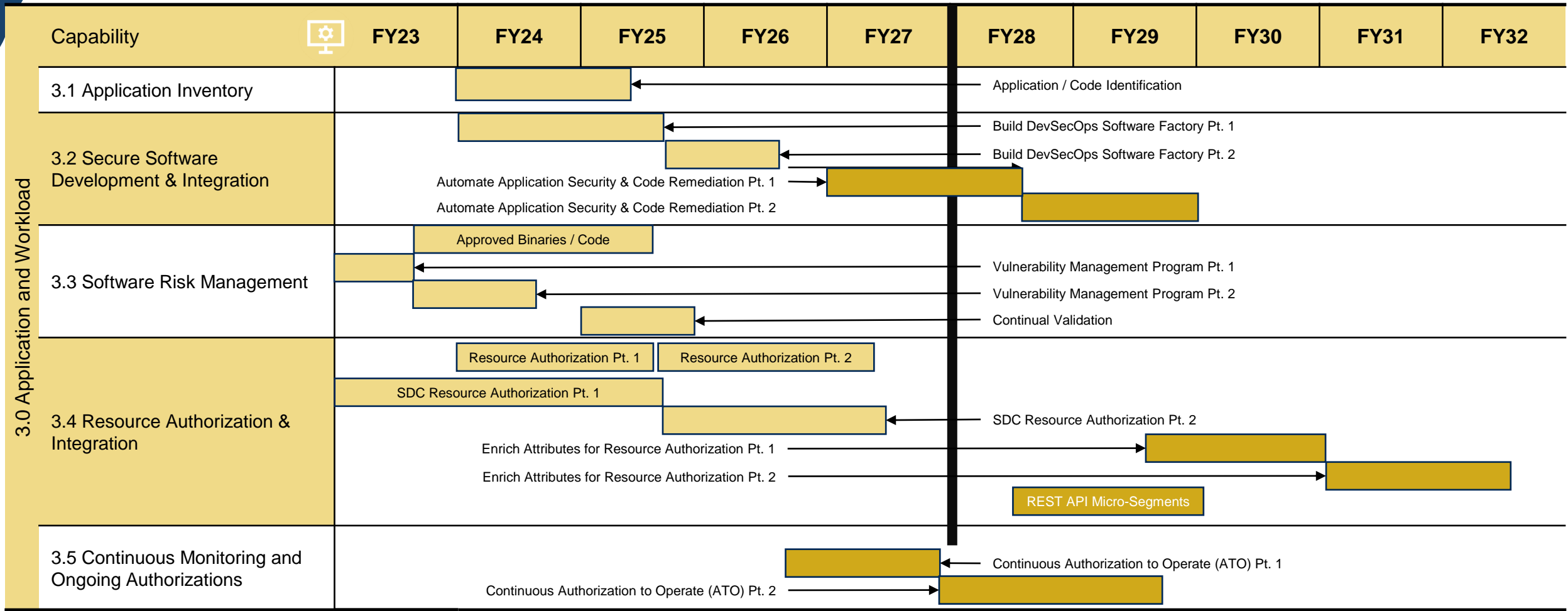
2.0 Device

- Implement UEDM or equivalent Tools
- Enterprise Device Management Pt. 1
- Enterprise Device Management Pt. 2
- Implement Endpoint Detection & Response (EDR) Tools & Integrate w / C2C
- Implement Extended Detection & Response (XDR) & Integrate w / C2C Pt. 1
- Implement Extended Detection & Response (XDR) & Integrate w / C2C Pt. 2

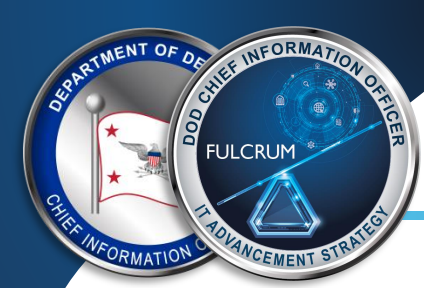
= Target Level ZT
 = Advanced ZT



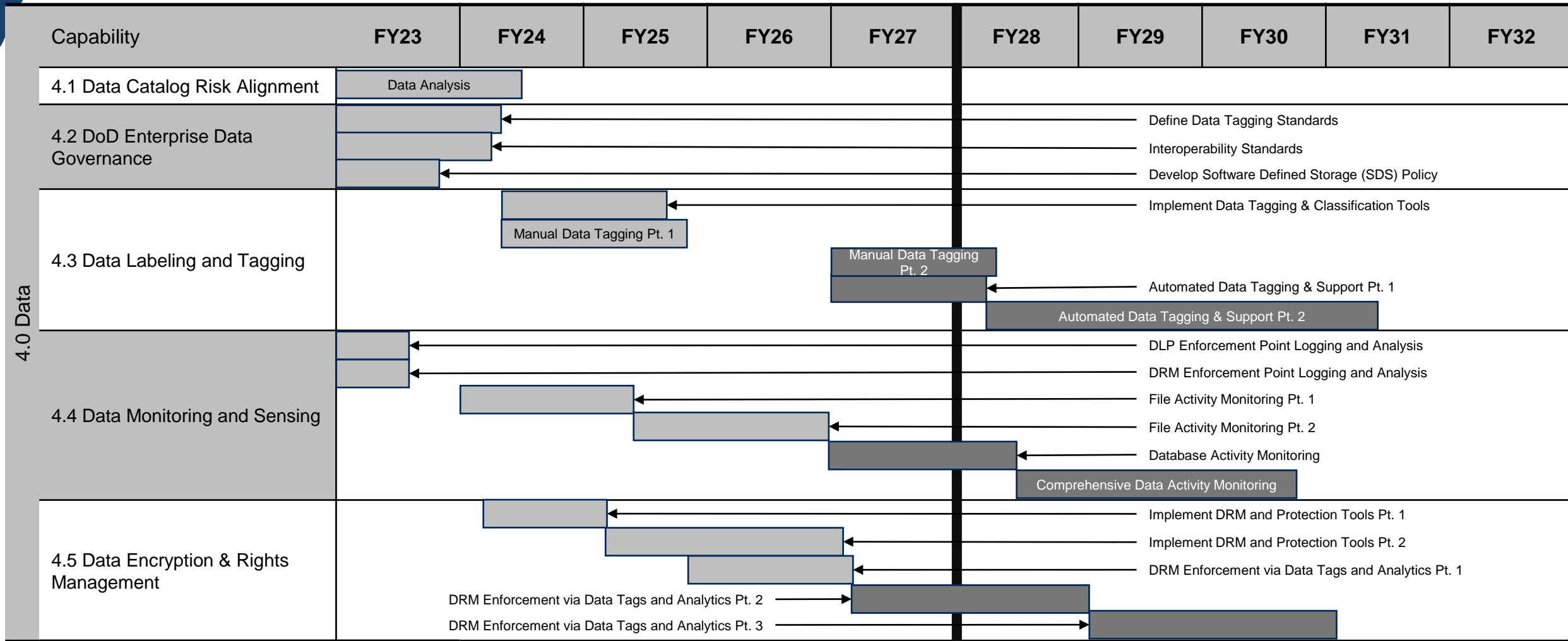
Application and Workload – COA 1



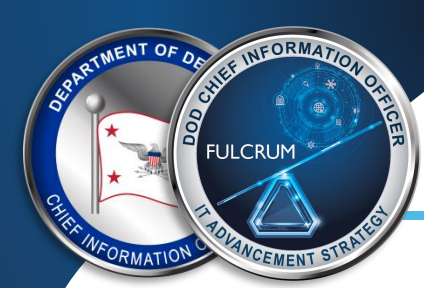
Light Yellow = Target Level ZT Dark Yellow = Advanced ZT



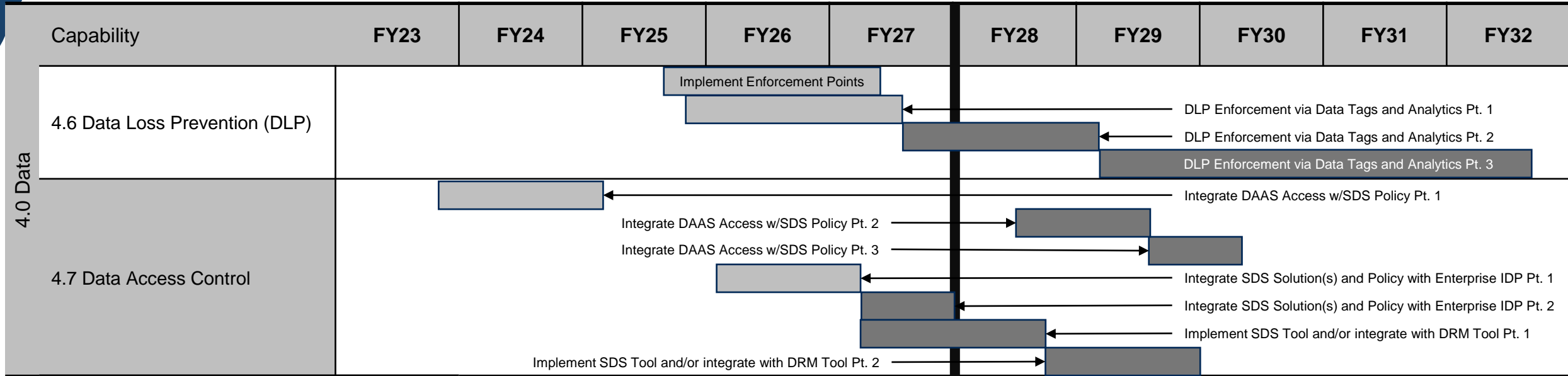
Data (1 of 2) – COA 1



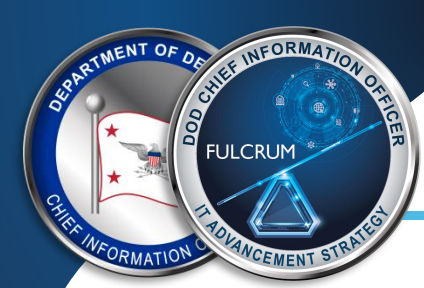
= Target Level ZT
 = Advanced ZT



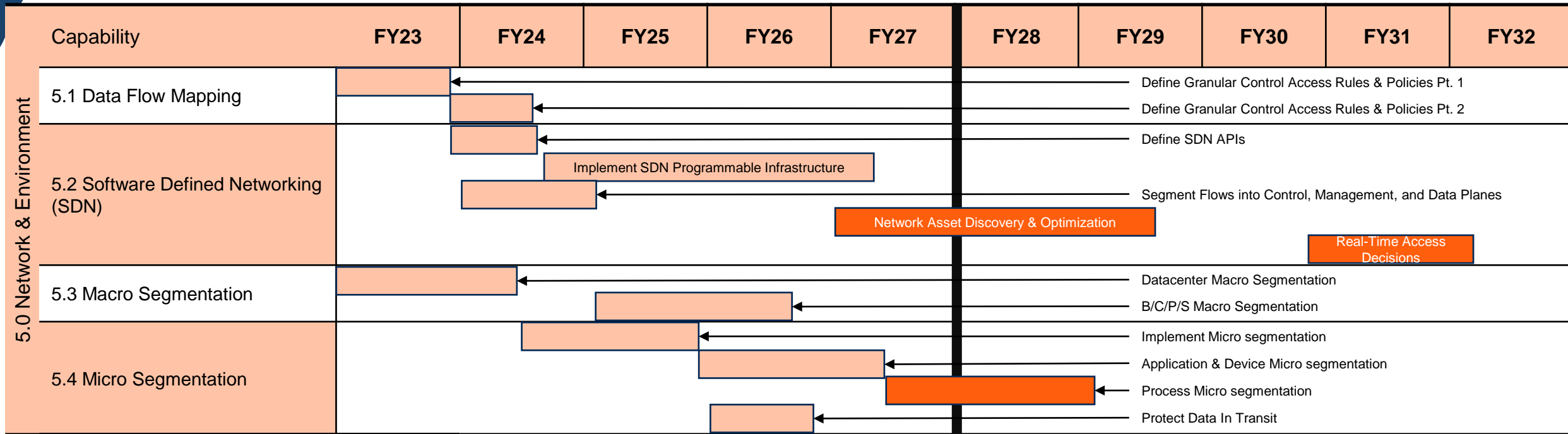
Data (2 of 2) – COA 1



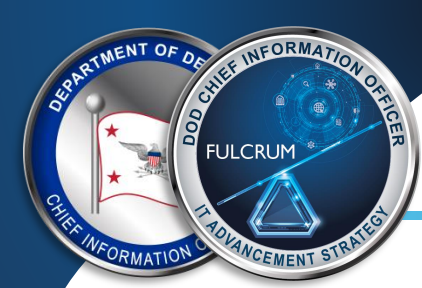
= Target Level ZT
 = Advanced ZT



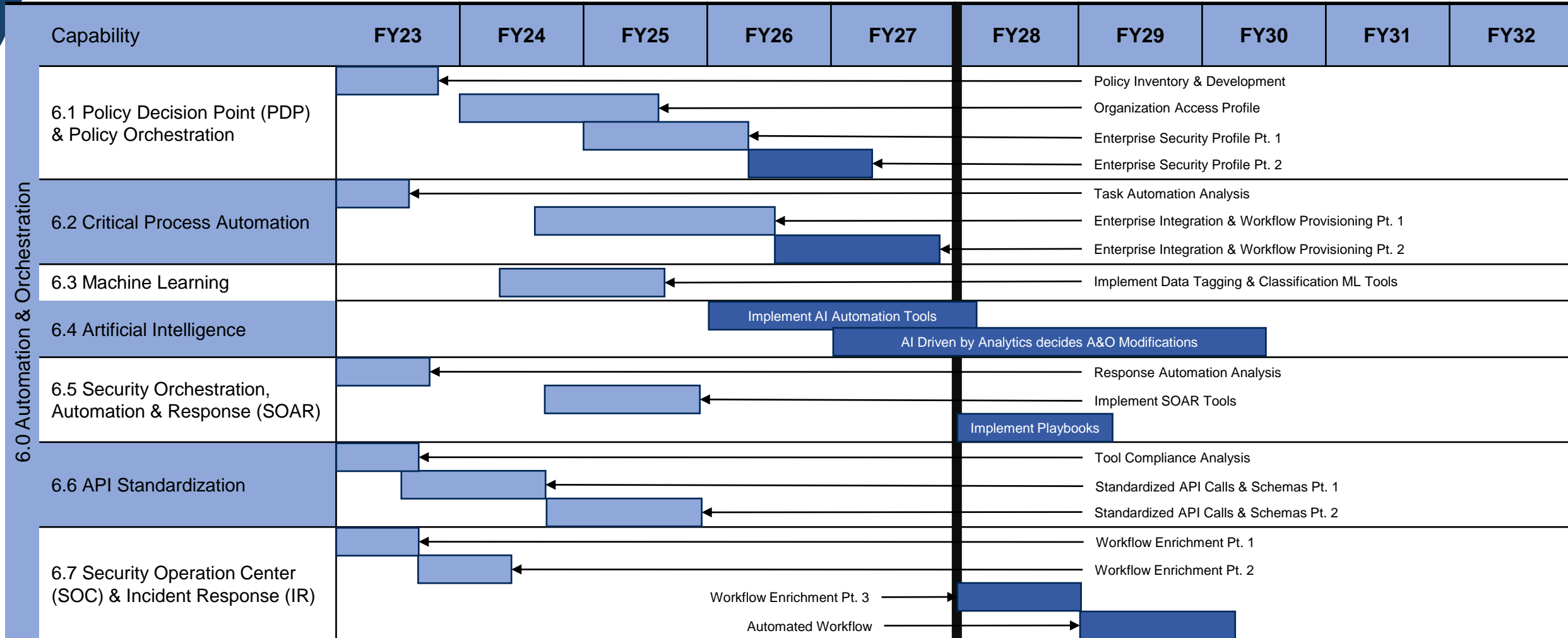
Network and Environment – COA 1



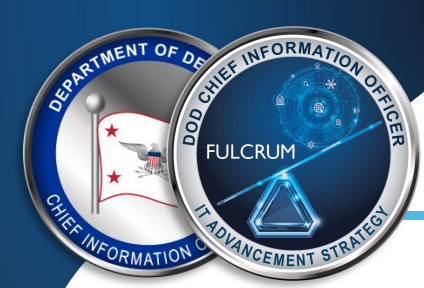
= Target Level ZT
 = Advanced ZT



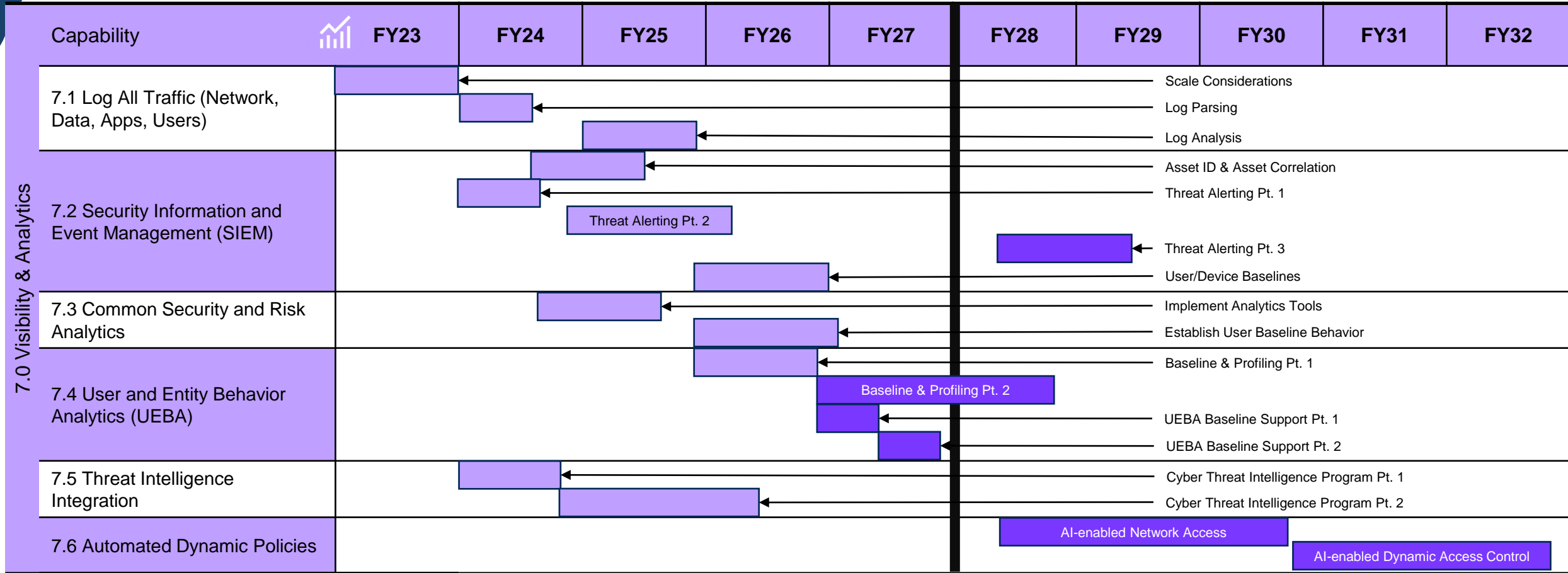
Automation & Orchestration – COA 1



= Target Level ZT
 = Advanced ZT



Visibility & Analytics – COA 1



= Target Level ZT
 = Advanced ZT



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"



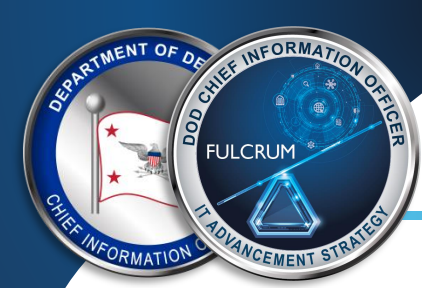
Appendix B: Capability Definitions

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						

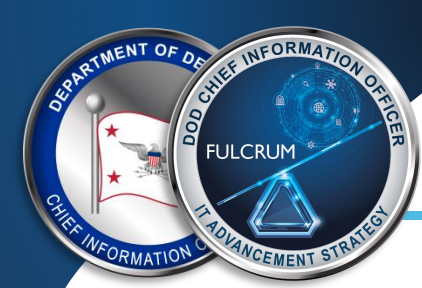
EXECUTION ENABLERS

- Doctrine
- Organization
- Training
- Material
- Leadership & Education
- Personnel
- Facilities
- Policy



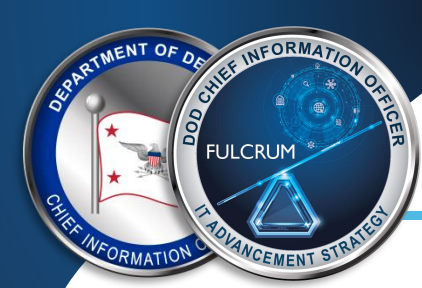
Capability Definitions

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



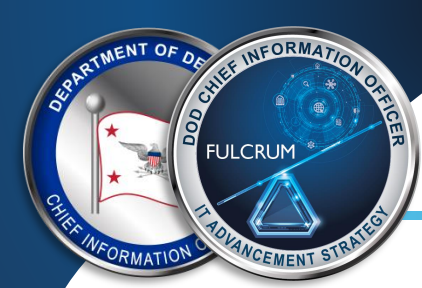
Capability Definitions

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.	<ul style="list-style-type: none"> * 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	<ul style="list-style-type: none"> * 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	<ul style="list-style-type: none"> * 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	<ul style="list-style-type: none"> * Single Authentication * Periodic Authentication * Continuous Authentication Pt1 * Continuous Authentication Pt2



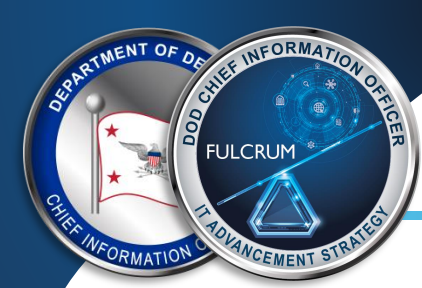
Capability Definitions

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	<ul style="list-style-type: none"> * 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	<ul style="list-style-type: none"> * 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	<ul style="list-style-type: none"> * Implement C2C/Compliance Based Network Authorization Pt1 * Implement C2C/Compliance Based Network Authorization Pt2



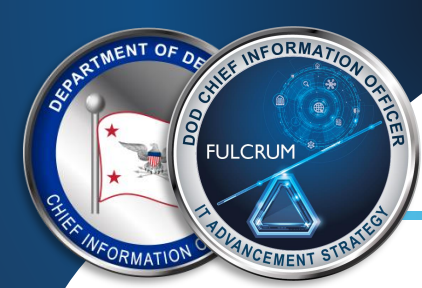
Capability Definitions

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	<ul style="list-style-type: none"> * 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	<ul style="list-style-type: none"> * 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	<ul style="list-style-type: none"> * 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	<ul style="list-style-type: none"> * Implement UEDM or equivalent Tools * Enterprise Device Management Pt1 * Enterprise Device Management Pt2



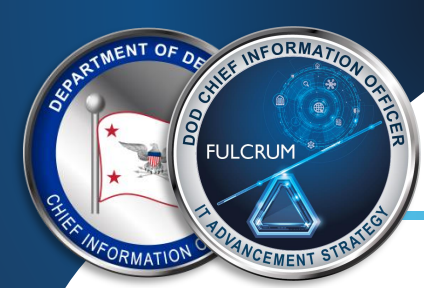
Capability Definitions

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)	<ul style="list-style-type: none"> * 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	<ul style="list-style-type: none"> * 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	<ul style="list-style-type: none"> * 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	<ul style="list-style-type: none"> * Approved Binaries/Code * Vulnerability Management Program Pt1 * Vulnerability Management Program Pt2 * Continual Validation



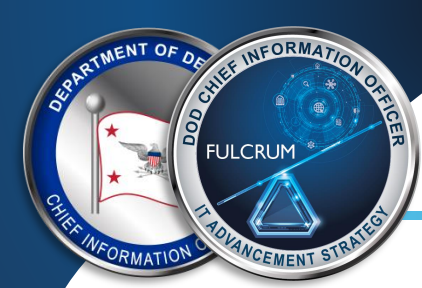
Capability Definitions

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 improve the ability to remove access when it is not needed.	<ul style="list-style-type: none"> * 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	<ul style="list-style-type: none"> * 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	<ul style="list-style-type: none"> * 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	<ul style="list-style-type: none"> * 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	<ul style="list-style-type: none"> * Implement Data Tagging & Classification Tools * Manual Data Tagging Pt1 * Manual Data Tagging Pt2 * Automated Data Tagging & Support Pt1 * Automated Data Tagging & Support Pt2



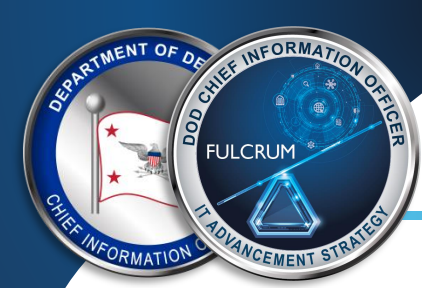
Capability Definitions

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	<ul style="list-style-type: none"> * 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	<ul style="list-style-type: none"> * 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	<ul style="list-style-type: none"> * 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 management 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	<ul style="list-style-type: none"> * 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



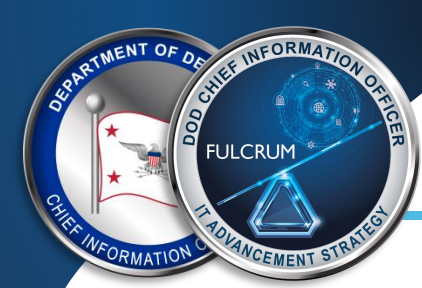
Capability Definitions

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	<ul style="list-style-type: none"> * 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	<ul style="list-style-type: none"> * Define SDN APIs* Implement SDN Programmable 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	<ul style="list-style-type: none"> * 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	<ul style="list-style-type: none"> * Implement Micro segmentation * Application & Device Micro segmentation * Process Micro segmentation * Protect Data In Transit



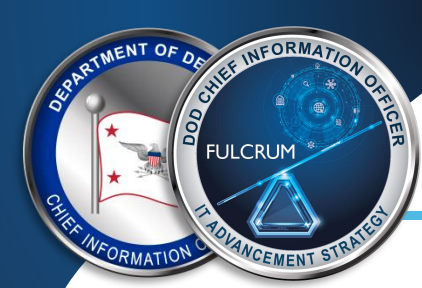
Capability Definitions

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	<ul style="list-style-type: none"> * 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	<ul style="list-style-type: none"> * 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	<ul style="list-style-type: none"> * 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	<ul style="list-style-type: none"> * Implement AI automation tools * AI Driven by Analytics decides A&O modifications



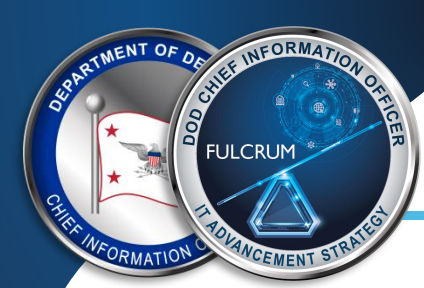
Capability Definitions

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	<ul style="list-style-type: none"> * 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	<ul style="list-style-type: none"> * 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	<ul style="list-style-type: none"> * 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	<ul style="list-style-type: none"> * Scale Considerations * Log Parsing * Log Analysis



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	<ul style="list-style-type: none"> * 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	<ul style="list-style-type: none"> * 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	<ul style="list-style-type: none"> * 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	<ul style="list-style-type: none"> * Cyber Threat Intelligence Program Pt1 * Cyber Threat Intelligence Program Pt2



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	<ul style="list-style-type: none"> * AI-enabled Network Access * AI-enabled Dynamic Access Control