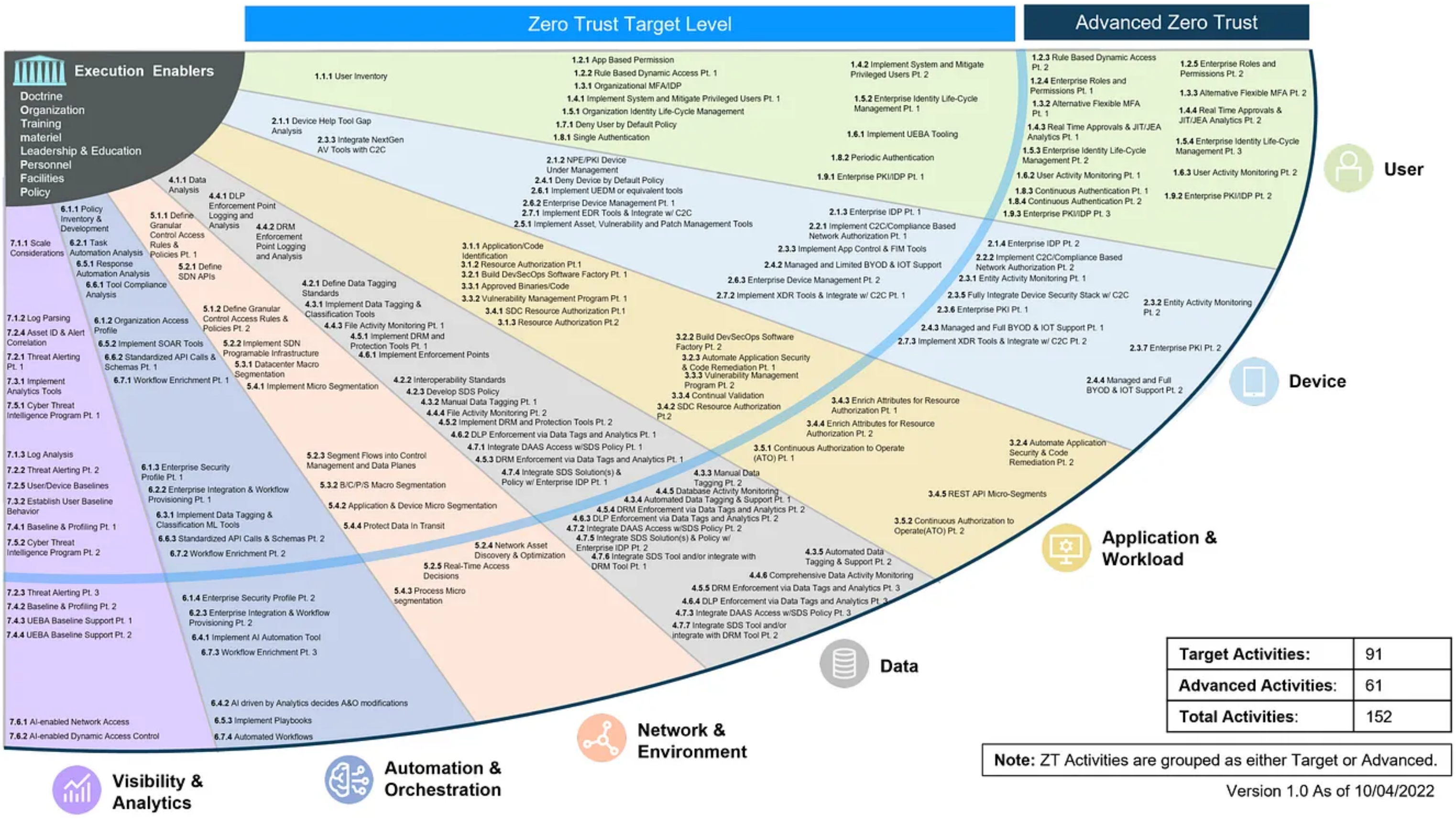
xage GOVERNMENT

Xage Support for DoD Zero Trust Roadmap

The U.S. Department of Defense (DoD) has committed to adopting a zero-trust cybersecurity framework by the end of fiscal year 2027. The roadmap for achieving this contains 152 activities, divided across seven pillars. 91 of the activities are considered "Target Level" which forms the baseline requirements that must be achieved by September 30, 2027. The other 61 are considered Advanced Zero Trust activities. The seven pillars and 152 activities are represented in the fan chart below.

Xage Security provides zero trust access, privileged access management, and zero trust data exchange products and services which fulfill many of the target level and advanced requirements of the DOD Zero Trust Roadmap. This document describes in detail how Xage delivers the requirements either as a standalone offering, or by integration with other solutions, to support the DoD and its contractors in rapidly achieving their zero trust requirements.


Zero Trust Target Level
Advanced Zero Trust
Execution Enablers
Doctrine
Organization
Training
materiel
Leadership & Education
Personnel
Facilities
Policy
1.1.1 User Inventory
1.2.1 App Based Permission
1.2.2 Rule Based Dynamic Access Pt. 1
1.3.1 Organizational MFA/IDP
1.4.1 Implement System and Mitigate Privileged Users Pt. 1
1.5.1 Organization Identity Life-Cycle Management
1.7.1 Deny User by Default Policy
1.8.1 Single Authentication
1.4.2 Implement System and Mitigate Privileged Users Pt. 2
1.5.2 Enterprise Identity Life-Cycle Management Pt. 1
1.6.1 Implement UEBA Tooling
1.8.2 Periodic Authentication
1.9.1 Enterprise PKI/IDP Pt. 1
1.2.3 Rule Based Dynamic Access Pt. 2
1.2.4 Enterprise Roles and Permissions Pt. 1
1.3.2 Alternative Flexible MFA Pt. 1
1.4.3 Real Time Approvals & JIT/JEA Analytics Pt. 1
1.5.3 Enterprise Identity Life-Cycle Management Pt. 2
1.6.2 User Activity Monitoring Pt. 1
1.8.3 Continuous Authentication Pt. 1
1.8.4 Continuous Authentication Pt. 2
1.9.3 Enterprise PKI/IDP Pt. 3
1.2.5 Enterprise Roles and Permissions Pt. 2
1.3.3 Alternative Flexible MFA Pt. 2
1.4.4 Real Time Approvals & JIT/JEA Analytics Pt. 2
1.5.4 Enterprise Identity Life-Cycle Management Pt. 3
1.6.3 User Activity Monitoring Pt. 2
1.9.2 Enterprise PKI/IDP Pt. 2
User
2.1.1 Device Help Tool Gap Analysis
2.3.3 Integrate NextGen AV Tools with C2C
2.1.2 NPE/PKI Device Under Management
2.4.1 Deny Device by Default Policy
2.6.1 Implement UEDM or equivalent tools
2.6.2 Enterprise Device Management Pt. 1
2.7.1 Implement EDR Tools & Integrate w/ C2C
2.5.1 Implement Asset, Vulnerability and Patch Management Tools
2.1.3 Enterprise IDP Pt. 1
2.2.1 Implement C2C/Compliance Based Network Authorization Pt. 1
2.3.3 Implement App Control & FIM Tools
2.4.2 Managed and Limited BYOD & IOT Support
2.6.3 Enterprise Device Management Pt. 2
2.7.2 Implement XDR Tools & Integrate w/ C2C Pt. 1
2.1.4 Enterprise IDP Pt. 2
2.2.2 Implement C2C/Compliance Based Network Authorization Pt. 2
2.3.1 Entity Activity Monitoring Pt. 1
2.3.5 Fully Integrate Device Security Stack w/ C2C
2.3.6 Enterprise PKI Pt. 1
2.4.3 Managed and Full BYOD & IOT Support Pt. 1
2.7.3 Implement XDR Tools & Integrate w/ C2C Pt. 2
2.3.2 Entity Activity Monitoring Pt. 2
2.3.7 Enterprise PKI Pt. 2
2.4.4 Managed and Full BYOD & IOT Support Pt. 2
Device
3.1.1 Application/Code Identification
3.1.2 Resource Authorization Pt.1
3.2.1 Build DevSecOps Software Factory Pt. 1
3.3.1 Approved Binaries/Code
3.3.2 Vulnerability Management Program Pt. 1
3.4.1 SDC Resource Authorization Pt.1
3.1.3 Resource Authorization Pt.2
3.2.2 Build DevSecOps Software Factory Pt. 2
3.2.3 Automate Application Security & Code Remediation Pt. 1
3.3.3 Vulnerability Management Program Pt. 2
3.3.4 Continual Validation
3.4.2 SDC Resource Authorization Pt.2
3.4.3 Enrich Attributes for Resource Authorization Pt. 1
3.4.4 Enrich Attributes for Resource Authorization Pt. 2
3.5.1 Continuous Authorization to Operate (ATO) Pt. 1
3.2.4 Automate Application Security & Code Remediation Pt. 2
3.4.5 REST API Micro-Segments
3.5.2 Continuous Authorization to Operate(ATO) Pt. 2
Application & Workload
4.1.1 Data Analysis
4.4.1 DLP Enforcement Point Logging and Analysis
4.4.2 DRM Enforcement Point Logging and Analysis
4.2.1 Define Data Tagging Standards
4.3.1 Implement Data Tagging & Classification Tools
4.4.3 File Activity Monitoring Pt. 1
4.5.1 Implement DRM and Protection Tools Pt. 1
4.6.1 Implement Enforcement Points
4.2.2 Interoperability Standards
4.2.3 Develop SDS Policy
4.3.2 Manual Data Tagging Pt. 1
4.4.4 File Activity Monitoring Pt. 2
4.5.2 Implement DRM and Protection Tools Pt. 2
4.6.2 DLP Enforcement via Data Tags and Analytics Pt. 1
4.7.1 Integrate DAAS Access w/SDS Policy Pt. 1
4.5.3 DRM Enforcement via Data Tags and Analytics Pt. 1
4.7.4 Integrate SDS Solution(s) & Policy w/ Enterprise IDP Pt. 1
4.3.3 Manual Data Tagging Pt. 2
4.4.5 Database Activity Monitoring
4.3.4 Automated Data Tagging & Support Pt. 1
4.5.4 DRM Enforcement via Data Tags and Analytics Pt. 2
4.6.3 DLP Enforcement via Data Tags and Analytics Pt. 2
4.7.2 Integrate DAAS Access w/SDS Policy Pt. 2
4.7.5 Integrate SDS Solution(s) & Policy w/ Enterprise IDP Pt. 2
4.7.6 Integrate SDS Tool and/or integrate with DRM Tool Pt. 1
4.3.5 Automated Data Tagging & Support Pt. 2
4.4.6 Comprehensive Data Activity Monitoring
4.5.5 DRM Enforcement via Data Tags and Analytics Pt. 3
4.6.4 DLP Enforcement via Data Tags and Analytics Pt. 3
4.7.3 Integrate DAAS Access w/SDS Policy Pt. 3
4.7.7 Integrate SDS Tool and/or integrate with DRM Tool Pt. 2
Data
5.1.1 Define Granular Control Access Rules & Policies Pt. 1
5.2.1 Define SDN APIs
5.1.2 Define Granular Control Access Rules & Policies Pt. 2
5.2.2 Implement SDN Programable Infrastructure
5.3.1 Datacenter Macro Segmentation
5.4.1 Implement Micro Segmentation
5.2.3 Segment Flows into Control Management and Data Planes
5.3.2 B/C/P/S Macro Segmentation
5.4.2 Application & Device Micro Segmentation
5.4.4 Protect Data In Transit
5.2.4 Network Asset Discovery & Optimization
5.2.5 Real-Time Access Decisions
5.4.3 Process Micro segmentation
Network & Environment
6.1.1 Policy Inventory & Development
6.2.1 Task Automation Analysis
6.5.1 Response Automation Analysis
6.6.1 Tool Compliance Analysis
6.1.2 Organization Access Profile
6.5.2 Implement SOAR Tools
6.6.2 Standardized API Calls & Schemas Pt. 1
6.7.1 Workflow Enrichment Pt. 1
6.1.3 Enterprise Security Profile Pt. 1
6.2.2 Enterprise Integration & Workflow Provisioning Pt. 1
6.3.1 Implement Data Tagging & Classification ML Tools
6.6.3 Standardized API Calls & Schemas Pt. 2
6.7.2 Workflow Enrichment Pt. 2
6.1.4 Enterprise Security Profile Pt. 2
6.2.3 Enterprise Integration & Workflow Provisioning Pt. 2
6.4.1 Implement AI Automation Tool
6.7.3 Workflow Enrichment Pt. 3
6.4.2 AI driven by Analytics decides A&O modifications
6.5.3 Implement Playbooks
6.7.4 Automated Workflows
Automation & Orchestration
7.1.1 Scale Considerations
7.1.2 Log Parsing
7.2.4 Asset ID & Alert Correlation
7.2.1 Threat Alerting Pt. 1
7.3.1 Implement Analytics Tools
7.5.1 Cyber Threat Intelligence Program Pt. 1
7.1.3 Log Analysis
7.2.2 Threat Alerting Pt. 2
7.2.5 User/Device Baselines
7.3.2 Establish User Baseline Behavior
7.4.1 Baseline & Profiling Pt. 1
7.5.2 Cyber Threat Intelligence Program Pt. 2
7.2.3 Threat Alerting Pt. 3
7.4.2 Baseline & Profiling Pt. 2
7.4.3 UEBA Baseline Support Pt. 1
7.4.4 UEBA Baseline Support Pt. 2
7.6.1 AI-enabled Network Access
7.6.2 AI-enabled Dynamic Access Control
Visibility & Analytics

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

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

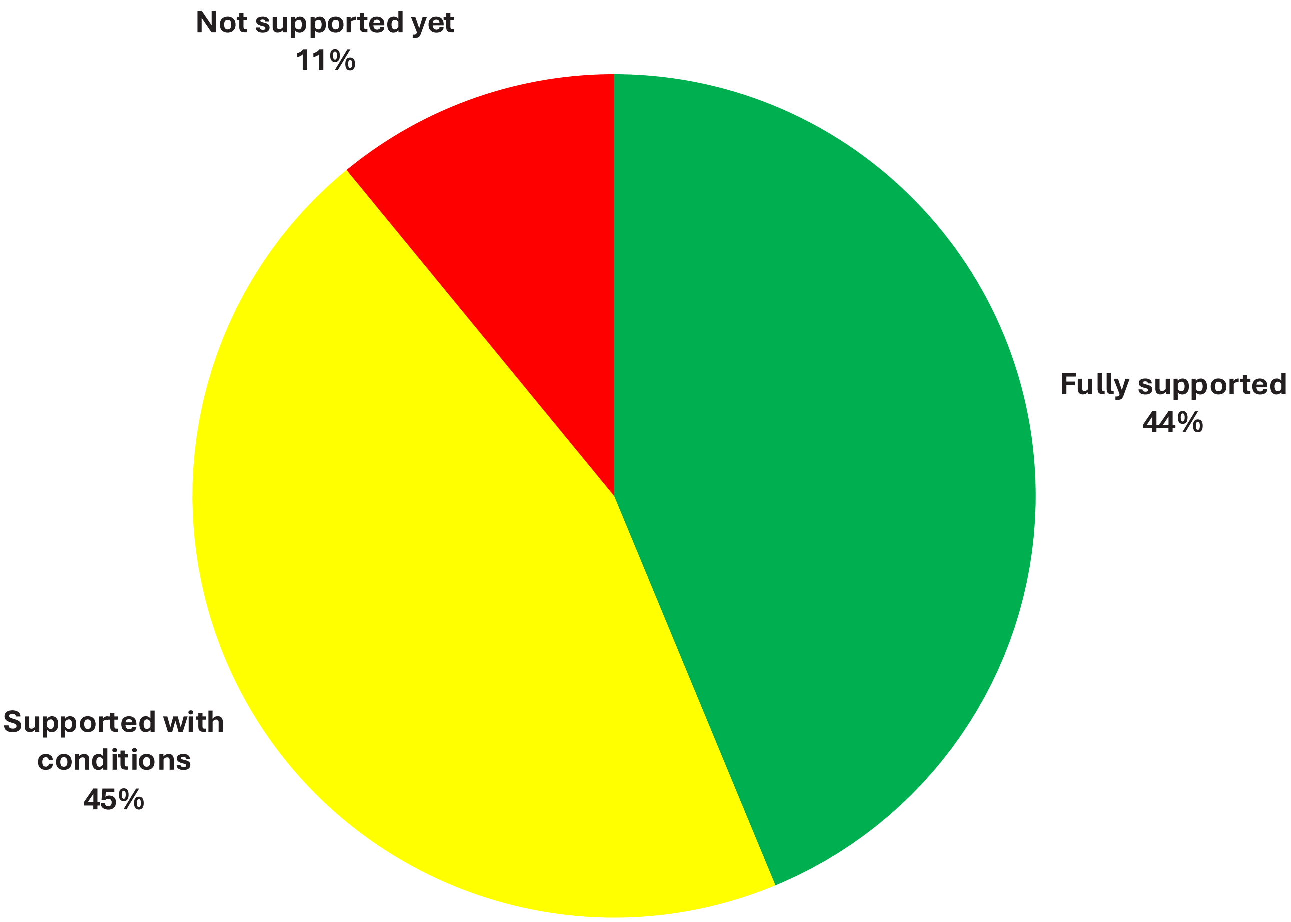
Version 1.0 As of 10/04/2022

Xage Zero Trust Roadmap Coverage Summary

Xage supports 90% of DoD Zero Trust Strategy Activities and Functions. In some cases, certain configurations or conditions must be met to achieve full support.

- **Green:** Xage offers full, independent support for the Zero Trust Activities and Functions
- **Yellow:** Supported with conditions: The feature is available under certain configurations or conditions.
- **Red:** The zero trust activity or function is not yet supported by Xage, but may be in the future.

Activities and functions supported



Pillar: User

ID #	Activity/Capability Name	Capability or Activity	Capability/Activity Description	Xage Alignment (G, Y, R)	An explanation on how Xage aligns
1.1	User Inventory	Capability	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.	G	All users are maintained within the Xage Manager. Each user is given access to their required workload through a policy manager.
1.1.1	User Inventory	Activity	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.	G	Users are created in the Xage Fabric in one of two ways: 1. Created users in the Xage Fabric 2. Sync users from external LDAP or Active Directory (AD) source periodically These are not mutually exclusive. You can use an available LDAP or AD list of users AND you can commingle users created in the Xage Fabric. There is no conflict. This gives you maximum flexibility when configuring access.
1.2	Conditional User Access	Capability	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.	G	Xage Fabric's blockchain-based technology utilizes a distributed mesh architecture with nodes deployed at various levels or layers, which interact and interface with different services to orchestrate a multilayered access authentication system. It doesn't rely solely on network-based protection like traditional IDAM, ICAM, or PAM tools. Instead, it secures unmanaged identities, unprotected systems, and access methods. This means it verifies every interaction, regardless of the environment, ensuring that only authorized entities gain access.
1.2.1	App Based Permission	Activity	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 Pt1" 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.	G	Xage Security unifies identity and access management into a single, simple interface. You can configure multiple AD instances across layers and sites, plus manage user privileges and access policies for the users for each of those ADs. That makes it easy for administrators to not only easily implement defense-in-depth, but also maintain separate AD instances not just across sites but also across different layers of security: one or more for IT, one or more for the DMZ, and another for operational technology (OT).
1.2.2	Rule Based Dynamic Access Pt1	Activity	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.	G	By default, Xage Fabric users are automatically logged out if there is no activity detected for one hour. You can change this setting for any Edge Node. For the Xage Manager, users are automatically logged out after one hour of inactivity, and this cannot be changed.
1.2.3	Rule Based Dynamic Access Pt2	Activity	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.	G	Xage fulfills this requirement by providing a built-in framework for dynamic, AI-driven access control. Xage's AI-Driven Adaptive Access engine is designed for making dynamic access decisions that account for risk based on real-time behavioral and contextual analytics. This native machine learning capability can also be integrated with a broader cross-pillar AI engine; Xage can feed its risk signals to such a system and, in turn, receive automated policy updates or response actions via its APIs. Furthermore, Xage's AI co-pilot, Xena, directly assists administrators in the automated rule management process by analyzing access patterns and recommending optimized, risk-based policies.
1.2.4	Enterprise Gov't roles and Permissions Pt1	Activity	DoD Organizations federate remaining user and group attributes as appropriate to the Enterprise Identity, Credential and Access Management (ICAM) solution. The updated attribute set is used to create universal roles for Organizations to use. Core functions of the Identity Provider (IdP) and Identity, Credential and Access Management (ICAM) solutions are migrated to cloud services and/or environments enabling improved resilience and performance.	G	Cloud-hosted Zero Trust Remote Access (ZTRA) services and centralized administration, configuration and access delivered via the cloud. Zero Trust Access to environments accessible from anywhere via a web browser
1.2.5	Enterprise Gov't roles and Permissions Pt2	Activity	DoD Organizations move all possible functions of the Identity Provider (IdP) and Identity, Credential and Access Management (ICAM) solutions to cloud environments. Enclave/DDIL environments local capabilities to support disconnected functions but ultimately are managed by the centralized Identity, Credential and Access Management (ICAM) solutions. Updated roles are now mandated for usage and exceptions are reviewed following a risk-based approach.	G	The ZTRA cloud service includes MFA, has no need for VPNs or jump boxes, and securely terminates vulnerable protocols such as RDP and VNC before they reach the outside world. Cloud sign-up, with on-site enforcement provided by self-configuring software to get the customer up and running in minutes.
1.3	Multi-Factor Authentication (MFA)	Capability	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.	G	Xage Fabric supports multi-factor authentication (MFA). Unless you restrict an MFA method in the Settings on the Advanced page, users who have MFA enabled for their account can choose whether to receive MFA codes by email or through an authenticator app. CAC or SAML authorization is currently supported. Users can specify their MFA preferences on their Profile page.

Pillar: User

1.3.1	Organizational MFA/IDP	Activity	DoD Organizations procure and implement a centralized Identity Provider (IdP) solution and Multi-Factor (MFA) solution. The IdP and MFA solution may be combined in a single application or separated as needed assuming automated integration is supported by both solutions. Both IdP and MFA support integration with the Enterprise PKI capability as well enabling key pairs to be signed by the trusted root certificate authorities. Mission/Task-Critical applications and services are utilizing the IdP and MFA solution for management of users and groups.	G	Xage's enables MFA for any device and application, so industrial organizations can enforce authentication with multiple-factors (passwords, one time token, biometric, etc.) across their entire system. For the very first time, operators can add MFA to all of their assets (new and legacy), and enforce universal multi-factor, identity-based, low latency access on remote assets, even over intermittent networks.
1.3.2	Alternative Flexible MFA Pt1	Activity	DoD Organization's Identity Provider (IdP) supports alternative methods of multi-factor authentication complying with Cyber Security requirements (e.g., FIPS 140-2, FIPS 197, etc.). Alternative tokens can be used for application-based authentication. Multi-Factor options support Biometric capability and can be managed using a self-service approach. Where possible multi-factor provider(s) is moved to cloud services instead of being hosted on-premise.	G	Xage Security unifies identity and access management into a single, simple interface. You can configure multiple AD instances across layers and sites, plus manage user privileges and access policies for the users for each of those ADs. That makes it easy for administrators to not only easily implement defense-in-depth, but also maintain separate AD instances not just across sites but also across different layers of security
1.3.3	Alternative Flexible MFA Pt2	Activity	Alternative tokens utilize user activity patterns from cross pillar activities such as "User Activity Monitoring (UAM) and User & Entity Behavior Analytics (UEBA)" to assist with access decision making (e.g., not grant access when pattern deviation occurs). This functionality is further extended onto Biometric enabled alternative tokens as well.	G	Enable local and remote users to use passwordless, hardware-based, and biometric MFA through multiple hops that may be mapped to different identity providers.
1.4	**Privileged Access Management (PAM)**	**Capability**	**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.**	G	**Xage natively meets these requirements through its unified platform. The Xage Fabric provides built-in User and Entity Behavior Analytics (UEBA) via its AI-Driven Adaptive Access engine, which automatically baselines activity and detects anomalies in real-time. Core Privileged Access Management (PAM) functions, including deep activity monitoring with command-level detail, are also native to the platform. Finally, Just in-Time (JIT) and Just-Enough-Access (JEA) are fundamental principles of the Xage policy engine, allowing for the direct creation of granular, temporary access rules. These capabilities are all performed by the Xage Fabric itself, without requiring a SIEM for the core functionality.**
1.4.1	Implement System and Migrate Privileged Users Pt1	Activity	DoD Organizations procure and implement a Privileged Access Management (PAM) solution support all critical privileged use cases. Application/Service integration points are identified to determine status of support for the PAM solution. Applications/Services that easily integrate with PAM solution are transitioned over to using solution versus static and direct privileged permissions.	G	Xage's Security Fabric starts with building an identity for machines, users, applications, and data. On top of that, it creates an identity-based universal access control layer that enables secure, fine-grained control over various interactions within the IT/OT environment. Fine-grained control includes flow and parameter-based control mapping, according to the policies and roles of identities involved in the interaction.
1.4.2	Implement System and Migrate Privileged Users Pt2	Activity	DoD Organizations utilize the inventory of supported and unsupported Applications/Services for integration with privileged access management (PAM) solution to extend integrations. PAM is integrated with the more challenging Applications/Services to maximize PAM solution coverage. Exceptions are managed in a risk-based methodical approach with the goal of migration off and/or decommissioning Applications/Services that do not support PAM solution.	G	Zero trust control over individual interactions (within and outside of trust zones) across edge, control center, datacenter, and cloud deployments
1.4.3	Real time Approvals & JIT/JEA Analytics Pt1	Activity	Identification of necessary attributes (Users, Groups, etc.) are automated and integrated into the Privileged Access Management (PAM) solution. Privilege access requests are migrated to the PAM solution for automated approvals and denials.	G	Site administrators can see all the users, access requests, devices, and policies on the Xage Manager. However, they can only modify resources such as policies with devices that are assigned to their site or are not assigned to a site.
1.4.4	Real time Approvals & JIT/JEA Analytics Pt2	Activity	DoD Organizations integrate User & Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) solutions with the Privileged Access Management (PAM) solution providing user pattern analytics for decision making.	G	Xage fulfills this requirement as a native, unified platform, eliminating the need to integrate separate UEBA, UAM, and PAM solutions. The Xage Fabric inherently combines these functions. As it manages privileged access (the PAM function), it simultaneously monitors all user sessions and commands (UAM). This data is then fed directly into its integrated UEBA engine, which analyzes user patterns to detect anomalies in real-time. Because these capabilities are part of a single system, Xage can instantly use its analytical findings for decision-making. For example, if a privileged user's activity deviates from their established baseline, Xage's policy engine can automatically terminate the session or require step-up authentication, directly connecting user pattern analytics to privileged access enforcement.
1.5	**Identity Federation & User Credentialing**	**Capability**	**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.**	G	**Xage enables single sign-on for all sites mapped to the same identity provider. When a user logs into an operational site via the Xage fabric, they can only see the assets for the site they've authenticated to. They can then authenticate into other sites without leaving the Xage Fabric, and any assets they are allowed to access will become visible, per their privileges and admin-controlled policies.**

Pillar: User

1.5.1	Organizational Identity Life-Cycle Management	Activity	DoD Organizations establish a process for life cycle management of users both privileged and standard. Utilizing the Organizational Identity Provider (IdP) the process is implemented and followed by the maximum number of users. Any users who fall outside of the standard process are approved through risk-based exceptions to be evaluated regularly for decommission.	G	Users are created in the Xage Fabric in one of two ways. Created users in the Xage Fabric meaning users are created via Xage Manager or "internal" and managed by the fabric. Sync users from external LDAP or Active Directory (AD) source periodically where users are synced from an "external" source and managed outside the Xage Fabric.
1.5.2	Enterprise Identity LifeCycle Management Pt1	Activity	The DoD Enterprise works with Organizations to review and align the existing Identity Lifecycle Processes, policy, and standards. A finalized agreed upon policy and supporting process are developed and followed by the DoD Organizations. Utilizing the centralized or federated Identity Provider (IdP) and Identity & Access Management (IdAM) solutions, DoD Organizations implement the Enterprise Lifecycle Management process for the maximum number of identities, groups, and permissions. Exceptions to the policy are managed in a risk based methodical approach.	G	You can use an available LDAP or AD list of users AND you can commingle users created in the Xage Fabric. There is no conflict. This gives you maximum flexibility when configuring access. Maintaining Users is a straightforward process and is performed through the Xage Manager. Regardless of how you add users in to the Xage Fabric, every user must belong to at least one user group.
1.5.3	Enterprise Identity LifeCycle Management Pt2	Activity	DoD Organizations further integrate the critical automation functions of the Identity Provider (IdP) and Identity, Credential and Access Management (ICAM) solutions following the Enterprise Lifecycle Management process to enable Enterprise automation and analytics. Identity Lifecycle Management primary processes are integrated into the cloud-based Enterprise ICAM solution.	G	Xage zero trust microsegmentation policies do not require cloud connectivity to function. If a remote site loses contact, policies are still stored and enforced locally. Security teams can be confident that your security posture is strong even if network connectivity is unstable.
1.5.4	Enterprise Identity LifeCycle Management Pt3	Activity	DoD Organizations integrate remaining Identity Lifecycle Management processes with the Enterprise Identity, Credential and Access Management solution. Enclave/DDIL environments while still authorized to operate integrate with the Enterprise ICAM using local connectors to the cloud environment.	G	Xage allows simple, centralized policy creation to protect every asset from core to edge to cloud.
1.6	**Behavioral, Contextual ID, and Biometrics**	**Capability**	**Xage Fabric integrates with Enterprise IDPs (LDAP, SAML) for basic user attributes and supports user activity monitoring via session recordings. It lacks native UEBA but can send logs to a SIEM for UEBA expansion with organizational attributes. Integration with PAM and JIT/JEA for anomaly detection requires SIEM configuration.**	G	**Xage natively provides a unified security platform with built-in User and Entity Behavior Analytics (UEBA), Privileged Access Management (PAM), and Just-in-Time (JIT) access controls. Its AI engine automatically detects anomalies, while its policy engine enforces granular, temporary access with detailed activity monitoring. These core functions are performed directly by the Xage Fabric itself, without requiring a SIEM for the initial detection, policy enforcement, or JIT functionality.**
1.6.1	Implement User & Entity Behavior Activity (UEBA) Tooling	Activity	DoD Organizations procure and implement User & Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) solutions. Initial integration point with Enterprise IdP is completed enabling future usage in decision making.	G	Xage meets this requirement by acting as a complete, natively unified platform, eliminating the need to procure and integrate separate UEBA and UAM solutions for the assets it protects. The Xage Fabric inherently combines these functions. Upon integrating with the Enterprise IdP, it immediately begins monitoring all user and entity activity (UAM) for every access session it manages. This rich activity data is automatically fed into its built-in AI engine to perform real-time behavioral analysis (UEBA), detecting anomalies against an established baseline. This allows Xage to make immediate, risk-based access decisions. In environments that have already invested in a separate enterprise UEBA tool, Xage also serves as a critical integration point, feeding it unparalleled data from OT/legacy systems and acting as the real-time enforcement arm for any threats the enterprise UEBA platform detects.
1.6.2	User Activity Monitoring Pt1	Activity	DoD Organizations integrate User & Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) solutions with Organizational Identity Providers (IdP) for extended visibility as needed. Analytics and data generated by UEBA and UAM for critical applications/services are integrated with the Just-in-Time and Just-Enough-Access solution improving decision making further.	G	Xage fulfills this requirement as a native, all-in-one platform, eliminating the complex integration work between separate UEBA, UAM, IdP, and JIT/JEA solutions. The Xage Fabric's architecture inherently connects these functions. Upon integrating with an organizational IdP, Xage immediately begins monitoring user and entity activity (UAM) for every access request. This activity data is automatically analyzed by its built-in UEBA engine to detect behavioral anomalies. Because the Just-in-Time (JIT) and Just-Enough-Access (JEA) policy engine is part of the same system, it instantly uses these UEBA analytics and risk signals to make smarter decisions. For example, a JIT access request to a critical application can be automatically denied or flagged for review if the user's current behavior is flagged as anomalous by the UEBA engine, thus directly integrating behavioral analytics with the JIT/JEA decision-making process.
1.6.3	User Activity Monitoring Pt2	Activity	DoD Organizations continue the analytics usage from User & Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) solutions by using generated data for all monitored applications and services when decision making occurs in the Just-in-Time and JustEnough-Access solution.	G	This continuous operational use-case is a core native strength of the Xage Fabric's unified design. Xage's User Activity Monitoring (UAM), User and Entity Behavior Analytics (UEBA), and Just-in-Time/Just-Enough-Access (JIT/JEA) functions are all part of a single platform, the data feedback loop is constant and immediate. For every access decision across all monitored applications and services, the Xage JIT/JEA policy engine automatically uses the live analytics generated by its UAM and UEBA engine. This ensures that every grant of access is informed by the most current behavioral risk assessment, fulfilling the requirement for continuous, data-driven decision-making without the latency or complexity of integrating separate tools.

Pillar: User

1.7	Least Privileged Access	Capability	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.	G	Xage Security unifies identity and access management into a single, simple interface. You can configure multiple AD instances across layers and sites, plus manage user privileges and access policies for the users for each of those ADs.
1.7.1	Deny User by Default Policy	Activity	DoD Organizations audit internal user and group usage for permissions and revoke permissions when possible. This activity includes the revocation and/or decommission of excess permissions and access for application/service-based identities and groups. Where possible static privileged users are decommissioned or reduced permissions preparing for future rule/dynamic based access.	G	Users Accessing the Xage Fabric will only be allowed to access the workload they are explicitly allowed to access. An unauthorized access will not be able to see any elements outside their authorized view.
1.8	Continuous Authentication	Capability	DoD organizations will advance beyond basic, single-session authentication by leveraging an enterprise-wide Identity Provider (IdP) for all users and Non-Person Entities (NPEs). This continuous authentication model will enforce re-validation based on time, risk, and user behavior, requiring step-up multi-factor authentication for access to sensitive data or privileged operations.	G	Xage natively delivers a complete continuous authentication model that fulfills this entire requirement. After an initial sign-on, which Xage validates against an Enterprise IdP, the platform enforces continuous verification throughout the session. Xage's policy engine can mandate periodic re-authentication based on time and, more importantly, can trigger real-time, step-up multi-factor authentication for specific high-risk actions, such as privilege changes or accessing critical services. Furthermore, its integrated UEBA engine continuously analyzes user patterns, automatically forcing re-authentication if behavior becomes anomalous. This inherent combination of time, transaction, and behavior-based checks ensures users are consistently validated, moving far beyond a simple one-time login.
1.8.1	Single Authentication	Activity	DoD Organizations employ basic authentication processes to authenticate users and NPEs at least once per session (e.g., logon). Importantly users being authenticated are managed by the parallel activity "Organizational MFA/IDP" with the Organizational Identity Provider (IdP) versus using application/service-based identities and groups.	G	Xage Fabric employs basic authentication for users and NPEs at session start (e.g., logon) via integration with Organizational IdPs (LDAP, SAML) and MFA, avoiding application/service-based identities.
1.8.2	Periodic Authentication	Activity	DoD Organizations enable period authentication requirements for applications and services. Traditionally these are based on duration and/or duration timeout but other period based analytics can be used to mandate re-authentication of user sessions.	G	This requirement is met natively by the Xage Fabric's policy enforcement engine. Xage allows administrators to easily configure periodic re-authentication policies for any application or service. These policies can enforce traditional re-authentication based on a fixed duration or session timeout, such as requiring a user to log in again every four hours. More powerfully, Xage also uses its native analytics to mandate re-authentication based on risk, automatically triggering a new MFA challenge if a user's behavior deviates from their established pattern during a session, thus fulfilling the need for more advanced, analytics-driven re-authentication triggers.
1.8.3	Continuous Authentication Pt 1	Activity	DoD Organizations' applications/service utilize multiple session authentications based on security attributes and access requested. Privilege changes and associational transaction requests required additional levels of authentication such as Multi-Factor Authentication (MFA) pushes to users.	G	Xage Fabric supports multiple session authentications based on security attributes and access requests, with additional MFA pushes for privilege changes and transaction requests via IdP integration (LDAP, SAML).
1.8.4	Continuous Authentication Pt 2	Activity	DoD Organizations continue usage of transaction-based authentication to include integration such as user patterns.	G	This advanced requirement is a core native capability of the Xage Fabric's unified architecture. Xage's policy engine is designed for transaction-based authentication, allowing policies to be set on specific actions or commands a user attempts to execute. This is then seamlessly integrated with its native User and Entity Behavior Analytics (UEBA). As Xage continuously monitors user activity to build individual patterns of behavior, it can automatically trigger step-up authentication for any transaction that deviates from a user's normal pattern. This means a user attempting an unusual but critical action is forced to re-validate their identity in that moment, directly fulfilling the requirement to integrate user patterns into transaction-based security decisions.
1.9	Integrated ICAM Platform	Capability	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.	G	Xage fulfills this requirement with its native capabilities. Xage natively integrates with and relies upon the DoD's enterprise-level identity management (IdM) and Public Key Infrastructure (PKI) systems, including federated models that trust a central root CA. It acts as the "access management tool" that verifies the identities of users, administrators, and NPEs against these central sources. Based on this verified identity, Xage's policy engine then enforces granular Just-in-Time (JIT) and Just-Enough-Access (JEA) controls, ensuring that access is strictly limited to only those who have the "need and right to know" at the moment of the request.

Pillar: Device

ID #	Activity/Capability Name	Capability or Activity	Capability/Activity Description	Xage Alignment (G, Y, R)	An explanation on how Xage aligns
2.1	**Device Inventory**	**Capability**	**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.**	G	**Xage Fabric contains inventories of devices and systems in the OT and IT environment. In addition, Xage provides capabilities to detect the addition of new devices/systems and the removal of these assets. Xage inventory can be integrated with additional visibility and resource management tools, and leveraged to automatically track inventory.**
2.1.1	Device Health Tool Gap Analysis	Activity	DoD Organizations develop a manual inventory of devices within the environment. Device attributes tracked in the inventory enable functionality outlined in the ZTA target level.	G	Xage Fabric contains inventories of devices and systems in the OT and IT environment. In addition, Xage provides capabilities to detect the addition of new devices/systems and the removal of these assets. Xage inventory can be integrated with additional visibility and resource management tools, and leveraged to automatically track inventory.
2.1.2	NPE/PKI, Device under Management	Activity	DoD Organizations utilize the DoD Enterprise PKI solution/service to deploy x509 certificates to all supported and managed devices. Additional other Non-Person Entities (NPEs) that support x509 certificates are assigned in the PKI and/or IdP systems.	G	Xage natively supports this requirement by integrating with existing Public Key Infrastructure (PKI) systems like the DoD Enterprise PKI. The Xage Fabric is designed to natively ingest and validate x.509 certificates from any trusted source, using them as a foundational element of device and Non-Person Entity (NPE) identity. By leveraging these existing DoD-issued certificates, Xage establishes a trusted, tamper-proof identity for every asset. This identity is then used as the basis for creating and enforcing dynamic, least-privilege access policies, ensuring that only cryptographically verified devices and services can participate in protected interactions.
2.1.3	Enterprise IDP Pt1	Activity	The DoD Enterprise Identity Provider (IdP) either using a centralized technology or federated organizational technologies integrates NonPerson Entities (NPEs) such as devices and service accounts. Integration is tracked in the Enterprise Device Management solution when applicable as to whether it is integrated or not. NPEs not able to be integrated with the IdP are either marked for retirement or excepted using a risk based methodical approach.	G	Xage directly and natively addresses this requirement, specializing in the very NPEs that cannot be integrated with a traditional IdP. Xage functions as a crucial identity proxy for legacy and operational devices that lack modern security protocols. The Xage Fabric enrolls these NPEs, such as service accounts or PLCs, and presents them as a single, modern application to the enterprise IdP. This means that assets previously marked for retirement or exception due to integration challenges can now be brought under the DoD's central identity governance. By providing this bridge, Xage offers the "risk-based methodical approach" to securing these assets rather than retiring them. While the connection to the IdP is a native Xage function, it can also integrate with an Enterprise Device Management solution via its APIs to update the status of an NPE from "excepted" to "fully integrated and managed."
2.1.4	Enterprise IDP Pt2	Activity	The DoD Enterprise Identity Provider (IdP) either using a centralized technology or federated organizational technologies adds additional dynamic attributes for NPEs such as location, usage patterns, etc.	G	This requirement is met natively by Xage's AI-Driven Adaptive Access and analytics capabilities. The Xage Fabric is purpose-built to continuously monitor the operational context and behavior of every Non-Person Entity (NPE) it manages. It automatically generates dynamic attributes by analyzing real-time data streams, which includes usage patterns (e.g., what other assets it communicates with, at what frequency, with what protocols) and location (e.g., its network segment or physical site). This behavioral baselining and anomaly detection engine enriches the NPE's identity with dynamic, risk-associated attributes. These attributes are then used by the Xage policy engine to make adaptive access decisions in real-time, directly fulfilling the DoD's need for a richer, more dynamic understanding of NPE identity and risk posture.
2.2	**Device Detection and Compliance**	**Capability**	**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)**	Y	**Xage supports the DoD's Comply to Connect (C2C) initiative and Zero Trust Architecture (ZTA) by integrating with DoD C2C policies and standards, ensuring vendor compatibility, and meeting base-level functionality requirements for Zero Trust environments. Xage's platform enforces compliance checks, supports granular access control, continuous authentication, and dynamic policy enforcement. It allows for scalable implementation, integrating with existing DoD systems and other vendors to provide a comprehensive C2C solution, enhancing the DoD's cybersecurity posture in alignment with Zero Trust principles.**
2.2.1	Implement C2C/Compliance Based Network Authorization Pt1	Activity	The DoD Enterprise working with the Organizations develops a policy, standard and requirements for Comply to Connect. Once agreement is reached solution procurement is started, a vendor(s) is selected, and implementation begins with base level functionality in ZT Target environments (low risk). Base level checks are implemented in the new Comply to Connection solution enabling the ability to meet ZTA target functionalities.	Y	Xage supports the DoD's Comply to Connect (C2C) initiative and Zero Trust Architecture (ZTA) by integrating with DoD C2C policies and standards, ensuring vendor compatibility, and meeting base-level functionality requirements for Zero Trust environments. Xage's platform enforces compliance checks, supports granular access control, continuous authentication, and dynamic policy enforcement. It allows for scalable implementation, integrating with existing DoD systems and other vendors to provide a comprehensive C2C solution, enhancing the DoD's cybersecurity posture in alignment with Zero Trust principles.

Pillar: Device

2.3.5	Fully Integrate Device Security stack with C2C	Activity	DoD Organizations continue the deployment of Application Control to all environments and in prevention mode. File Integrity Monitoring (FIM) and Application Controls analytics are integrated into Comply to Connect for expanded access decision making data points. Comply to Connect analytics are evaluated for further device/endpoint security stack data points such as UEDM and are integrated as necessary.	Y	Xage supports the DoD's expanded deployment of Application Control and File Integrity Monitoring (FIM) by integrating these security measures into its Comply to Connect (C2C) framework. The platform can incorporate Application Control analytics and FIM data points into its access decision-making process, enhancing the overall security posture. Xage's policy engine can leverage these additional data points, along with Unified Endpoint Device Management (UEDM) information, to make more informed and dynamic access control decisions. This integration allows for prevention-mode operation across all environments, ensuring that only authorized applications are executed and that file integrity is maintained. By continuously evaluating these expanded security stack data points, Xage enables DoD organizations to implement more robust, context-aware access controls that align with zero trust principles, further strengthening their cybersecurity defenses.
2.3.6	Enterprise PKI Pt1	Activity	The DoD Enterprise Public Key Infrastructure (PKI) is expanded to include the addition of NPE and device certificates. NPEs and device that do not support PKI certificates are marked for retirement and decommission starts.	G	Xage meets this requirement natively by acting as a security proxy for assets that cannot handle certificates. A Xage enforcement node is deployed in front of the legacy device and manages the DoD-issued PKI certificate on its behalf. This instantly provides a modern, compliant identity to the non-PKI asset without any changes to the device itself, satisfying the mandate and preventing the need for costly retirement and decommissioning.
2.3.7	Enterprise PKI Pt2	Activity	DoD Organizations utilize certificates for device authentication and machine to machine communications. Unsupported devices complete retirement and exceptions are approved using a risk based methodical approach.	G	Xage Enforcement Point allows for device to device authentication and enforces machine to machine communications via Device to Device policies as defined within the PDP (Xage Manager). The Xage Fabric implements trust based mechanisms that are responsible for the consensus voting that either permits or denies communications based on device attributes. Xage uses certificates and ensures that M2M communications are encrypted with an AES-256 tunnel for individual interactions. Xage automatically manages keys, certificates, and related authentication.
2.4	**Remote Access**	**Capability**	**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.**	Y	**For Phase 1, Xage is deployed in a monitor mode to natively audit all existing access processes. It discovers and maps every interaction between devices, users, and applications, providing the comprehensive visibility needed to establish an initial least-privilege policy baseline. In Phase 2, Xage natively extends access to BYOD and IoT devices by enforcing authentication through the Enterprise IdP for any application it protects, acting as a proxy for IoT devices that cannot otherwise support modern identity. Finally, in the mature phase, Xage combines its native AI-driven attributes (like device usage patterns and behavioral analytics) with integrated attributes from other tools (such as a BYOD's compliance status from an MDM) to deliver the required granular, attribute-based access control for any device connecting to any service.**
2.4.1	Deny Device by Default Policy	Activity	DoD Organizations block all unmanaged remote and local device access to resources. Compliant managed devices are provided risk based methodical access following ZTA target level concepts.	G	Xage supports DoD organizations in blocking all unmanaged remote and local device access to resources by enforcing strict access controls and ensuring that only compliant, managed devices are granted access. The platform integrates with network access solutions to mandate risk-based, methodical access for compliant devices, following Zero Trust Architecture (ZTA) target level concepts.
2.4.2	Managed and Limited BYOD & IOT Support	Activity	DoD Organizations utilize Unified Endpoint and Device Management (UEDM) and similar solutions to ensure that managed Bring Your Own Device (BYOD) and Internet of Things (IoT) devices are fully integrated with Enterprise IdP enable user and device-based authorization are supported. Device access for all applications requires dynamic access policies.	Y	Xage can permit logging into systems via nothing more than a browser which can be an unmanaged, BYOD system. Access can be granted in a dynamic way by calling Xage REST API's using other detection tooling. Xage is able to integrate with MDM or UEDM solutions to either permit or deny access based on predetermined attributes.
2.4.3	Managed and Full BYOD & IOT Support Pt1	Activity	DoD Organizations utilize Unified Endpoint and Device Management (UEDM) and similar solutions to enable access for managed and approved devices to Mission and Operational Critical services/applications using dynamic access policies. BYOD and Internet of Things (IoT) devices are required to meet standard baseline checks before authorization.	Y	The Xage Fabric protects all equipment, from new IoT devices to vulnerable legacy systems, delivering identity management, single sign-on, and access control with in-field enforcement across the mission operation. Xage can shield vulnerable devices while customers work with their vendors to update/patch as there will always be situations that exist that may prevent a system from receiving a patch (hardware flaws, etc.) and yet require that a system still be able to send sensor data across a ZT Gateway such as the Xage Enforcement Point.

Pillar: Device

2.7.2	Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt1	Activity	DoD Organizations procure and implement Extended Detection & Response (XDR) solution(s). Integration points with cross pillar capabilities are identified and prioritized based on risk. The riskiest of these integration points are actioned and integration is started. EDR continues coverage of endpoints to include the maximum number of services and applications as part of the XDR implementation. Basic analytics are sent from the XDR solution stack to the SIEM.	Y	Xage Fabric does not natively include an XDR solution but supports user activity monitoring via session recordings and audit trails. It can integrate with cross-pillar capabilities via SIEM, prioritizing risky points for action, and send basic analytics to the SIEM, with EDR coverage extended to maximum services via external integration.
2.7.3	Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt2	Activity	XDR solution stack completes identification of integration points expanding coverage to the fullest amount possible. Exceptions are tracked and managed using a risk based methodical approach for continued operation. Extended analytics enabling ZT Advanced functionalities are integrated into the SIEM and other appropriate solutions.	Y	While Xage is not the XDR solution itself, it serves as a critical integration point and an essential data source for the XDR and SIEM ecosystem, particularly in closing coverage gaps. Xage extends the XDR stack's visibility and control into OT, IoT, and other non-standard environments where traditional agents cannot be deployed, providing a risk-based, methodical approach for managing these exceptions. Furthermore, Xage streams its highly granular, identity-centric access logs (both successful and failed attempts) to the SIEM. This data is a cornerstone for the "extended analytics" required for ZT Advanced functionalities, allowing the security stack to correlate endpoint and network telemetry from the XDR with precise user and machine access events to detect sophisticated threats.

Pillar: Application & Workload

ID #	Activity/Capability Name	Capability or Activity	Capability/Activity Description	Xage Alignment (G, Y, R)	An explanation on how Xage aligns
3.1	**Application Inventory**	**Capability**	**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**	Y	**Xage is designed to integrate with an organization's CMDB or asset management system, which serves as the official inventory of identified and authorized applications and components. Xage then uses this inventory data to natively build and enforce granular access control policies. If any application or component not on the authorized inventory list attempts to communicate across the network, Xage will block the connection by default, ensuring that only explicitly authorized and inventoried software can operate within the system owner's purview.**
3.1.1	Application/Code Identification	Activity	DoD Organizations create an inventory of approved applications and code (e.g., source code, libraries, etc.). Each organization will track the supportability (i.e., active, legacy, etc.) and hosted location (i.e., cloud, on-premise, hybrid, etc.) at least in the inventory.	G	Xage supports this by integrating with asset management systems and leveraging this inventory data to enforce access controls and compliance checks. Currently, Xage is mainly deployed on-premises in virtualized environments, but it also supports cloud environments, ensuring comprehensive protection across various deployment scenarios.
3.1.2	Resource Authorization Pt1	Activity	The DoD Enterprise standardizes on resource authorization approaches (e.g., Software Defined Perimeter) with the organizations. At a minimum the resource authorization gateways will be integrated with identities and devices. Organizations deploy approved resource authorization gateways and enable for external facing applications/services. Additional applications for migration and applications unable to be migrated are identified for exception or decommission.	Y	Xage Fabric integrates identities and devices with its policy engine but does not natively implement a distinct resource authorization gateway like Software Defined Perimeter. It manages access control and can identify applications for migration or decommissioning through policy enforcement.
3.1.3	Resource Authorization Pt2	Activity	Resource authorization gateways are used for all possible applications/services. Application unable to utilize gateways are either decommissioned or excepted using a risk based methodical approach. Authorizations are further integrated with the CI/CD pipeline for automated decision making.	G	Xage supports the DoD's requirement for resource authorization gateways by ensuring that all possible applications and services utilize these gateways. Applications unable to use the gateways are either decommissioned or granted exceptions based on a risk-based approach. Xage integrates these authorizations with the CI/CD pipeline, enabling automated decision-making processes. While not everything is currently automated, Xage is actively working towards full automation, ensuring that only authorized personnel have access to CI/CD pipelines through a rigorous review and authorization process.
3.2	**Secure Software Development & Integration**	**Capability**	**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.**	Y	**Xage delivers real-time runtime protection by controlling all interactions between running applications based on Zero Trust policies. It functions as a secure API gateway, microsegmenting traffic and enforcing authorization on a per-request basis. For container and serverless security, Xage provides a consistent identity based policy enforcement mesh that governs all communications, which is ideal for ephemeral workloads. While Xage does not perform code reviews, it integrates with the results from such tools to enforce stricter runtime controls on applications flagged as high-risk.**
3.2.1	Build DevSecOps Software Factory Pt1	Activity	The DoD enterprise creates the foundational standards for modern DevSecOps processes and CI/CD pipelines. The concepts are applied in a standardized technology stack across DoD organizations able to meet future Application Security requirements. An enterprise-wide Vulnerability Management program is integrated with the CI/CD pipelines following the Vulnerability Management Program activities.	Y	Xage Fabric supports secure access and authentication via IdP integration (LDAP, SAML) but does not natively provide DevSecOps processes, CI/CD pipelines, or an enterprise-wide Vulnerability Management program. These can be integrated via external DevSecOps tools.
3.2.2	Build DevSecOps Software Factory Pt2	Activity	DoD Organizations will use their approved CI/CD pipelines to develop most new applications. Any exceptions will follow a standardized approval process to be allowed to develop in a legacy fashion. DevSecOps processes are also used to develop all new applications and update existing applications. Continual validation functions are integrated into the CI/CD pipelines and DevSecOps processes and integrated with existing applications.	Y	Xage Fabric supports secure access and authentication via IdP integration (LDAP, SAML) but does not natively provide CI/CD pipelines, DevSecOps processes, or continual validation functions. These can be integrated via external CI/CD and DevSecOps tools for new and existing applications.
3.2.3	Automate Application Security & Code Remediation Pt1	Activity	A standardized approach to application security including code remediation is implemented across the DoD enterprise. Part one (1) of this activity includes the integration of a Secure API gateway with applications utilizing API or similar calls. Code reviews are conducted in a methodical approach and standardized protections for containers and their infrastructure are in place. Additionally, any serverless functions where the 3rd party manages the infrastructure such as Platform as a Service utilize adequate serverless security monitoring and response functions. Code Reviews, Container and Serverless security functions are integrated into the CI/CD and/or DevSecOps process appropriate.	Y	Xage Fabric supports secure access via IdP integration (LDAP, SAML) but does not natively provide a Secure API gateway, code remediation, or standardized protections for containers and serverless functions. These can be integrated via external tools into CI/CD and DevSecOps processes.

Pillar: Application & Workload

3.2.4	Automate Application Security & Code Remediation Pt2	Activity	functions (e.g., code review, container and serverless security) are implemented as part of CI/CD and DevSecOps and secure architectures by allowing for quicker changes to code in each microservice as security issues are discovered. Further advancement security remediation activities continue across the DoD Enterprise with the inclusion of runtime security functions for containers as appropriate, automated vulnerable library updates and automated CI/CD approvals during the release process.	Y	Xage Fabric supports secure access via IdP integration (LDAP, SAML) but does not natively implement code review, container/serverless security, runtime security, or automated updates/approvals in CI/CD and DevSecOps. These can be integrated via external tools.
3.3	Software Risk Management	Capability	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.	Y	Xage integrates with the tools that manage software Bills of Materials (BoM), supplier risk, and vulnerability scanning. It consumes the risk data from these systems to act as a powerful compensating control and enforcement point. For example, if a vulnerability management program identifies a critical flaw in an application, a native Xage policy can be enforced to immediately isolate that application or severely restrict its network access until it is remediated. Furthermore, Xage can enforce policies that block applications from communicating with unapproved repositories or update channels. By integrating with CI/CD pipelines, these risk-based access policies can be automatically applied, ensuring continuous validation and enforcement throughout the development lifecycle.
3.3.1	Approved Binaries/Code	Activity	The DoD enterprise uses best practice approaches to manage approved binaries and code in a methodical approach. These approaches will include supplier sourcing risk management, approved repository usage, bill of materials supply chain risk management, and industry standard vulnerability management.	Y	Xage Lacks native management of approved binaries and code. Requires external tools for supplier sourcing risk, approved repositories, bill of materials supply chain risk, and industry-standard vulnerability management.
3.3.2	Vulnerability Management Program Pt1	Activity	The DoD Enterprise works with Organizations to establish and manage a Vulnerability Management program. The program includes a policy and standards agreed upon by all Organizations. The developed program includes at a minimum the track and management of public vulnerabilities based on DoD applications/services. Organizations establish a vulnerability management team with key stakeholders where vulnerabilities are discussed and managed following the Enterprise policy and standards.	Y	Xage lacks native Vulnerability Management program. Requires external tools to track and manage public vulnerabilities for DoD applications/services and establish a team per enterprise policy.
3.3.3	Vulnerability Management Program Pt2	Activity	Processes are established at the DoD Enterprise level for managing the disclosure of vulnerabilities in DoD maintained/operated services both publicly and privately accessible. DoD Organizations expand the vulnerability management program to track and manage closed vulnerability repositories such as DIB, CERT, and others.	Y	Xage lacks native processes for managing vulnerability disclosures or tracking closed repositories like DIB and CERT. Requires external tools to expand vulnerability management.
3.3.4	Continual Validation	Activity	DoD Organizations will implement a continual validation approach for application development where parallel deployment is conducted and integrated with an approved environment level (e.g., UAT, Prod). Applications unable to integrate continual validation into their CI/CD process are identified and exceptions are provided as needed using a methodical approach.	Y	Xage lacks native continual validation for application development or parallel deployment integration. Requires external CI/CD tools; exceptions need manual identification and methodical approval.
3.4	Resource Authorization & Integration	Capability	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 microsegmented using authorizations.	G	Xage functions as a programmatic, software-defined gateway where security policies are managed as code, allowing them to be seamlessly integrated into and deployed via CI/CD pipelines. For every transaction in the live environment, Xage makes a real-time, risk-based authorization decision by analyzing the security posture of the User (from the IdP), the Device (via integration with EDR/UEM tools), and the Data itself. This ability to continuously enrich decisions with attributes from across the pillars allows Xage to enforce granular microsegmentation for enterprise APIs, authorizing or denying each programmatic request based on its comprehensive risk assessment.
3.4.1	SDC Resource Authorization Pt1	Activity	The DoD Enterprise provides a standardized approach for code based compute management (i.e., Software Defined Compute) following industry best practices. Using risk-based approaches baselines are created using the approved set of code libraires and packages. DoD Organizations work with the approved code/binaries activities to ensure that applications are identified which can and cannot support the approach. Applications which can support a modern software-based configuration and management approaches are identified and transitioning begins. Applications which cannot follow software-based configuration and management approaches are identified and allowed through exception using a methodical approach.	G	Xage is deployed to manage all identified legacy applications and systems that require an exception. Xage natively wraps these applications in a software-defined security layer, allowing administrators to manage all their access control policies as code via API. This brings the non-compliant legacy assets under a modern, programmatic management framework without any changes to the underlying applications themselves, thus securing the exceptions and enabling the broader standardization effort to proceed.
3.4.2	SDC Resource Authorization Pt2	Activity	Xage relies on the DoD for transitioning applications to software-based configuration in production. Requires external tools to identify and decommission incompatible applications.	G	Xage is deployed specifically to manage and secure the legacy and OT applications that have been identified as incompatible with modern approaches. Rather than requiring the decommissioning of these systems, Xage's core function is to extend their life by wrapping them in a software-defined security fabric. This allows administrators to manage access policies for these incompatible applications as code, bringing them under a modern security model and eliminating the need for their immediate retirement.

Pillar: Application & Workload

3.4.3	Enrich Attributes for Resource Authorization Pt1	Activity	Initial attributes from sources such as User and Entity Activity Monitoring, Micro-segmentation services, DLP and DRM are integrated into the Resource Authorization technology stack and policy. Any additional attributes for later integration are identified and planned. Attributes are used to create basic risk posture of users, NPEs and devices allowing for authorization decisions.	G	All API calls to Xage Manager must transit through a secure gateway. Once client identification is verified and authorized, a valid API key with a specified time-to-live (TTL) will be issued for use within the application.
3.4.4	Enrich Attributes for Resource Authorization Pt2	Activity	Extended identified attributes are integrated with the resource authorization technology and policy. Confidence scoring is introduced across the attributes to create a more advanced method of authorization decision making in an automated fashion.	G	Xage relies on the DoD for integrating extended attributes with resource authorization and policy. Requires external tools for confidence scoring and automated authorization decisions.
3.4.5	REST API Micro-Segments	Activity	Xage relies on the DoD for approved API gateways and micro-segmentation of application calls to authenticated destinations. Requires external tools for integrating API micro-segmentation consoles with SDP or SDN consoles.	G	While Xage's product operates on a single broker model rather than a multi-tenant setup, user group policies are implemented to segment users effectively. In multi-tenant environments, micro-segmentation APIs are typically advantageous for enhancing security and control.
3.5	Continuous Monitoring and Ongoing Authorizations	Capability	DoD organizations employ automated tools and processes to continuously monitor applications and assess their authorization to operate	G	Xage acts as an automated tool to continuously monitor applications and enforce their authorization to operate. Once an application's authorized communication paths and behaviors are defined, they are codified as policies within the Xage policy engine. Xage then continuously monitors all of the application's network interactions in real time. If the application attempts any communication that falls outside the explicit bounds of its authorization, or if its behavior becomes anomalous, Xage automatically blocks the unauthorized action and generates an alert, providing a constant, automated assessment that the application is operating as intended.
3.5.1	Continuous Authorization to Operate (cATO) Pt1	Activity	DoD Organizations utilize automation solutions within the environment to standardize the monitoring of controls and offer the capability to identify deviations. Where appropriate monitoring and testing is integrated with DevSecOps processes.	G	Xage natively standardizes the monitoring of controls by continuously enforcing access policies across all protected assets and applications. Its integrated AI engine automatically identifies deviations by comparing real-time activity against both explicit rules and learned behavioral baselines, instantly flagging anomalies. To support DevSecOps, Xage's API-first, policy-as-code design allows it to be directly integrated into CI/CD pipelines. This enables development teams to automatically provision, test, and deploy access controls as part of their workflow, ensuring security monitoring is built into the application lifecycle from the start.
3.5.2	Continuous Authorization to Operate (cATO) Pt2	Activity	DoD Organizations fully automate control derivation, testing and monitoring processes. Deviations are automatically tested and resolved using existing cross pillar automation infrastructure. Dashboarding is used to monitor the status of authorizations and analytics are integrated with the responsible authorizing officials.	G	Xage's policy-as-code architecture allows organizations to fully automate the derivation, testing, and deployment of access controls. Its AI-driven engine natively and continuously monitors for deviations from established policies and baselines, automatically resolving many issues by blocking or isolating the offending asset in real time. For broader issues, Xage can integrate with cross-pillar automation infrastructure (like a SOAR platform) to trigger orchestrated responses. Furthermore, the native Xage Insights dashboard provides real-time status monitoring of authorizations and system-wide analytics, which can be used directly by or integrated with dashboards for authorizing officials.

Pillar: Data

ID #	Activity/Capability Name	Capability or Activity	Capability/Activity Description	Xage Alignment (G, Y, R)	An explanation on how Xage aligns
4.1	**Data Catalog Risk Alignment**	**Capability**	**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 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**	**y**	**While Xage does not perform data discovery and classification to create the inventory, it is the primary tool for enforcing the data owners' policies and protecting that cataloged landscape. Once data owners identify and inventory critical data assets, they use Xage to define granular access policies for them. Xage then acts as the secure gateway to these assets, ensuring that any attempt to access or alter data is authenticated and authorized against the owner's policy. By blocking and logging all unauthorized attempts, Xage automatically mitigates the risks of data loss or alteration and provides a complete audit trail for risk review, ensuring the integrity of the data landscape.**
4.1.1	Data Analysis	Activity	DoD Organizations update the service and application catalog(s) with data classifications. Data tags are also added to each service and application.	y	While Xage is not the tool used to classify data or update the service catalog, it is the enforcement engine that leverages those data tags and classifications to secure access.
4.2	**DoD Enterprise Data Governance**	**Capability**	**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.**	**R**	**We are continuing to make progress in this area and aim to have a feature released soon that supports this requirement.**
4.2.1	Define Data Tagging Standards	Activity	The DoD Enterprise works with organizations to establish data tagging and classification standards based on industry best practices. Classifications are agreed upon and implemented in processes. Tags are identified as manual and automated for future activities.	R	We are continuing to make progress in this area and aim to have a feature released soon that supports this requirement.
4.2.2	Interoperability Standards	Activity	The DoD Enterprise collaborating with the organizations develops interoperability standards integrating mandatory Data Rights Management (DRM) and Protection solutions with necessary technologies to enable ZT target functionality.	R	We are continuing to make progress in this area and aim to have a feature released soon that supports this requirement.
4.2.3	Develop Software Defined Storage (SDS) Policy	Activity	The DoD enterprise working with organizations establishes a software define storage (SDS) policy and standards based on industry best practices. DoD organizations evaluate current data storage strategy and technology for implementation of SDS. Where appropriate storage technology is identified for SDS implementation.	R	We are continuing to make progress in this area and aim to have a feature released soon that supports this requirement.
4.3	**Data Labeling and Tagging**	**Capability**	**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.**	**R**	**We are continuing to make progress in this area and aim to have a feature released soon that supports this requirement.**
4.3.1	Implement Data Tagging & Classification Tools	Activity	DoD Organizations utilize the enterprise standard and requirements to implement data tagging and classification solution(s). Organizations ensure that future ML and AI integrations are supported by solutions through DoD enterprise requirements.	R	We are continuing to make progress in this area and aim to have a feature released soon that supports this requirement.
4.3.2	Manual Data Tagging Pt1	Activity	Using the DoD Enterprise data tagging and classification policy and standards, manual tagging starts using basic data level attributes to meet ZT target functionality.	R	We are continuing to make progress in this area and aim to have a feature released soon that supports this requirement.
4.3.3	Manual Data Tagging Pt2	Activity	DoD organizational specific data level attributes are integrated into the manual data tagging process. DoD enterprise and organizations collaborate to decide which attributes are required to meet ZTA advanced functionality. Data level attributes for ZTA advanced functionality are standardized across the enterprise and incorporated.	R	We are continuing to make progress in this area and aim to have a feature released soon that supports this requirement.
4.3.4	Automated Data Tagging & Support Pt1	Activity	DoD Organizations use data loss prevention, rights management, and/or protection solutions to conduct scanning of data repositories. Standardized tags are applied to supported data repositories and data types. Unsupported data repositories and types are identified.	R	We are continuing to make progress in this area and aim to have a feature released soon that supports this requirement.
4.3.5	Automated Data Tagging & Support Pt2	Activity	Remaining supported data repositories have basic and extended data tags which are applied using machine learning and artificial intelligence. Extended data tags are applied to existing repositories. Unsupported data repositories and data types are evaluated for decommissioning using a risk based methodical approach. Approved exceptions utilize manual data tagging approaches with data owners and/or custodians to manage tagging.	R	We are continuing to make progress in this area and aim to have a feature released soon that supports this requirement.

Pillar: Data

4.4	**Data Monitoring and Sensing**	**Capability**	**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.**	**Y**	**Xage natively provides the core fabric for identity-based access control, policy enforcement, and the monitoring of anomalous access activity for data assets like file shares and databases. This allows it to natively capture active metadata related to access requests and use. However, for comprehensive, content-aware Data Loss Prevention (DLP) and Data Rights Management (DRM) analysis, Xage is designed to integrate with and serve as the enforcement point for specialized external tools. Therefore, it meets the requirement through a combination of native capabilities for access control and monitoring, and robust integration with dedicated third-party DLP/ DRM solutions.**
4.4.1	DLP Enforcement Point Logging and Analysis	Activity	DoD Organizations identify data loss prevention (DLP) enforcement points such as specific services and user endpoints. Using the established DoD Enterprise cybersecurity incident response standard, DoD organizations ensure the appropriate detail of data is captured. Additionally, protection, detection, and response use cases are developed to better outline solution coverage.	Y	Xage Fabric can forward security events, i.e., Audit Logs, to external Security Information and Event Management (SIEM) tools. Events are transported with the syslog protocol and can be forwarded to a centralized log repository.
4.4.2	DRM Enforcement Point Logging and Analysis	Activity	DoD Organizations identify data rights management (DRM) enforcement points such as specific services and user endpoints. Using the established DoD Enterprise cybersecurity incident response standard, DoD organizations ensure the appropriate detail of data is captured. Additionally, protection, detection, and response use cases are developed to better outline solution coverage.	Y	Xage Fabric can forward security events, i.e., Audit Logs, to external Security Information and Event Management (SIEM) tools. Events are transported with the syslog protocol and can be forwarded to a centralized log repository.
4.4.3	File Activity Monitoring Pt1	Activity	DoD Organizations utilize File Monitoring tools to monitor the most critical data classification levels in applications, services, and repositories. Analytics from monitoring is fed into the SIEM with basic data attributes to accomplish ZT Target functionality.	Y	Xage natively monitors all access to critical files and data by acting as the identity-based gatekeeper for every transaction. Our fabric intercepts every request, capturing detailed logs including user/machine identity, asset requested, time, and location before it's granted. This granular audit data and any policy violation alerts are then streamed via standard protocols like Syslog directly to your SIEM. This provides the SIEM with the precise, attributed data it needs to correlate events and accomplish Zero Trust analytics, fulfilling the requirement through Xage's native monitoring and forwarding capabilities without needing a separate file monitoring tool for the systems Xage protects.
4.4.4	File Activity Monitoring Pt2	Activity	DoD Organizations utilize File Monitoring tools to monitor all regulatory protected data (e.g., CUI, PII, PHI, etc.) in applications, services, and repositories. Extended integration is used to send data to appropriate inter/intra-pillar solutions such as Data Loss Prevention, Data Rights Management/Protection and User & Entity Behavior Analytics.	Y	Xage Fabric can forward security events, i.e., Audit Logs, to external User and Entity Behavior Analytic (UEBA) tools. Events are transported with the syslog protocol and can be forwarded to a centralized log repository.
4.4.5	Database Activity Monitoring	Activity	DoD Organizations procure, implement, and utilize Database Monitor solutions to monitor all databases containing regulated data types (CUI, PII, PHI, etc.). Logs and analytics from the database monitoring solution are fed to the SIEM for monitoring and response. Analytics are fed into cross pillar activities such as "Enterprise Security Profile" and "Real Time Access" to better direct decision making.	Y	Xage Fabric can forward security events, i.e., Audit Logs, to external Security Information and Event Management (SIEM) tools. Events are transported with the syslog protocol and can be forwarded to a centralized log repository.
4.4.6	Comprehensive Data Activity Monitoring	Activity	DoD Organizations expand monitoring of data repositories including databases as appropriate based on a methodical risk approach. Additional data attributes to meet the ZT Advanced functionalities are integrated into the analytics for additional integrations.	Y	Xage Fabric can forward security events, i.e., Audit Logs, to external SIEM/SOAR tools. Events are transported with the syslog protocol and can be forwarded to a centralized log repository.
4.5	**Data Encryption & Rights Management**	**Capability**	**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**	**Y**	**While Xage is not the DRM tool that applies tag-based encryption to files, it provides two critical functions for the overall strategy. First, Xage natively encrypts all data-in-transit for access sessions it proxies, securing the communication path to the data. Second, it acts as the intelligent access gateway to the data-at-rest; it integrates with the data tagging system and uses that information, along with its own AI-powered behavioral analytics, to ensure only authorized users under normal conditions can access the repositories where DRM-protected data is stored. This provides a crucial layer of access control that works in concert with the DRM encryption itself.**
4.5.1	Implement DRM and Protection Tools Pt1	Activity	DoD Organizations procure and implement DRM and Protection solution(s) as needed following the DoD Enterprise standard and requirements. Newly implement DRM and protection solution(s) are implemented with high risk data repositories using ZTA target level protections.	Y	All data repositories within the Xage Fabric will be controlled at the granular level. Only user with explicit policies dictating that users have access are accepted into the Xage Fabric.
4.5.2	Implement DRM and Protection Tools Pt2	Activity	DRM and protection coverage is expanded to cover all in scope data repositories. Encryption keys are automatically managed to meet best practices (e.g., FIPS). Extended data protection attributes are implemented based on the environment classification.	Y	As data is produced, it is digitally-signed with a unique key. The key's certificate is shared via the Fabric trusted immutable ledger, guaranteeing the data origin alongside existing unique device records in the Fabric. It can then be matched with relevant metadata, to identify the data's originating device.
4.5.3	DRM Enforcement via Data Tags and Analytics Pt1	Activity	Data rights management (DRM) and protection solutions are integrated with basic data tags defined by the DoD Enterprise standard. Initial data repositories are monitored and have protect and response actions enabled. Data at rest is encrypted in repositories.	Y	As data is exchanged and extracted, Xage ensures integrity via data fingerprints (cryptographic hashes and signatures), which are replicated across the Fabric, allowing the data's integrity to be checked anywhere as needed.

Pillar: Data

4.5.4	DRM Enforcement via Data Tags and Analytics Pt2	Activity	Extended data repositories are protected with DRM and Protection solutions. DoD Organizations implement extended data tags applicable to organizations versus mandated enterprise. Data is encrypted in extended repositories using additional tags.	Y	Data source client is a unique identifier of a data publisher (writer) or a data subscriber (reader). In addition to data source client, data source topic is also added. Data source topic is a specific data stream to be secured within the Xage Fabric.
4.5.5	DRM Enforcement via Data Tags and Analytics Pt3	Activity	DRM and Protection solutions integrate with AI and ML tooling for encryption, rights management and protection functions.	Y	The Xage Fabric provides several REST APIs specifically for Zero Trust Data Exchange. These APIs are available at the core/center on the Xage Broker and can be made available at the edge/site on each Xage Node.
4.6	**Data Loss Prevention (DLP)**	**Capability**	**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.**	**R**	**We are continuing to make progress in this area and aim to have a feature released soon that supports this requirement.**
4.6.1	Implement Enforcement Points	Activity	Data loss prevention (DLP) solution is deployed to the in-scope enforcement points. DLP solution is set to "monitor-only" and/or "learning" mode limiting impact. DLP solution results are analyzed, and policy is fine tuned to manage risk to an acceptable level.	R	We are continuing to make progress in this area and aim to have a feature released soon that supports this requirement.
4.6.2	DLP Enforcement via Data Tags and Analytics Pt1	Activity	Data loss prevention (DLP) solution is updated from monitor only mode to prevention mode. Basic data tags are utilized for DLP solution and logging schema is integrated.	R	We are continuing to make progress in this area and aim to have a feature released soon that supports this requirement.
4.6.3	DLP Enforcement via Data Tags and Analytics Pt2	Activity	Data loss prevention (DLP) solution is updated to include extended data tags based on parallel Automation activities.	R	We are continuing to make progress in this area and aim to have a feature released soon that supports this requirement.
4.6.4	DLP Enforcement via Data Tags and Analytics Pt3	Activity	Data loss prevention (DLP) solution is integrated with automated data tagging techniques to include any missing enforcement points and tags.	R	We are continuing to make progress in this area and aim to have a feature released soon that supports this requirement.
4.7	**Data Access Control**	**Capability**	**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.**	**Y**	**Xage's policy engine is natively designed to make access decisions by evaluating a combination of properties in real time: the user/NPE's attributes (from the IdP), the device's security posture (via integration with UEM/EDR), and the data's classification tag (via integration with data labeling tools). By acting as the enforcement gateway in front of the SDS, Xage ensures that only authorized users on compliant devices can access specific data segments. This provides a critical layer of Zero Trust enforcement that works in concert with the underlying SDS permissions and complements the file-level protections offered by integrated DRM tooling.**
4.7.1	Integrate DAAS Access w/ SDS Policy Pt1	Activity	Utilizing the DoD enterprise SDS policy, organizational DAAS policy is developed with intended integration in mind. SDS implementation guide is developed by DoD organizations due to environment specific nature.	G	With the Xage Fabric you can access your workload through a policy based browser session. This also eliminates the ability to access other browser sessions.
4.7.2	Integrate DAAS Access w/ SDS Policy Pt2	Activity	DoD Organizations implement the DAAS policy in an automated fashion.	G	Xage directly addresses the automated implementation of a Data as a Service (DAAS) policy by functioning as a universal control and enforcement fabric. Our platform automates policy enforcement by sitting in the path of every access request and evaluating it in real-time against your centrally defined rules.
4.7.3	Integrate DAAS Access w/ SDS Policy Pt3	Activity	Newly implemented SDS technology and/or functionalities are integrated with the DAAS policy in a risk-based fashion. A phased approach should be taken to during implementation to measure results and adjust accordingly.	Y	The Xage Fabric is purpose-built to integrate new technologies like Software-Defined Security (SDS) with existing policies in a controlled, risk-based manner. Our overlay architecture allows you to connect a new SDS solution and use its output (e.g., threat intelligence, device posture) as a dynamic, risk-based attribute within your DAAS access policies. For a phased implementation, you can initially apply these new, stricter policies in a "monitor-only" mode to a limited set of assets. This allows you to measure the results and analyze the detailed audit logs Xage generates to see the impact of the policy without blocking access. Based on these results, you can adjust the policy and then incrementally expand enforcement from lower-risk systems to your most critical assets, ensuring a seamless and risk-managed integration.

Pillar: Data

4.7.4	Integrate Solution(s) and Policy with Enterprise IDP Pt1	Activity	DoD Organizations develop an integration plan using the SDS policy and technology/functionality with the enterprise Identity Provider (IdP) solution.	Y	Xage serves as the central integration fabric for connecting your enterprise Identity Provider (IdP), such as a CAC/PIV system or Azure AD, with your SDS policies and technologies. The integration plan is straightforward: you first configure Xage to trust your IdP using standard protocols like SAML or OpenID Connect, allowing Xage to use it as the authoritative source for user identity. Simultaneously, you configure Xage to receive real-time risk data from your SDS tools via its flexible APIs. The core of the plan involves using Xage's policy engine to combine the verified identity from the IdP with the risk context from the SDS to create and automate fine-grained access rules, effectively using Xage as the bridge that makes the IdP and SDS work together to secure every asset.
4.7.5	Integrate Solution(s) and Policy with Enterprise IDP Pt2	Activity	Newly implemented SDS technology and/or functionalities are integrated with the Enterprise Identity Provider (IdP) following the integration plan. Identity attributes required to meet ZT Target functionalities are required for integration.	G	Within the Xage Fabric the REST API provides a flexible and standard method to Create, Read, Update and Delete data for any application or services using HTTP/HTTPS
4.7.6	Implement SDS Tool and/or integrate with DRM Tool Pt1	Activity	Depending on the need for a Software Defined Storage tool, a new solution is implemented or an existing solution is identified meeting the functionality requirements to be integrated with DLP, DRM/Protection, and ML solutions.	G	Within the Xage Fabric the REST API provides a flexible and standard method to Create, Read, Update and Delete data for any application or services using HTTP/HTTPS
4.7.7	Implement SDS Tool and/or integrate with DRM Tool Pt2	Activity	DoD Organizations configure the SDS functionality and/or solution to be integrated with the underlying DLP and DRM/Protection infrastructure as appropriate. Lower-level integrations enable more effective protection and response.	G	Within the Xage Fabric the REST API provides a flexible and standard method to Create, Read, Update and Delete data for any application or services using HTTP/HTTPS

Pillar: Network & Environment

ID #	Activity/Capability Name	Capability or Activity	Capability/Activity Description	Xage Alignment (G, Y, R)	An explanation on how Xage aligns
5.1	Data Flow Mapping	Capability	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.	G	Xage provides network monitoring utilizing the Traffic Interactions view within the Xage Manager UI. The traffic interactions view is dependent on the utilization of Xage Enforcement Points and provides output related to affected policies, access beign allowed or denied and metadata around source, destination, protocols and traffic count.
5.1.1	Define Granular Control Access Rules & Policies Pt1	Activity	The DoD Enterprise working with the Organizations creates granular network access rules and policies. Associated Concept of Operations (ConOps) are developed in alignment with access policies as well ensure future supportability. Once agreed upon, DoD Organizations will implement these access policies into existing network technologies (e.g., Next Generation Firewalls, Intrusion Prevention Systems, etc.) to improve initial risk levels.	G	In the Xage fabric, user groups are mapped to device groups to create user access policies. User groups can have any number of users and users can exist across multiple user groups. Device groups may contain any number of device access methods and device access methods can exist in multiple device groups. Alternatively, device groups can be mapped to one another to enable device to device access controls when Xage Enforcement Points are in use within the environment in front of both devices. Similar to device to device policies, a network resource policy allows access to a XEP protected device from a non XEP protected device. Via the Zero Trust Data Exchange product feature, policies enabling read/write access to specific data topics can be created by mapping data clients to specific data topics.
5.1.2	Define Granular Control Access Rules & Policies Pt2	Activity	DoD Organizations utilize data tagging and classification standards to develop data filters for API access to the SDN Infrastructure. API Decision Points are formalized within the SDN architecture and implemented with non-mission/task critical applications and services.	**Y**	Via the use of Xage Zero Trust Data Exchange, data ingested by the Xage Fabric via API can be tagged as orgainized as configurable data topics. Access to those data topics is defined by policy both for read and write permissions. Leveraging the distributed nature of the Xage Fabric, those data topics become available anywhere Xage is deployed via API.
5.2	**Software Defined Networking (SDN)**	**Capability**	**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.**	Y	Xage provides a distributed fabric across the network environment as an overlay to the existing archtecture. At minimum this includes the Xage core services (Xage Manager, Xage Broker and four Center Peers) and at least one Xage Edge Node. The Edge Nodes can be deployed across multiple network segements and forwarding to higher levels of the network stack can be enabled allowing for remote access of devices in different segments from the Xage Edge Node at the network segement where the device lives and from the Xage Edge Node above them. Due to the distributed nature of the Xage Fabric, information is securely stored and distributed across all Xage components and used to provide access control based on identity.
5.2.1	Define SDN APIs	Activity	The DoD Enterprise works with the Organizations to define the necessary APIs and other programmatic interfaces to enable Software Defined Networking (SDN) functionalities. These APIs will enable Authentication Decision Point, Application Delivery Control Proxy and Segmentation Gateways automation.	G	The Xage provided API's for user, device and policy management are held exclusivley on the Xage Manager and not available at the edge. These API endpoints require user bearer token based authentication to interact with them. Alternatively, the Xage Edge Nodes host API's allowing for some user interactions with endpoint devices and with the Zero Trust Data Exchange product.
5.2.2	Implement SDN Programable Infrastructure	Activity	Following the API standards, requirements and SDN API functionalities, DoD Organizations will implement Software Defined Networking (SDN) infrastructure to enable automation tasks. Segmentation Gateways and Authentication Decision Points are integrated into the SDN infrastructure along with output logging into a standardized repository (e.g., SIEM, Log Analytics) for monitoring and alerting.	G	Xage provides audit logs and traffic interaction logs that can be exported to a SIEM logging host. The audit logs detail every user interaction and component interaction within the deployment. User sessions are also available to be recorded when using SSH, RDP and VNC proxy methods. User sessions can be terminated from the Xage Manager interface as well as allowing for those sessions to be monitored and the users accounts being suspended.
5.2.3	Segment Flows into Control, Management, and Data Planes	Activity	Network infrastructure and flows are segmented either physically or logically into control, management, and data planes. Basic segmentation using IPv6/VLAN approaches is implemented to better organize traffic across data planes. Analytics and NetFlow from the updated infrastructure is automatically fed into Operations Centers and analytics tools.	**R**	Xage does not currently utilize IPV6 protocols or VLANs though Xage does support deployment of Xage Components across multiple vlans. Additionally, Xage builds IPSec tunnels between Xage Nodes allowing for secure transmission of data from point to point.
5.2.4	Network Asset Discovery & Optimization	Activity	DoD Organizations automate network asset discovery through the SDN infrastructure limiting access to devices based on risk based methodical approaches. Optimization is conducted based on the SDN analytics to improve overall performance along with provide necessary approved access to resources.	**Y**	Via the use of third party integrators like Nozomi, Xage has the ability to ingest data from said integrator to create device records and device accesmethods in an automated fashion.
5.2.5	Real-Time Access Decisions	Activity	SDN Infrastructure utilizes cross Pillar data sources such as User Activity Monitoring, Entity Activity Monitoring, Enterprise Security Profiles and more for real-time access decisions. Machine learning is used to assist decision making based on advanced network analytics (full packet capture, etc.). Policies are consistently implemented across the Enterprise using unified access standards.	Y	This requirement is met through a combination of native Xage capabilities and necessary integrations. Xage natively provides the unified policy engine, the real-time decision-making framework, and machine learning to analyze the access patterns it observes. However, to leverage the full spectrum of cross-pillar data such as inputs from dedicated User Activity Monitoring tools, enterprise security profiles, or advanced network analytics based on full packet capture Xage is designed to integrate with these specialized systems. In summary, Xage is the native engine that makes the real-time decision, but it requires integration to consume the diverse, external data sources mentioned.

Pillar: Network & Environment

5.3	Macro Segmentation	Capability	**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.**	G	Due to the distributed nature of the Xage Fabric, Xage components can be placed across multiple network segments and provide protocol breaks and IPSec tunneling between components. Devices are accessed via reverse proxy ensuring that the sessions from node to node are unique and not replicated. Users are provisioned access to devices on an allow only basis, ensuring unauthorized access is not available. If there is not a policy defining the users access to a device, the user will not have the option to connect to the device.
5.3.1	Datacenter Macro segmentation	Activity	DoD Organizations implement data center focused macrosegmentation using traditional tiered (web, app, db) and/or service-based architectures. Proxy and/or enforcement checks are integrated with the SDN solution(s) based on device attributes and behavior.	G	Xage Insights provides usefule and actionable data based on current and historical data captured by the Xage Fabric. This includes user and device interactions, trends and other metadata that can be displayed to the administrator in the form of graphs and charts on a SIEM. This data can then be output to alternate vendors to utilize Machine Learning and AI capabilities to enhance the administration of the deployment. Scripting can be created to utilize the data to perform actions against the Xage API's to take actions based on these trends and data findings.
5.3.2	B/C/P/S Macro segmentation	Activity	DoD Organizations implement base, camp, post, and station macrosegmentation using logical network zones limiting lateral movement. Proxy and/or enforcement checks are integrated with the SDN solution(s) based on device attributes and behavior.	Y	Access to endpoint devices when using either native application on the users workstation or via web proxy is available via the Xage Fabric UI. This allows web applications, RDP, VNC, SSH and other protocols to be proxied throught the Xage Fabric ensuring that no additional communications are premissable and that access is always authenticated prior to accessing the device. Records are kept of that access within the Xage audit logs and traffic interaction logs. Users must be authenticated and have a policy allowing them explicit access to the endpoint device(s) prior to being allowed to access the device, without these privisions, the user will not have access to the endpoint device(s).
5.4	Micro Segmentation	Capability	**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.**	G	By leveraging the Xage Enforcement Point in front of a single or multiple devices, segmentation of those devices from the rest of the network can be easily accomplished. The Xage Enforcement Point acts as a Layer 2 and Layer 3 in line filter only allowing communications to endpoint devices when there is an explicit policy allowing those communications. Additionally, devices that may be connected downstream from the XEP may not require protection and as such, the concept of Xage Protected Devices allows for the granular configuration of policies to define which devices communications will be protected for and those that will not.
5.4.1	Implement Micro segmentation	Activity	DoD Organizations implement Micro-Segmentation infrastructure into SDN environment enabling basic segmentation of service components (e.g., web, app, db), ports and protocols. Basic automation is accepted for policy changes including API decision making. Virtual hosting environments implement micro-segmentation at the host/container level.	G	Due to the XEPs handling traffic flow to protected devices, Xage can automate the opening and closing of the device communication pathways to allow users access only when they are authenticated to the Xage Fabric. When users logout or are no longer authenticated to the Xage Fabric, the rules allowing the communication to the endpoint device are closed and removed. This provides just in time access to endpoint devices when and only if there is a policy allowing the authenticated user to access the device.
5.4.2	Application & Device Micro segmentation	Activity	DoD Organizations utilize Software Defined Networking (SDN) solution(s) to establish infrastructure meeting the ZT Target functionalities – logical network zones, role, attribute and conditional based access control for user and devices, privileged access management services for network resources, and policy-based control on API access.	G	Due to the in-line positioning of the Xage Enforcement Point as an in-line network traffic filter, network zones, Xage Logical Sites and network segmentation is not only maintained but improved. The XEP also allows for the protection of device to device communications by automating the building of IPSec tunnles between XEPs that require communication with one another. This is accomplished automatically via the Xage Fabric when a policy allows the communication between the endpoint devices.
5.4.3	Process Micro segmentation	Activity	DoD Organizations utilize existing micro-segmentation and SDN automation infrastructure enabling process micro-segmentation. Hostlevel processes are segmented based on security policies and access is granted using real-time access decision making.	G	The Xage Enforcement Point provides micro segementation between the network and one or more devices downstream of the XEP. The XEP acts as a Layer 2 and Layer 3 in-line filter that operates on allow only polcies ensuring that any un-authenticated access or communication to downstream devices is prohibited. Logs are kept of attempted access to protected devices and policies are on a just in time basis. Just in time access policies ensure that users provisioned with access policies allowing them to access downstream devices are only premitted to do so when the user is fully authenticated through the Xage Fabric, and when that authentication is revoked (user logs out or session is terminiated) the access is closed and the policy is removed from the XEP. Due to the in-line positioning of the XEP, network zones, Xage Logical Sites and network segmentation is not only maintained but improved. The XEP also allows for the protection of device to device communications by automating the building of IPSec tunnles between XEPs that require communication with one another. This is accomplished automatically via the Xage Fabric when a policy allows the communication between the endpoint devices.
5.4.4	Protect Data In Transit	Activity	Based on the data flow mappings and monitoring, policies are enabled by DoD Organizations to mandate protection of data in transit. Common use cases such as Coalition Information Sharing, Sharing Across System Boundaries and Protection across Architectural Components are included in protection policies.	G	Xage protects data in transit in a multitude of fashions including but not limited to IPSec tunneling between Xage Components, use of the Xage Enforcement Point to protect data transmission between protected devices and the utilization of the Zero Trust Data Exchange product allowing for secure reading and writing of data directly to the Xage Fabric.

Pillar: Automation & Orchestration

ID #	Activity/Capability Name	Capability or Activity	Capability/Activity Description	Xage Alignment (G, Y, R)	An explanation on how Xage aligns
6.1	**Policy Decision Point (PDP) & Policy Orchestration**	**Capability**	**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.**	G	Xage directly implements the mature state of this requirement by providing a unified Policy Decision Point (PDP) and Policy Enforcement Point (PEP) framework for DAAS access. In the Xage Fabric, administrators centrally define and document all access policies the "who, what, where, when, and how" which serves as the PDP. These policies are then distributed to Xage's software- or hardware-based Enforcement Points, which act as PEPs at the edge. These PEPs make real-time access determinations, enabling, monitoring, and terminating every connection between a user or device and a DAAS resource strictly according to the centrally defined policy, thus providing the exact orchestration and dynamic control the requirement calls for.
6.1.1	Policy Inventory & Development	Activity	The DoD Enterprise works with the Organizations to catalog and inventory existing Cyber Security policies and standards. Policies are updated and created in cross pillar activities as needed to meet critical ZT Target functionality.	G	While Xage does not write the high-level governance documents, it serves as the platform to implement, digitize, and inventory the access control components of those cybersecurity policies. As policies are updated or created in cross-pillar activities, the specific access control rules such as which roles can access what data, from which devices, under what conditions are configured directly within the Xage Fabric. This provides a centralized, machine-readable catalog of all active, enforced access policies, translating high-level standards into the granular, auditable enforcement required to meet critical Zero Trust (ZT) target functionality.
6.1.2	Organization Access Profile	Capability	DoD Organizations develop basic access profiles for mission/task and non-mission/task DAAS access using the data from the User, Data, Network, and device pillars. The DoD Enterprise works with the Organizations to develop an Enterprise Security Profile using the existing Organizational security profiles to create a common access approach to DAAS. A phased approach can be used in organizations to limit risk to mission/task critical DAAS access once the security profile(s) are created.	Y	Xage serves as the platform to implement, digitize, and inventory the access control components of those cybersecurity policies. As policies are updated or created in cross-pillar activities, the specific access control rules (e.g., which roles can access what data, from which devices, under what conditions) are configured directly within the Xage Fabric. This provides a centralized, machine-readable catalog of all active, enforced access policies, translating high-level standards into the granular, auditable enforcement required to meet critical Zero Trust (ZT) target functionality.
6.1.3	Enterprise Security Profile Pt1	Activity	The Enterprise Security profile covers the User, Data, Network and Device pillars initially. Existing Organizational Security Profiles are integrated for non-mission/task DAAS access following an iterative approach to tuning access.	Y	While Xage is not the document repository for security profiles, it is the enforcement engine that integrates and tunes them for live operational use. Xage implements the Enterprise Security Profile by creating unified access control policies that span all pillars: User (identity-based authorization), Device (enforcement at the asset), Network (session management), and Data (access to specific applications/resources). Existing Organizational Security Profiles for non-mission DAAS access are modeled as granular, role-based policies within the Xage Fabric. This centralized control allows security teams to follow an iterative approach, easily tuning and updating these specific policies over time to refine access without disrupting the broader enterprise security posture.
6.1.4	Enterprise Security Profile Pt2	Activity	The minimum number of Enterprise Security Profile(s) exist granting access to the widest range of DAAS across Pillars within the DoD Organizations. Mission/task organization profiles are integrated with the Enterprise Security Profile(s) and exceptions are managed in a risk based methodical approach.	Y	While Xage does not define the enterprise profiles themselves, it provides the ideal framework to implement and enforce this hierarchical policy structure. Within the Xage Fabric, broad Enterprise Security Profiles can be created as baseline roles granting wide, least-privilege access to common DAAS resources. More specific mission/task profiles are then layered on top, inheriting the baseline permissions and adding more specific entitlements. For necessary exceptions, Xage enforces a risk-based approach through its granular controls, such as requiring multi-factor authentication, secondary approval, or time-limited session access for out-of-band requests, ensuring even non-standard access is managed methodically and securely.
6.2	**Critical Process Automation**	**Capability**	**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.**	Y	Xage provides the secure foundation and enforcement layer for automation tools like Robotic Process Automation (RPA). By assigning unique identities and least-privilege policies to RPA bots, Xage ensures they operate securely within their intended scope. Furthermore, Xage's API allows these automation platforms to execute critical functions as part of their workflows, such as instructing Xage to instantly isolate a device or revoke credentials, enabling secure and effective automated incident response and security control management.
6.2.1	Task Automation Analysis	Activity	DoD Organizations identify and enumerate all task activities that can be executed both manually and in an automated fashion. Task activities are organized into automated and manual categories. Manual activities are analyzed for possible retirement.	R	Xage does not currently utilize IPV6 protocols or VLANs though Xage does support deployment of Xage Components across multiple vlans. Additionally, Xage builds IPSec tunnels between Xage Nodes allowing for secure transmission of data from point to point.
6.2.2	Enterprise Integration & Workflow Provisioning Pt1	Activity	The DoD enterprise establishes baseline integrations within the Security Orchestration, Automation and Response solution (SOAR) required to enable target level ZTA functionality. DoD organizations identify integration points and prioritize key ones per the DoD enterprise baseline. Critical integrations occur meeting key services enabling recovery and protection capabilities.	Y	Xage's REST "Swagger API" can provide a flexible and standard method to Create, Read, Update, and Delete (CRUD) data for any applications or services using HTTPs. In the Body of the request you can include data to be submitted to the server such as a Data blob (JSON, formdata).

Pillar: Automation & Orchestration

6.2.3	Enterprise Integration & Workflow Provisioning Pt2	Activity	DoD Organizations integrate remaining services to meet baseline requirements and advanced ZTA functionality requirements as appropriate per environment. Service provisioning is integrated and automated into workflows where required meeting ZTA target functionalities.	R	We are continuing to make progress in this area and aim to have a feature released soon that supports this requirement.
6.3	**Machine Learning**	**Capability**	**DoD organizations employ ML to execute (and enhance execution of) critical functions such as incident response, anomaly detection, user baselining, and data tagging.**	**Y**	This capability is met through a combination of native features and integration. Xage natively employs Machine Learning to perform user baselining and anomaly detection, learning normal access patterns and automatically identifying deviations that could indicate a threat. This built-in ML also enables automated incident response, where a detected anomaly can trigger an immediate policy action like blocking a user or terminating a session. For data tagging, while Xage's policies can enforce rules based on existing data tags, the platform itself does not use ML to perform data classification. Instead, it integrates with dedicated data classification and tagging tools, consuming their output to inform its access control decisions.
6.3.1	Implement Data Tagging & Classification ML Tools	Activity	DoD Organizations utilize existing Data Tagging and Classification standards and requirements to procure Machine Learning solution(s) as needed. Machine Learning solution(s) is implemented in organizations and existing tagged and classified data repositories are used to establish baselines. Machine learning solution(s) applies data tags in a supervised approach to continually improve analysis.	Y	Xage supports this process through integration. Our platform is designed to be the enforcement layer that operationalizes the intelligence from your chosen ML data tagging solution. While DoD organizations procure a dedicated ML tool to scan repositories and apply tags, Xage integrates with that tool by consuming those tags as real-time metadata. This allows Xage to automatically enforce access policies based on the ML-generated classifications for instance, dynamically blocking access to a file the moment it is tagged as "Top Secret." Xage does not perform the ML-based tagging but makes the tags actionable for zero-trust security.
6.4	**Artificial Intelligence**	**Capability**	**DoD organizations employ AI to execute (and enhance execution of) critical functions - particularly risk and access determinations and environmental analysis.**	**R**	**We are continuing to make progress in this area and aim to have a feature released soon that supports this requirement.**
6.4.1	Implement AI automation tools	Activity	DoD Organizations identify areas of improvement based on existing machine learning techniques for Artificial Intelligence. AI solutions are identified, procured, and implemented using the identified areas as requirements.	Y	Xage's recently launched Xena AI Copilot, uses GenAI to generate scripts based on smart prompts based on user's abnormal behaviors. These scripts can be run on Xage to take advanced actions such as enforcing user MFA or password change. In the near future, the script based actions can be automated.
6.4.2	AI Driven by Analytics decides A&O modifications	Activity	DoD Organizations utilizing existing machine learning functions implement and use AI technology such as neural networks to drive automation and orchestration decisions. Decision making is moved to AI as much as possible freeing up human staff for other efforts. Utilizing historical patterns, AI will make anticipatory changes in the environment to better reduce risk.	Y	Xage's recently launched Xena AI Copilot, uses GenAI to generate scripts based on smart prompts based on user's abnormal behaviors. These scripts can be run on Xage to take advanced actions such as enforcing user MFA or password change. In the near future, the script based actions can be automated.
6.5	**Security Orchestration, Automation & Response (SOAR)**	**Capability**	**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.**	**R**	**We are continuing to make progress in this area and aim to have a feature released soon that supports this requirement.**
6.5.1	Response Automation Analysis	Activity	DoD Organizations identify and enumerate all response activities that executed both manually and in an automated fashion. Response activities are organized into automated and manual categories. Manual activities are analyzed for possible retirement.	Y	Xage directly provides the core Policy Enforcement Point (PEP) and Policy Decision Point (PDP) architecture required to achieve this automated orchestration capability. The Xage Fabric serves as the central PDP, managing all access policies, while its distributed Enforcement Points act as the PEPs, enforcing those policies at the asset. When a threat is detected by another tool (like a SIEM), it triggers a playbook in a SOAR platform. This playbook then uses Xage's APIs to programmatically update the policy in the PDP, and Xage instantly enforces the change such as quarantining a device or revoking user access at the PEP, providing immediate, automated incident response and remediation.
6.5.2	Implement SOAR Tools	Activity	DoD enterprise working with Organizations develops a standard set of requirements for security orchestration, automation, and response (SOAR) tooling to enable target level ZTA functions. DoD Organizations use approved requirements to procure and implement SOAR solution. Basic infrastructure integrations for future SOAR functionality is completed.	R	We are continuing to make progress in this area and aim to have a feature released soon that supports this requirement.

Pillar: Automation & Orchestration

6.5.3	Implement Playbooks	Activity	DoD organizations review all existing playbooks to identify for future automation. Existing manual and automated processes missing playbooks have playbooks developed. Playbooks are prioritized for automation to be integrated with the Automated Workflows activities covering Critical Processes. Manual processes without playbooks are authorized using a risk based methodical approach.	Y	Xage serves as a foundational tool for both the automation of playbooks and the secure authorization of manual processes. For automation, Xage's comprehensive APIs allow it to be a primary target for security playbooks developed in SOAR platforms. Automated workflows can directly call the Xage Fabric to execute critical response actions like isolating endpoints, revoking credentials, or altering access policies. For necessary manual processes that lack a playbook, Xage provides the required risk-based enforcement by enabling temporary, time-limited access with multi-factor or multi-person approval, ensuring even non-automated critical tasks are performed under a stringent zero-trust policy.
6.6	**API Standardization**	**Capability**	**DoD establishes and enforces enterprise-wide programmatic interface (e.g., API) standards; all non-compliant APIs are identified and replaced.**	G	Xage fully meets this requirement as its platform is built on an API-first architecture that uses modern, programmatic standards. The Xage Fabric utilizes standard RESTful APIs for all its functions, from policy management to device administration and reporting. This design ensures seamless interoperability with other compliant systems, such as SIEM, SOAR, and identity management tools, across the DoD enterprise. By providing a fully documented and standards-based API, Xage enables secure, programmatic integration and automation, aligning perfectly with the mandate to enforce enterprise-wide API standards.
6.6.1	Tool Compliance Analysis	Activity	Automation and Orchestration tooling and solutions are analyzed for compliance and capabilities based on the DoD Enterprise programmatic interface standard and requirements. Any additional tooling or solutions are identified to support the programmatic interface standards and requirements.	G	Xage fully meets this requirement as its platform is built on an API-first architecture that uses modern, programmatic standards. The Xage Fabric utilizes standard RESTful APIs for all its functions, from policy management to device administration and reporting. This design ensures seamless interoperability with other compliant systems, such as SIEM, SOAR, and identity management tools, across the DoD enterprise. By providing a fully documented and standards-based API, Xage enables secure, programmatic integration and automation, aligning perfectly with the mandate to enforce enterprise-wide API standards.
6.6.2	Standardized API Calls & Schemas Pt1	Activity	The DoD enterprise works with organizations to establish a programmatic interface (e.g., API) standard and requirements as needed to enable target ZTA functionalities. DoD Organizations update programmatic interfaces to the new standard and mandate newly acquired/developed tools to meet the new standard. Tools unable to meet the standard are allowed by exception using a risk based methodical approach.	G	Xage fully meets this requirement as its platform is built on an API-first architecture that uses modern, programmatic standards. The Xage Fabric utilizes standard RESTful APIs for all its functions, from policy management to device administration and reporting. This design ensures seamless interoperability with other compliant systems, such as SIEM, SOAR, and identity management tools, across the DoD enterprise. By providing a fully documented and standards-based API, Xage enables secure, programmatic integration and automation, aligning perfectly with the mandate to enforce enterprise-wide API standards.
6.6.3	Standardized API Calls & Schemas Pt2	Activity	DoD Organizations complete the migration to the new programmatic interface standard. Tools marked for decommission in the previous activity are retired and functions are migrated to modernized tools. Approved schemas are adopted based on the DoD Enterprise standard/requirements.	G	Xage fully meets this requirement as its platform is built on an API-first architecture that uses modern, programmatic standards. The Xage Fabric utilizes standard RESTful APIs for all its functions, from policy management to device administration and reporting. This design ensures seamless interoperability with other compliant systems, such as SIEM, SOAR, and identity management tools, across the DoD enterprise. By providing a fully documented and standards-based API, Xage enables secure, programmatic integration and automation, aligning perfectly with the mandate to enforce enterprise-wide API standards.
6.7	**Security Operations Center (SOC) & Incident Response (IR)**	**Capability**	**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.**	Y	Xage provides critical data and enforcement capabilities that are foundational to modern SOC operations and automated workflows. For upward visibility, the Xage Fabric provides SOC analysts with a centralized dashboard view of all managed assets, user access, and active policy enforcement status. For downward tactical implementation, Xage integrates with SOAR platforms and other automation tools via its APIs. This allows the SOC to create automated workflows where alerts from the SIEM can be enriched with Xage's identity data and trigger a SOAR playbook that automatically directs Xage to quarantine a device or revoke a user's access, streamlining response without manual intervention.
6.7.1	Workflow Enrichment Pt1	Activity	DoD Enterprise works with organizations to establish a cybersecurity incident response standard using industry best practices such as NIST. DoD Organizations utilize the enterprise standard to determine incident response workflows. External sources of enrichment are identified for future integration.	Y	Xage provides critical data and enforcement capabilities that are foundational to modern SOC operations and automated workflows. For upward visibility, the Xage Fabric provides SOC analysts with a centralized dashboard view of all managed assets, user access, and active policy enforcement status. For downward tactical implementation, Xage integrates with SOAR platforms and other automation tools via its APIs. This allows the SOC to create automated workflows where alerts from the SIEM can be enriched with Xage's identity data and trigger a SOAR playbook that automatically directs Xage to quarantine a device or revoke a user's access, streamlining response without manual intervention.

Pillar: Automation & Orchestration

6.7.2	Workflow Enrichment Pt2	Activity	DoD organizations identify and establish extended workflows for additional incident response types. Initial enrichment data sources are used for existing workflows. Additional enrichment sources are identified for future integrations.	Y	Xage provides critical data and enforcement capabilities that are foundational to modern SOC operations and automated workflows. For upward visibility, the Xage Fabric provides SOC analysts with a centralized dashboard view of all managed assets, user access, and active policy enforcement status. For downward tactical implementation, Xage integrates with SOAR platforms and other automation tools via its APIs. This allows the SOC to create automated workflows where alerts from the SIEM can be enriched with Xage's identity data and trigger a SOAR playbook that automatically directs Xage to quarantine a device or revoke a user's access, streamlining response without manual intervention.
6.7.3	Workflow Enrichment Pt3	Activity	DoD organizations use final enrichment data sources on basic and extended threat response workflows.	Y	Xage provides critical data and enforcement capabilities that are foundational to modern SOC operations and automated workflows. For upward visibility, the Xage Fabric provides SOC analysts with a centralized dashboard view of all managed assets, user access, and active policy enforcement status. For downward tactical implementation, Xage integrates with SOAR platforms and other automation tools via its APIs. This allows the SOC to create automated workflows where alerts from the SIEM can be enriched with Xage's identity data and trigger a SOAR playbook that automatically directs Xage to quarantine a device or revoke a user's access, streamlining response without manual intervention.
6.7.4	Automated Workflow	Activity	DoD organizations focus on automating Security Orchestration, Automation and Response (SOAR) functions and playbooks. Manual processes within security operations are identified and fully automated as possible. Remaining manual processes are decommissioned when possible or marked for exception using a risk based approach.	Y	Xage provides critical data and enforcement capabilities that are foundational to modern SOC operations and automated workflows. For upward visibility, the Xage Fabric provides SOC analysts with a centralized dashboard view of all managed assets, user access, and active policy enforcement status. For downward tactical implementation, Xage integrates with SOAR platforms and other automation tools via its APIs. This allows the SOC to create automated workflows where alerts from the SIEM can be enriched with Xage's identity data and trigger a SOAR playbook that automatically directs Xage to quarantine a device or revoke a user's access, streamlining response without manual intervention.

Pillar: Visibility & Analytics

ID #	Activity/Capability Name	Capability or Activity	Capability/Activity Description	Xage Alignment (G, Y, R)	An explanation on how Xage aligns
7.1	Log All Traffic (Network, Data, Apps, Users)	Capability	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.	G	Xage captures and forwards comprehensive, identity-centric logs for every user and device interaction, directly supporting this requirement. The Xage Fabric generates detailed audit logs for every access request, application use, and data transfer whether granted or denied providing critical user and device event data. These logs are exported in standardized formats like Syslog or CEF to the designated DoD log collectors or SIEM, making them immediately available to the CNDSP or SOC for the development of tailored analytics, rules, and compliance reporting.
7.1.1	Scale Considerations	Activity	DoD Organizations conduct analysis to determine current and future needs of scaling. Scaling is analyzed following common industry best practice methods and ZT Pillars. The team works with existing Business Continuity Planning (BCP) and Disaster Recovery Planning (DPR) groups to determine distributed environment needs in emergencies and as organizations grow.	G	With the ability to add or remove Xage Nodes from the fabric as more devices come on line, there are no concerns around user or device count to add to the infastructure. All XN's are created through the XM and can immedieatley forward all log information.
7.1.2	Log Parsing	Activity	DoD Organizations identify and prioritize log and flow sources (e.g., Firewalls, Endpoint Detection & Response, Active Directory, Switches, Routers, etc.) and develop a plan for collection of high priority logs first then low priority. An open industry-standard log format is agreed upon at the DoD Enterprise level with the Organizations and implemented in future procurement requirements. Existing solutions and technologies are migrated to the format on a continual basis.	G	Xage captures and forwards comprehensive, identity-centric logs for every user and device interaction, directly supporting this requirement. The Xage Fabric generates detailed audit logs for every access request, application use, and data transfer whether granted or denied providing critical user and device event data. These logs are exported in standardized formats like Syslog or CEF to the designated DoD log collectors or SIEM, making them immediately available to the CNDSP or SOC for the development of tailored analytics, rules, and compliance reporting.
7.1.3	Log Analysis	Activity	Common user and device activities are identified and prioritized based on risk. Activities deemed the most simplistic and risky have analytics created using different data sources such as logs. Trends and patterns are developed based on the analytics collected to look at activities over longer periods of time.	Y	Xage captures and forwards comprehensive, identity-centric logs for every user and device interaction, directly supporting this requirement. The Xage Fabric generates detailed audit logs for every access request, application use, and data transfer whether granted or denied providing critical user and device event data. These logs are exported in standardized formats like Syslog or CEF to the designated DoD log collectors or SIEM, making them immediately available to the CNDSP or SOC for the development of tailored analytics, rules, and compliance reporting.
7.2	Security Information and Event Management (SIEM)	Capability	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.)	G	Xage provides the foundational data and baseline enforcement necessary for advanced SIEM monitoring by the CNDSP or SOC. Xage enforces the established user and device baselines by controlling all access and then forwards a detailed, high-fidelity log of every approved and denied interaction to the SIEM. This stream of identity-centric data provides the SOC with precise ground truth of all activity. Within the SIEM, this data is used to create and refine alerts, which can be correlated against other advanced data points like cyber threat intelligence to detect and analyze sophisticated threats with high confidence.
7.2.1	Threat Alerting Pt1	Activity	DoD Organizations utilize existing Security Information and Event Management (SIEM) solution to develop basic rules and alerts for common threat events (malware, phishing, etc.) Alerts and/or rule firings are fed into the parallel "Asset ID & Alert Correlation" activity to being automation of responses.	Y	Xage provides the foundational data and baseline enforcement necessary for advanced SIEM monitoring by the CNDSP or SOC. Xage enforces the established user and device baselines by controlling all access and then forwards a detailed, high-fidelity log of every approved and denied interaction to the SIEM. This stream of identity-centric data provides the SOC with precise ground truth of all activity. Within the SIEM, this data is used to create and refine alerts, which can be correlated against other advanced data points like cyber threat intelligence to detect and analyze sophisticated threats with high confidence.
7.2.2	Threat Alerting Pt2	Activity	DoD Organizations expand threat alerting in the Security Information and Event Management (SIEM) solution to include Cyber Threat Intelligence (CTI) data feeds. Deviation and anomaly rules are developed in the SIEM to detect advanced threats.	Y	Xage provides the SIEM a stream of identity-based access logs and its anomaly alerts. This data provides a record of access attempts, which the SIEM can correlate against the CTI feeds it ingests. When the SIEM's rules detect a threat based on this data, it can trigger a response via an API call to Xage, instructing the platform to block a user or quarantine a system. This process turns the intelligence within the SIEM into enforcement actions.

Pillar: Visibility & Analytics

7.2.3	Threat Alerting Pt3	Activity	Threat Alerting is expanded to include advanced data sources such as Extended Detection & Response (XDR), User & Entity Behavior Analytics (UEBA), and User Activity Monitoring (UAM). These advanced data sources are used to develop improved anomalous and pattern activity detections.	Y	Xage sends its access logs to XDR, UEBA, and UAM platforms, which use the logs as a data source for their detection models. When one of these platforms generates an alert or updates an entity's risk score, Xage receives that information. The Xage platform then uses the information from the alert to enforce access policies, such as blocking a user or terminating a session. This process makes the detections from the external systems actionable.
7.2.4	Asset ID & Alert Correlation	Activity	DoD Organizations develop basic correlation rules using asset and alert data. Response to common threat events (e.g., malware, phishing, etc.) are automated within the Security Information and Event Management (SIEM) solution.	Y	Xage provides asset data and alert data to the SIEM through its logs. These logs are used in the SIEM's correlation rules. When a rule in the SIEM detects a threat, the SIEM can automate a response. This response includes making an API call to the Xage platform. Xage then executes an enforcement action, such as blocking the user account or isolating the asset.
7.2.5	User/Device Baselines	Activity	DoD Organizations develop user and device baseline approaches based on DoD Enterprise standards for the appropriate pillar. Attributes utilized in baselining are pulled from the enterprise wide standards developed in cross pillar activities.	G	Xage creates enforceable baselines for users and devices by applying policies based on the very attributes defined in DoD Enterprise standards. It integrates with enterprise identity systems (like Active Directory) to understand user attributes and discovers devices and their characteristics across the network. Using this information, Xage enforces granular access policies for example, allowing only a specific user role to communicate with a specific device type using a standard protocol thereby establishing a precise, enforceable baseline that aligns with cross-pillar DoD standards.
7.3	**Common Security and Risk Analytics**	**Capability**	**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.**	Y	**Xage functions as a data source for the tools used by a CNDSP or SOC. The platform generates logs for access events, user activities, and policy enforcement actions it manages. Xage forwards these logs to the SOC's central data collection tools, such as a SIEM. This process contributes to the unification of data collection. SOC analysts then use the Xage data within their platforms to examine events and behaviors.**
7.3.1	Implement Analytics Tools	Activity	DoD Organizations procure and implement basic Cyber-focused analytics tools. Analytics development is prioritized based on risk and complexity looking for easy impactful analytics first. Continued analytics development focuses on Pillar requirements to better meet reporting needs.	Y	Xage functions as a data source for the cyber analytics tools that organizations procure. The platform's logs provide structured data fields such as user, asset, location, and time. This information supports the development of initial analytics, such as detecting access from new locations or outside of standard hours. The data in Xage logs also maps to Zero Trust Pillars, including Identity, Network, and Data. Forwarding these logs to analytics tools allows organizations to develop reports and metrics aligned with Pillar requirements.
7.3.2	Establish User Baseline Behavior	Activity	Utilizing the analytics developed for users and devices in a parallel activity, baselines are established in a technical solution. These baselines are applied to an identified set of users based on risk initially and then expanded to the larger DoD Organization user base. The technical solution used is integrated with machine learning functionality to begin automation.	Y	Xage is a technical solution that natively performs these functions. The platform's machine learning functionality establishes baselines of user and device access patterns for specific assets. Policies within Xage can apply these baselines first to an identified set of users based on risk. The scope of the policy can then be expanded to the larger user base. When the machine learning detects a deviation from an established baseline, it triggers automated enforcement actions defined in the system's policies.
7.4	**User and Entity Behavior Analytics**	**Capability**	**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.**	Y	**Xage supports both the initial and mature stages of this analytics capability. For organizations at the initial stage, Xage's native machine learning engine profiles user and entity access, establishes behavioral baselines, and detects anomalies for the systems it protects. For a mature SOC or CNDSP, Xage integrates with their analytics platforms. In that model, Xage provides its logs and anomaly alerts as a data source to the SOC's tools and also functions as an enforcement point, taking direction from the analytics platform to block users or terminate sessions.**

Pillar: Visibility & Analytics

7.4.1	Baseline & Profiling Pt1	Activity	Utilizing the analytics developed for users and devices in a parallel activity, common profiles are created for typical user and device types. Analytics taken from baselining are updated to look at larger containers, profiles.	Y	While Xage is not the analytics platform itself, it provides the essential mechanism for creating and enforcing the common profiles for users and devices mentioned in the requirement. Xage's core functionality is centered on creating granular, role-based access control policies that function as "common profiles" for typical user and device types (e.g., 'maintenance technician,' 'HVAC controller,' 'flow meter'). Instead of managing permissions for each individual entity, administrators define access rights for these profiles. The Xage Fabric then enforces these policies across the infrastructure, and its detailed logs provide the analytics platform with precise data on how these profiles are being used. This allows the analytics engine to shift its focus from baselining individual entities to monitoring the collective behavior of these larger container profiles, enabling more efficient and scalable anomaly detection based on group norms.
7.4.2	Baseline & Profiling Pt2	Activity	DoD Organizations expand baselines and profiles to include unmanaged and non-standard device types including Internet of Things (IoT) and Operational Technology (OT) through data output monitoring. These devices are again profiled based on standardized attributes and use cases. Analytics are updated to consider the new baselines and profiles accordingly enabling further detections and response. Specific risky users and devices are automatically prioritized for increased monitoring based on risk. Detection and response are integrated with cross pillar functionalities.	G	Xage is designed to extend baselines to IoT and OT devices. The platform establishes these baselines by monitoring access requests and data flows through its enforcement points. This process creates a standardized profile of device activity based on attributes and use cases. The platform's analytics engine uses these profiles to detect anomalies. Policy rules can automatically apply increased data monitoring to specific users or devices based on risk. Because Xage ties user identity to device access over the network, its detection and response functions are integrated across the Identity, Device, and Network pillars.
7.4.3	UEBA Baseline Support Pt 1	Activity	User & Entity Behavior Analytics (UEBA) within DoD Organizations expands monitoring to advanced analytics such as Machine Learning (ML). These results are in turn reviewed and fed back into the ML algorithms to improve detection and response.	Y	Xage provides the foundational data on user and device interactions required by User & Entity Behavior Analytics (UEBA) platforms. By enforcing granular, identity-based access control down to the individual asset, Xage generates a high-fidelity audit trail of all access requests, commands, and file transfers, including policy violations, which serves as the primary input for machine learning algorithms within a separate UEBA tool. While Xage itself does not perform the ML-based behavioral analytics, it feeds this critical, contextualized data to dedicated DoD analytics platforms to build dynamic baselines of normal behavior, detect sophisticated anomalies, and, through API integration, can receive feedback to automatically adjust user permissions or terminate sessions in response to threats identified by the UEBA's ML models.
7.4.4	UEBA Baseline Support Pt 2	Activity	User & Entity Behavior Analytics (UEBA) within DoD Organizations completes it expansion by using traditional and machine learning (ML) based results to be fed into Artificial Intelligence (AI) algorithms. Initially AI based detections are supervised but ultimately using advanced techniques such as neural networks, UEBA operators are not part of the learning process	Y	Xage provides the essential input and action framework for the DoD's autonomous AI security model. It feeds the high-fidelity user and asset interaction data required to train AI algorithms from their initial supervised state to a fully unsupervised one. As the AI matures, it leverages Xage's APIs to directly enforce its decisions, automatically updating policies or blocking threats, thus closing the security loop without the need for human operator intervention.
7.5	**Threat Intelligence Integration**	**Capability**	**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.**	Y	**The Xage Fabric generates detailed audit logs for every access attempt successful or denied providing the CNDSP or SOC with precise data on who (user or machine), is trying to access what (specific asset or application), when, and how. This granular log data is forwarded to the SIEM, where it is fused with external threat intelligence feeds. By correlating Xage's ground-truth data on internal access patterns with known adversary TTPs, motivations, and compromised identities from threat streams, the SOC can rapidly identify and respond to attacks that leverage known threat actor characteristics against critical infrastructure.**

Pillar: Visibility & Analytics

7.5.1	Cyber Threat Intelligence Program Pt1	Activity	The DoD Enterprise works with the Organizations to develop and Cyber Threat Intelligence (CTI) program policy, standard and process. Organizations utilize this documentation to develop organizational CTI teams with key mission/task stakeholders. CTI Teams integrate common feeds of data with the Security Information and Event Management (SIEM) for improved alerting and response. Integrations with Device and Network enforcement points (e.g., Firewalls, Endpoint Security Suites, etc.) are created to conduct basic monitoring of CTI driven data.	Y	The Xage Fabric generates detailed audit logs for every access attempt successful or denied providing the CNDSP or SOC with precise data on who (user or machine), is trying to access what (specific asset or application), when, and how. This granular log data is forwarded to the SIEM, where it is fused with external threat intelligence feeds. By correlating Xage's ground-truth data on internal access patterns with known adversary TTPs, motivations, and compromised identities from threat streams, the SOC can rapidly identify and respond to attacks that leverage known threat actor characteristics against critical infrastructure.
7.5.2	Cyber Threat Intelligence Program Pt2	Activity	DoD Organizations expand their Cyber Threat Intelligence (CTI) teams to include new stakeholders as appropriate. Authenticated, private and controlled CTI data feeds are integrated into Security Information and Event Management (SIEM) and enforcement points from the Device, User, Network and Data pillars.	Y	The Xage Fabric generates detailed audit logs for every access attempt successful or denied providing the CNDSP or SOC with precise data on who (user or machine), is trying to access what (specific asset or application), when, and how. This granular log data is forwarded to the SIEM, where it is fused with external threat intelligence feeds. By correlating Xage's ground-truth data on internal access patterns with known adversary TTPs, motivations, and compromised identities from threat streams, the SOC can rapidly identify and respond to attacks that leverage known threat actor characteristics against critical infrastructure.
7.6	**Automated Dynamic Policies**	**Capability**	**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.**	Y	**While Xage is not the ML or AI decision engine itself, it serves as the essential action and enforcement layer for it.** **Xage's API-driven architecture allows DoD ML and AI solutions to translate their findings into immediate, automated action. Based on continuous risk and confidence scores generated by the AI, that external platform can make an API call to Xage to dynamically update a user or device's security profile, instantly changing access rights, enforcing MFA, or quarantining a system by revoking all its privileges. For automated configuration and patch management, Xage integrates with the designated management tools, ensuring that only the authorized, automated system can gain the necessary privileged access to deploy a patch or update a device's configuration, enforcing a zero-trust, machine-to-machine workflow.**
7.6.1	AI-enabled Network Access	Activity	DoD Organizations utilize the SDN Infrastructure and Enterprise Security Profiles to enable Artificial Intelligence (AI)/Machine Learning (ML) driven network access. Analytics from previous activities is used to teach the AI/ML algorithms improving decision making.	Y	While Xage is not the ML or AI decision engine itself, it serves as the essential action and enforcement layer for it. Xage's API-driven architecture allows DoD ML and AI solutions to translate their findings into immediate, automated action. Based on continuous risk and confidence scores generated by the AI, that external platform can make an API call to Xage to dynamically update a user or device's security profile, instantly changing access rights, enforcing MFA, or quarantining a system by revoking all its privileges. For automated configuration and patch management, Xage integrates with the designated management tools, ensuring that only the authorized, automated system can gain the necessary privileged access to deploy a patch or update a device's configuration, enforcing a zero-trust, machine-to-machine workflow.
7.6.2	AI-enabled Dynamic Access Control	Activity	DoD Organizations utilize previous rule based dynamic access to teach Artificial Intelligence (AI)/Machine Learning (ML) algorithms to make access decision to various resources. The "AI-enabled Network Access" activity algorithms are updated to enable broader decision making to all DAAS.	Y	While Xage is not the ML or AI decision engine itself, it serves as the essential action and enforcement layer for it. Xage's API-driven architecture allows DoD ML and AI solutions to translate their findings into immediate, automated action. Based on continuous risk and confidence scores generated by the AI, that external platform can make an API call to Xage to dynamically update a user or device's security profile, instantly changing access rights, enforcing MFA, or quarantining a system by revoking all its privileges. For automated configuration and patch management, Xage integrates with the designated management tools, ensuring that only the authorized, automated system can gain the necessary privileged access to deploy a patch or update a device's configuration, enforcing a zero-trust, machine-to-machine workflow.