xage
GOVERNMENT

Xage Delivers Comprehensive Zero Trust Coverage for DoW OT

Mapping Xage Capabilities to Department of War Zero Trust Activities and Outcomes

Zero Trust for Operational Technology (OT) is no longer just a conceptual framework. It is an active mandate rapidly reshaping cybersecurity expectations across the defense industrial base and national security infrastructure. The Department of War's Zero Trust guidance for OT, "Zero Trust for Operational Technology Activities and Outcomes" (Nov. 18, 2025) reflects a decisive shift toward protection-first security models, with aggressive timelines that demand practical, deployable capabilities capable of operating in complex, critical environments.

OT Zero Trust is fundamentally preventative. While important, detection capabilities are secondary to prevention and defense in these critical environments. OT Zero Trust prioritizes identity-based access control, segmentation, privileged access management, continuous authorization and monitoring, enforcement, and operational resilience. These priorities align directly with Xage's platform, which was purpose-built to secure critical environments where safety, uptime, and legacy system compatibility are non-negotiable. Xage focuses on stopping unauthorized actions before they occur, preventing lateral movement, and building defense-in-depth, rather than on post-compromise reactive actions. This distinction is essential for OT and defense environments.

Scope of Applicability

The guidance applies to Department of War–owned OT environments and control systems up to the point of demarcation with Weapon Systems and Defense Critical Infrastructure. It includes OT systems that enable and support missions, such as facility controls, power, water, transportation, logistics, manufacturing, and life safety systems. The guidance does not cover internal Weapon System or DCI components, such as targeting or firing systems, which will be addressed in separate guidance.

Mapping Xage to DoW Zero Trust Activities and Outcomes

This whitepaper maps Xage's capabilities directly to the Department of War's Zero Trust for OT activities and outcomes, demonstrating comprehensive coverage across all Zero Trust pillars. In particular, Xage fully covers user and network pillars with major coverage for the remaining pillars—including devices, data, applications & workloads, automation & orchestration, and visibility & analytics. Xage delivers solutions through a unified security fabric designed specifically for OT. Unlike IT-centric tools retrofitted for industrial use, Xage operates natively across enterprise IT, operational IT, and process control systems, covering all environments while also preserving separation and defense-in-depth.

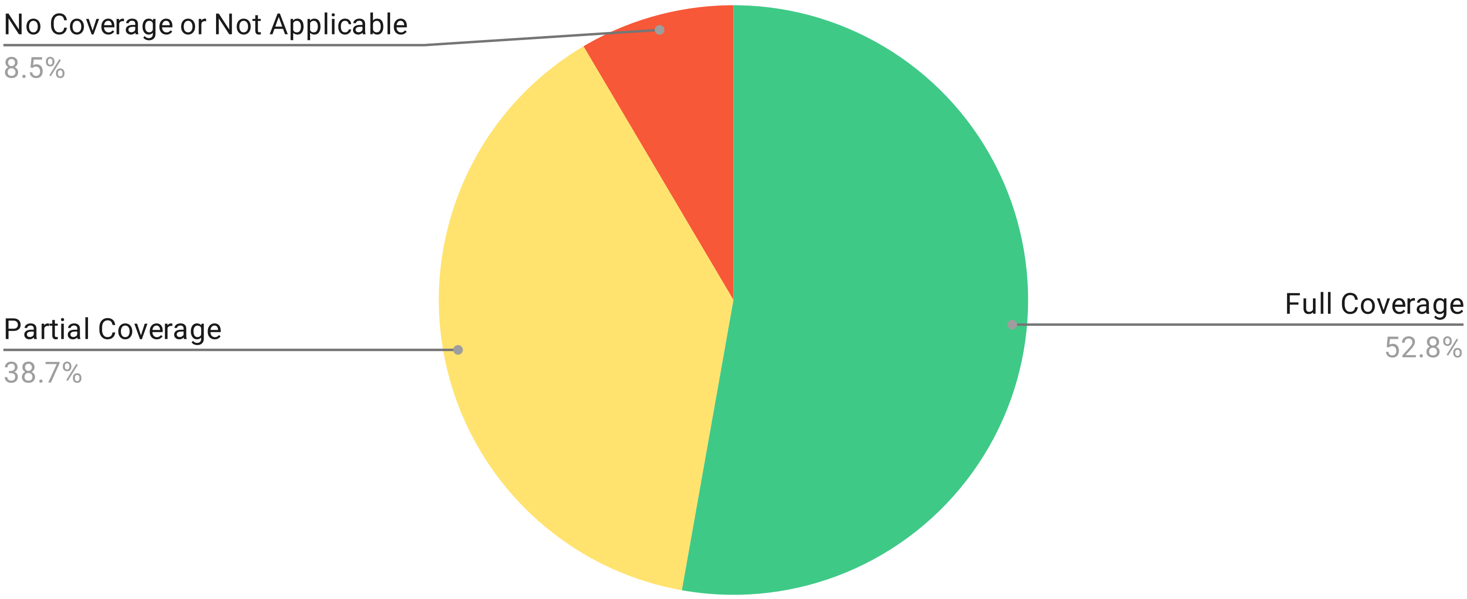
A key differentiator of Xage is its ability to deliver Zero Trust as an overlay without requiring replacement or modernization of legacy OT assets. Xage enforces access and protection controls across heterogeneous environments, including brownfield systems, remote sites, and air-gapped or intermittently connected operations. This approach enables defense organizations to meet Zero Trust objectives rapidly while preserving existing investments and operational stability.

Xage uniquely unifies secure access, privileged access management, segmentation, data protection, and AI security into a single distributed fabric. Enforcement occurs locally close to assets to maintain safety and uptime, while policy is centrally defined and consistently applied across bases, facilities, and geographically dispersed operations. This architecture makes Zero Trust operationally practical at scale, supporting both centralized governance and distributed execution.

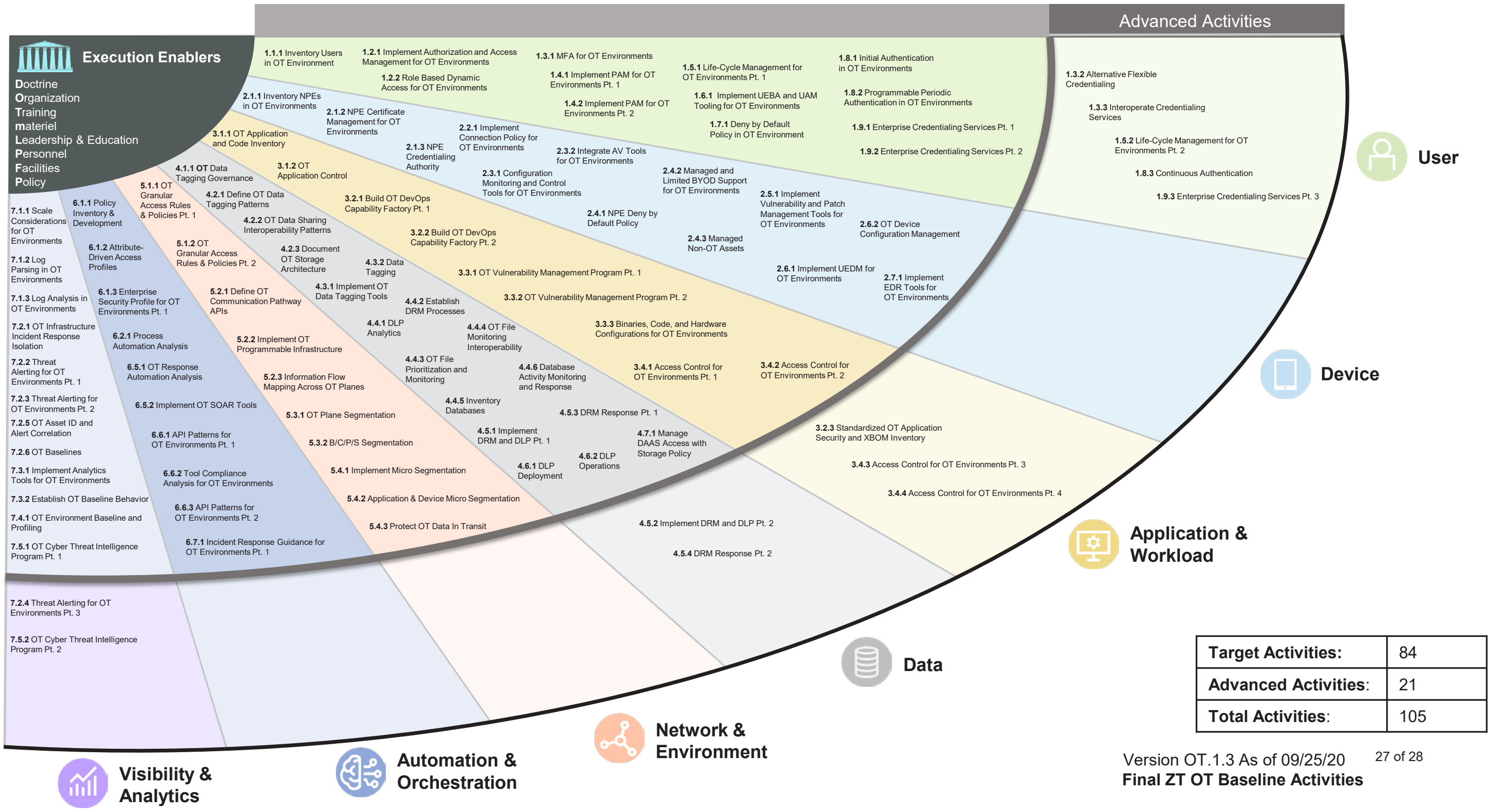
In addition, Xage provides full identity-enabled visibility, including detailed logging, session recording, behavioral telemetry, and command-level insights. This telemetry strengthens analytics, user and entity behavior analytics (UEBA), security information and event management (SEIM), and cyber threat intelligence (CTI) programs, while also enabling adaptive, context-aware access decisions that evolve with risk and operational conditions.

Aligned with federal and defense Zero Trust architectures and reinforced by Xage's participation in CISA's Joint Cyber Defense Collaborative (JCDC), Xage offers a credible, OT-native path to achieving the Department of War's Zero Trust objectives. The capability mapping that follows illustrates how Xage translates Zero Trust principles into enforceable controls that protect mission systems today, not just in theory, but in real-world operational environments.

Activities and Functions Supported



Zero Trust Fan Chart for Operational Technologies


Advanced Activities
Execution Enablers
Doctrine
Organization
Training
materiel
Leadership & Education
Personnel
Facilities
Policy
1.1.1 Inventory Users in OT Environment
1.2.1 Implement Authorization and Access Management for OT Environments
1.2.2 Role Based Dynamic Access for OT Environments
1.3.1 MFA for OT Environments
1.4.1 Implement PAM for OT Environments Pt. 1
1.4.2 Implement PAM for OT Environments Pt. 2
1.5.1 Life-Cycle Management for OT Environments Pt. 1
1.6.1 Implement UEBA and UAM Tooling for OT Environments
1.7.1 Deny by Default Policy in OT Environment
1.8.1 Initial Authentication in OT Environments
1.8.2 Programmable Periodic Authentication in OT Environments
1.9.1 Enterprise Credentialing Services Pt. 1
1.9.2 Enterprise Credentialing Services Pt. 2
1.3.2 Alternative Flexible Credentialing
1.3.3 Interoperate Credentialing Services
1.5.2 Life-Cycle Management for OT Environments Pt. 2
1.8.3 Continuous Authentication
1.9.3 Enterprise Credentialing Services Pt. 3
2.1.1 Inventory NPEs in OT Environments
2.1.2 NPE Certificate Management for OT Environments
2.1.3 NPE Credentialing Authority
2.2.1 Implement Connection Policy for OT Environments
2.3.1 Configuration Monitoring and Control Tools for OT Environments
2.3.2 Integrate AV Tools for OT Environments
2.4.1 NPE Deny by Default Policy
2.4.2 Managed and Limited BYOD Support for OT Environments
2.4.3 Managed Non-OT Assets
2.5.1 Implement Vulnerability and Patch Management Tools for OT Environments
2.6.1 Implement UEDM for OT Environments
2.6.2 OT Device Configuration Management
2.7.1 Implement EDR Tools for OT Environments
3.1.1 OT Application and Code Inventory
3.1.2 OT Application Control
3.2.1 Build OT DevOps Capability Factory Pt. 1
3.2.2 Build OT DevOps Capability Factory Pt. 2
3.3.1 OT Vulnerability Management Program Pt. 1
3.3.2 OT Vulnerability Management Program Pt. 2
3.3.3 Binaries, Code, and Hardware Configurations for OT Environments
3.4.1 Access Control for OT Environments Pt. 1
3.4.2 Access Control for OT Environments Pt. 2
3.2.3 Standardized OT Application Security and XBOM Inventory
3.4.3 Access Control for OT Environments Pt. 3
3.4.4 Access Control for OT Environments Pt. 4
4.1.1 OT Data Tagging Governance
4.2.1 Define OT Data Tagging Patterns
4.2.2 OT Data Sharing Interoperability Patterns
4.2.3 Document OT Storage Architecture
4.3.1 Implement OT Data Tagging Tools
4.3.2 Data Tagging
4.4.1 DLP Analytics
4.4.2 Establish DRM Processes
4.4.3 OT File Prioritization and Monitoring
4.4.4 OT File Monitoring Interoperability
4.4.5 Inventory Databases
4.4.6 Database Activity Monitoring and Response
4.5.1 Implement DRM and DLP Pt. 1
4.5.3 DRM Response Pt. 1
4.6.1 DLP Deployment
4.6.2 DLP Operations
4.7.1 Manage DAAS Access with Storage Policy
4.5.2 Implement DRM and DLP Pt. 2
4.5.4 DRM Response Pt. 2
5.1.1 OT Granular Access Rules & Policies Pt. 1
5.1.2 OT Granular Access Rules & Policies Pt. 2
5.2.1 Define OT Communication Pathway APIs
5.2.2 Implement OT Programmable Infrastructure
5.2.3 Information Flow Mapping Across OT Planes
5.3.1 OT Plane Segmentation
5.3.2 B/C/P/S Segmentation
5.4.1 Implement Micro Segmentation
5.4.2 Application & Device Micro Segmentation
5.4.3 Protect OT Data In Transit
6.1.1 Policy Inventory & Development
6.1.2 Attribute-Driven Access Profiles
6.1.3 Enterprise Security Profile for OT Environments Pt. 1
6.2.1 Process Automation Analysis
6.5.1 OT Response Automation Analysis
6.5.2 Implement OT SOAR Tools
6.6.1 API Patterns for OT Environments Pt. 1
6.6.2 Tool Compliance Analysis for OT Environments
6.6.3 API Patterns for OT Environments Pt. 2
6.7.1 Incident Response Guidance for OT Environments Pt. 1
7.1.1 Scale Considerations for OT Environments
7.1.2 Log Parsing in OT Environments
7.1.3 Log Analysis in OT Environments
7.2.1 OT Infrastructure Incident Response Isolation
7.2.2 Threat Alerting for OT Environments Pt. 1
7.2.3 Threat Alerting for OT Environments Pt. 2
7.2.5 OT Asset ID and Alert Correlation
7.2.6 OT Baselines
7.3.1 Implement Analytics Tools for OT Environments
7.3.2 Establish OT Baseline Behavior
7.4.1 OT Environment Baseline and Profiling
7.5.1 OT Cyber Threat Intelligence Program Pt. 1
7.2.4 Threat Alerting for OT Environments Pt. 3
7.5.2 OT Cyber Threat Intelligence Program Pt. 2
User
Device
Application & Workload
Data
Network & Environment
Automation & Orchestration
Visibility & Analytics

Target Activities:	84
Advanced Activities:	21
Total Activities:	105

Version OT.1.3 As of 09/25/20

27 of 28

Final ZT OT Baseline Activities

Xage Capability Mapping to Zero Trust for OT Activities and Outcomes

OT Activity ID	OT Activity Name	Pillar	Activity Type	OT Activity Description	OT Activity Outcomes	Supported	Xage Capability
1.1.1.OT	Inventory Users in OT Environment	User	Target	DoW Components establish and update a user inventory within the OT environment, manually if necessary, preparing for an automated approach in later stages. Privileged OT accounts will be identified. Both standard and privileged accounts for applications and systems with local identity stores will be identified for future migration and/or decommissioning. Shared group accounts, must-run accounts, or service OT accounts must be identified for future migration to inventory and/or decommissioning.	1. Identified and documented inventory of accounts across both the Operational IT and Process Control environments 2. All applications and systems with local identity stores have been identified 3. Local user, local privileged, shared, must-run, and service OT accounts have been identified for migration and/or decommissioning.	Y	Xage automatically discovers, classifies, and inventories local, privileged, shared, and service accounts across systems, applications, machines, and identity stores within the OT environment. Its distributed architecture ensures that accounts and assets in remote or isolated locations are fully captured, eliminating blind spots. This comprehensive visibility supports the identification of privileged OT accounts, shared or must-run accounts, and other local identities that need to be migrated, managed, or decommissioned as part of a mature Zero Trust program
1.2.1.OT	Implement Authorization and Access Management for OT Environments	User	Target	DoW Components implement OT or Enterprise ICAM governance, or other authorized credentialing services, in accordance with applicable policies and regulations. The authorized credentialing service establishes a set of attributes for authentication and authorization within the OT environment. Attributes are integrated with the 2.1.3.OT activity process for a complete IdP process. The OT credentialing service is enabled for adding and updating attributes for users. OT privileged access and authorization are approved and tailored as specified by the roles. For OT systems on which it is technically capable, any shared group, must-run, and service OT accounts are migrated to proper identities or are decommissioned. Any OT systems identified that cannot be migrated and/or decommisioned are tracked using a risk-based methodology for future migration and/or decommision.	1. Authorized Credentialing service is implemented for the Operational IT environment 2. Attributes for authentication and authorization of users are defined 3. OT credentialing service enabled to add and update attributes 4. OT privileged accounts are authorized based on roles and attributes 5. Shared group, must-run, and service OT accounts have been migrated and/or decommissioned.	Y	Xage enables granular governance of identities, accounts, credentials, and policies. Xage provides ability to centrally manage policies for user to machine and account access and enforce them across a distributed deployment footprint. With Xage, users can utilize managed identities with ABAC and MFA instead of local/shared accounts when accessing assets such as SCADA systems, PLCs, RTUs which do not natively support managed accounts or ABAC. Additionally, Xage integrates with existing IdP across multiple networks and layers to extend managed identity based access to isolated OT assets. Xage provides audit logs for every interaction (user <-> device/app, device <-> device) and access control utilizes just-in-time and just-enough access principles.
1.2.2.OT	Role Based Dynamic Access for OT Environments	User	Target	DoW Components develop rules, both technical and procedural, for remote and third-party access into the OT environment. All users must have strict role-based access controls prior to access or connection into the OT environment. Remote and third-party access should be limited to the account of least privilege required to perform work. OT privileged accounts required for operations are accessed through the Authorized Credentialing Service. Identify high-privileged accounts and require these use dynamic access control.	1. Rules are defined for third party and remote access into the OT environment 2. Role-based enforcement of user access to the environment; Authorized Credentialing service required for Privileged accounts 3. Identified High-privileged accounts and enforced using dynamic access.	Y	Xage provides granular least privilged access to OT assets based on role, policy, and attributes. Xage Secure Remote Access utilized a multi-network-hop approach such that there is never a direct connection to the OT assets. All access is proxied and relayed one-network-hop at a time reaching isolated assets without exposing them to external connections. Multiple network layers of isolation are supported. Each Xage Nodes provides session termination and protocol breaks eliminating direct connections. Insecure protocols such as RDP, VNC, SSH, Telnet, SMB and idustrial protcols are terminated inside the isolated networks and all interactions are emulated and delivered through HTTPs. Indisvidual users only see assets they are allowed to inetract with per policy, just-in-time, and just-enough access. This capability applies to both internal users as well as 3rd parties.
1.3.1.OT	MFA for OT Environments	User	Target	DoW Components enable or integrate the Authorized Credentialing Service with Multifactor Authentication (MFA), or an approved alternative authoritative credentialing solution, either technical or procedural, for access within the OT Environment.	1. MFA, or approved authoritative credentialing solution, is implemented with the Authorized Credentialing Service for access.	Y	Xage provides multiple MFA methods including phishing-resistant MFA with full offline support as well as multiple CAC methods including CAC Passthrough to any asset in the OT environment including assets such as PLCs and RTUs which do not natively support MFA. Xage deploys as an overlay eliminating the need to rip and replace or requiring any asset or network changes.

1.3.2.OT	Alternative Flexible Credentialing	User	Advanced	DoW Components shall support alternative methods of authentication that can be managed using a self-service approach. The solution will be approved and implemented following DoW Enterprise policy recommendations and guidance.	1. Authoritative Credentialing service provides user self-service alternative authentication solutions 2. DoW Component provides solutions approved per policy.	Y	Xage supports alternative flexible credentialing services including built-in capability to act as an IdP, ability to extend IdP capability to isolated environments, and layer multiple IdP services into workload requiring verification at every step as user traverses to more sensitive assets (enterprise, network, workstation, sensitive asset). Self-service methods for enrolling accounts and requesting access are provided as well.
1.3.3.OT	Interoperate Credentialing Services	User	Advanced	DoW Component Authentication solution is extended to interoperate with DoW Approved Credentialing services.	1. DoW Component authentication solution interoperates with all approved credentialing services.	Y	Xage integrates with multiple credential services and provides ability to layer credential services as well. Supported services include LDAP, SAML, CAC cards, CAC Passthrough, FIDO2 with offline support to any application, machine, or device.
1.4.1.OT	Implement PAM for OT Environments Pt. 1	User	Target	DoW Components procure and implement an OT Privileged Access Management (PAM) solution that supports all critical privileged use cases, as appropriate in the OT environment. Integration points for applications, services, and/or devices are identified to determine the status of support for the PAM solution. Applications, services, and/or devices that are able to integrate with the PAM solution are transitioned to using the solution.	1. OT PAM solution implemented 2. Integration points with appropriate applications, services, and devices are identified to support interoperability across the environment 3. Applications, services, devices that can be readily integrated with the PAM solution are integrated.	Y	Xage Extended Privileged Access Management provides management of privileged identities, accounts, entitlements, and credetials with granular session management and recording across a broad set of assets in enteprise and OT environments. Xage provides an easy-to-deploy and management solution utilizes a modern software stack that delivers value from day one.
1.4.2.OT	Implement PAM for OT Environments Pt. 2	User	Target	DoW Components extend integrations with the OT PAM Solution to all use cases, inclusive of all critical use cases. Applications, services, and devices that cannot integrate with the PAM solution shall be managed in a risk-based methodical approach to be migrated and/or decommissioned where operationally possible in the OT Environment.	1. OT PAM solution extended for all use cases 2. Applications, services, and devices that are not integrated with the OT PAM solution are migrated and/or decommissioned.	Y	Xage XPAM can integrate with any asset (application, device, machine) utilzing the extensible connector framework with extensive collection of connectors. Furthermore, Xage provides ability to manage priviledged access to assets that do not natively support credentials or roles such as PLCs and RTUs. Xage provides overlay enforcement points that control access to these assets based on identity of the users utilzing managed idenities and polciies with MFA. Enabling customers to preserve capital investments in OT assets.
1.5.1.OT	Life-Cycle Management for OT Environments Pt. 1	User	Target	DoW Components develop and document an Identity Life-Cycle Management (ILM) process for the OT Environment. The process is implemented for all users that access, connect, and operate with the OT Environment.	1. OT Environment Identity Life-Cycle Management process developed, documented, and implemented.	Y	Xage provides the workflows and technical controls for Idenitity Life Cycle management for OT environments.
1.5.2.OT	Life-Cycle Management for OT Environments Pt. 2	User	Advanced	DoW Components works with the DoW Enterprise to review and align the OT Environment ILM process with existing ILM processes, policies, and standards. Exceptions are identified and are managed in a risk-based methodical approach.	1. Standardized ILM processes and policies for OT environments.	Y	Xage provides the workflows and technical controls for Idenitity Life Cycle management for OT environments.
1.6.1.OT	Implement User & Entity Behavior Activity (UEBA) and User Activity Monitoring (UAM) Tooling for OT Environments	User	Target	DoW Components procure and implement UEBA and UAM solutions that are designed specifically for OT environments for all users, PEs and NPEs, as appropriate. UEBA and UAM solutions are integrated with the Authorized Credentialing Service and configured actions prioritize safety, reliability, and resilience within the OT environment.	1. UEBA and UAM functionality is implemented for all users, PEs and NPEs, as appropriate.	Y	Xage provides OT-purpose-built User Activity Monitoring, adaptive access control, and high-fidelity telemetry for UEBA across users, privileged entities, and non-person entities. All access is brokered through Xage and tied to the Authorized Credentialing Service, ensuring every action is authenticated, authorized, and monitored. Xage evaluates contextual factors such as role, asset sensitivity, and session behavior as well as input from UEBA tools to dynamically adjust privileges or restrict sessions when risk increases, all without disrupting OT operations.

1.7.1.OT	Deny by Default Policy in OT Environments	User	Target	DoW Components conduct a comprehensive review of all user accounts and their assigned permissions, applying the principle of least privilege to revoke unnecessary access rights while maintaining the safety and reliability of OT processes. Identify and decommission static privileged accounts where possible, or reduce their permissions to the minimum required. Automate audit logging and governance processes to continuously monitor access and prepare for the implementation of more granular, attribute-based or dynamic access control mechanisms.	1. Default permission levels have been significantly reduced, thorough audit of identity and group usage with revocation of unnecessary permissions 2. Auditing process has been automated where possible 3. Static privileged users decommissioned or had permissions reduced.	Y	Xage identity-centric access fabric centralizes control of human and machine accounts, brokers all privileged operations, and replaces shared or static credentials with just-in-time, role and attribute-based access aligned to operational safety. Xage automatically logs every access attempt and action, providing continuous auditability and governance while supporting “deny-by-default” policies that restrict access unless explicitly authorized.
1.8.1.OT	Initial Authentication in OT Environments	User	Target	DoW Components implement authentication processes to authenticate users at the start of every session in the Operational IT environment, in the Enterprise IT environment when it interoperates with the OT environment, and in the Process Control environment via technical or procedural means, as appropriate.	1. Authentication of users is implemented across applications per session.	Y	Xage enforces strong, identity-based authentication at every session start across Operational IT, Enterprise IT, and Process Control environments, even when these domains operate with separate identity providers. Xage’s unique multi-network-hop access architecture creates layered authentication and isolation at each boundary ensuring users, privileged entities, and services must re-authenticate as they move between network zones, assets, or protocols. This design enables multiple tiers of verification without exposing OT systems directly, while supporting different IdPs where required. By brokering each hop and enforcing identity checks at every stage, Xage maintains strict separation of environments, prevents unauthorized lateral movement, and ensures that authentication remains consistent, resilient, and aligned with OT safety and reliability requirements.
1.8.2.OT	Programmable Periodic Authentication in OT Environments	User	Target	DoW Components enable programmable periodic authentication requirements in the Operational IT environment, in the Enterprise IT environment when it interoperates with the OT environment, and in the Process Control environment, as appropriate on a session basis. Alternative mitigating controls, technical or procedural, must be deployed and documented when OT devices do not support periodic authentication.	1. Programmable periodic authentication of users is implemented multiple times per session 2. Alternative mitigating controls are deployed for OT devices that do not support periodic authentication.	P	Xage natively delivers a continuous authentication model that fulfills the intent of this requirement. Furthermore, Xage enables these continous authetication to assets that not natively support access control such as OT PLCs and RTUs utilizing a compensating methods such as proxy and filtering servicies vis Xage Nodes and Xage Enforcement Points. The platform enforces ongoing verification throughout user sessions using multiple adaptive controls, aligning with DoD zero- trust principles. While Xage currently does not prompt additional re-authentication at fixed intervals, it can be configured to require step-up authentication through various triggers such as access to a particular site, access through to an additional layer of security separation, or access to an digital compartment.
1.8.3.OT	Continuous Authentication	User	Advanced	DoW Components monitor transaction-based authentications for Policy Violations. Any violations are escalated for response to the incident response process.	1. Transaction authentication monitoring detects Policy Violations and escalated for action.	Y	Xage continuously monitors and enforces transaction-level authentication and authorization throughout every OT session. Because all access flows through Xage’s nodes which act as control points, each command, request, or access operation is evaluated against policy in real time, enabling immediate detection of policy violations such as unauthorized commands, off-hours access, or privilege escalation attempts. When a violation occurs, Xage can automatically blockas access and generates precise, identity-linked logs that feed directly into the organization’s incident response process. This ensures that organizayion are protected against policy violations and potential policy breaches are identified quickly, escalated appropriately, and responded to in a way that protects OT safety, reliability, and mission continuity.

1.9.1.OT	Enterprise Credentialing Services Pt. 1	User	Target	The DoW Enterprise works with DoW Components to implement DoW approved Credentialing Services in a centralized and/or federated fashion in the Operational IT environment, in the Enterprise IT environment when it interoperates with the OT environment, and in the Process Control environment, as appropriate. DoW Components credentialing services interoperate with the DoW Enterprise, while also ensuring all risks involving communications between Process Control and Operational IT environments are mitigated beforehand. DoW Component local credentialing solutions are identified for future migration and decommissioning.	1. DoW Component implements approved Credentialing Services in the OT environment 2. Component Credentialing Service interoperates with DoW Enterprise approved Credentialing Authority when possible 3. Local Credentialing solutions are identified for future migration and decommissioning.	Y	Xage enables DoW Components to implement centralized or federated credentialing services across Operational IT, Enterprise IT, and Process Control environments while maintaining the security and separation required in OT. Xage integrates with multiple credential sources, including separate IdPs utilizing LDAP or SAML, while centralizing policy management and distributing enforcement to the edge, ensuring that authentication occurs at the correct layer for each environment. As interactions move between domains or toward more sensitive OT assets, Xage re-authenticates users and services to maintain strict trust boundaries and prevent unintended exposure. This layered credential mediation reduces risks associated with cross-environment communication and allows existing local credentialing solutions to operate safely under unified Zero Trust controls
1.9.2.OT	Enterprise Credentialing Services Pt. 2	User	Target	DoW Component local credentialing solution is decommissioned and users are migrated to the DoW Approved Credentialing Authority as appropriate. All systems are assessed for compliance with this directive. Systems unable to comply due to technical or operational constraints, including Stand-Alone systems, where migration may be delayed due to inherent limitations, are subject to a documented risk assessment process to be migrated and decommissioned in the future, and compensating controls are implemented to maintain equivalent security posture. Any users that are in violation are escalated for review and remediated.	1. Local Credentialing is decommissioned and migrated to DoW Approved solution 2. Users unable to migrate are escalated and remediated.	Y	Xage provides compensating controls to enable credential authority services to assets that have inherent limitations such as many of the OT automation assets (e.g. PLCs and RTUs). Xage provides the ability to use managed identities, credentials, and zero-trust policies with MFA on any type of an asset including ones deep in isolated IT environments.
1.9.3.OT	Enterprise Credentialing Services Pt. 3	User	Advanced	DoW Components shall apply authentication from DoW Approved Credentialing Authority to all OT Assets.	1. Authentication from a DoW approved Credentialing Authority has been applied to all OT Assets, enabling interoperable access across all OT componentry.	Y	Xage enables Approved Credential Authority based authentication to any asset including application, machines, and devices whether legacy or new utilzing multiple methods and where needed compensating controls such as proxy and filtering.
2.1.1.OT	Inventory NPEs in OT Environment	Device	Target	DoW Components develop a centralized inventory for NPEs in the Operational IT and Process Control environments. Existing inventories are identified and manual and/or passive discovery-based automated solutions shall be used to update the centralized inventory. Automated inventories must be manually verified and audited periodically for accuracy as new equipment is deployed in the environment.	1. DoW Components have developed a centralized inventory of NPE, incorporating existing inventories through manual and/or passive discovery-based automated solutions. 2. Inventories are manually validated and audited periodically.	Y	Xage enables DoW Components to build and maintain a centralized inventory of NPEs across Operational IT and Process Control environments by providing passive asset discovery, interaction mapping, and account identification capabilities. Xage can automatically detect OT devices, their communication patterns, and their associated machine or service accounts without disrupting operations, creating a continuously refreshed view of the environment. This passive discovery supports and accelerates the creation of a unified NPE inventory, while still allowing Components to manually verify and audit entries as required for accuracy.

2.1.2.OT	NPE Certificate Management for OT Environment	Device	Target	DoW Components utilize the Public Key Infrastructure (PKI) solution, or DoW approved Credentialing Authority, to deploy X.509 certificates to all supported and managed NPEs in the Operational IT environment. NPEs within the Process Control environment supporting X.509 certificates are assigned. NPEs incapable are marked for retirement or excepted using a risk based methodical approach. In addition, break-glass mechanisms are implemented to revert system to non-secure OT protocols in the event of mission critical requirement. Break-glass mechanisms must have mitigation controls in place to prevent misuse or exploitation.	1. NPEs are managed via available PKI/IdP solutions, where possible 2. DoW Components have established break-glass mechanisms to revert Process Control environment NPEs to utilize non-secure OT protocols in the event of mission critical requirements.	P	Xage enables DoW Components to meet this requirement by acting as an identity proxy for OT assets and NPEs that cannot natively support X.509 certificates. Through its fabric-based architecture, Xage provides certificate-backed authentication and overlay encryption on behalf of these constrained devices, securing their communications without requiring hardware or firmware changes. Xage also supports controlled transitions between encrypted and unencrypted modes to satisfy break-glass operational needs, with mitigation controls such as policy gating, session logging, and time-bound authorization to prevent misuse. This allows Components to align with DoW credentialing and PKI requirements while safely accommodating legacy OT systems that cannot participate directly in certificate-based security.
2.1.3.OT	NPE Credentialing Authority	Device	Target	The DoW approved Credentialing Authority, using either a centralized or federated technologies, integrates NPEs from both the Operational IT and Process Control environments. The Operational IT and Process Control IdP solution should be separate from the Enterprise IT solution. An Operational IT Device Management solution is used to track NPE integration. As appropriate, process Control NPEs shall be integrated into the PKI and/or IdP system to enable secure OT protocols (e.g., BACnet Secure Connect (BACnet/SC), DNP3 Secure).	1. NPEs from both Operational IT and Process Control environments are integrated using either centralized or federated technologies. 2. NPEs are tracked in the Operational IT environment Device Management solution, indicating whether they are integrated into the IdP and/or PKI system. 3. Process Control NPEs are integrated into the PKI and/or IdP system as appropriate to enable secure OT protocols. 4. NPEs not integrated are marked for retirement or an exception is documented with a risk-based, methodical approach.	P	Xage supports decentralized and federated authentication across Operational IT, Process Control, and Enterprise IT by integrating with multiple IdPs—allowing each environment to maintain its own identity service while still enforcing unified Zero Trust policies. Xage provides identity proxying and overlay encryption for NPEs that cannot natively join PKI or IdP systems, enabling secure OT protocols such as BACnet/SC or DNP3 Secure. Its distributed enforcement fabric also tracks NPE integration across environments, allowing credentialing to remain separated where required while still benefiting from centralized policy management.
2.1.4.OT	Automated NPE Discovery	Device	Advanced	DoW Components automate OT network NPE discovery through the OT environment, limiting access to NPEs based on risk-based methods. OT network asset discovery shall utilize active discovery methods that are optimized to mitigate operational disturbances through configurations that avoid aggressive network scans, especially for equipment in the Process Control environment. In addition, SIEM, SOAR, and IDS solutions shall be configured to permit traffic from authorized active discovery tools to reduce false alarms.	1. NPE discovery is automated through the entire OT environment 2. Automated discovery utilizes active discovery methods, as opposed to passive discovery methods 3. The incidence of false alarms is reduced compared to Target Activities by configuring the SIEM, SOAR, and IDS solution to permit traffic from discovery tools.	P	Xage provides passive discovery of NPEs across OT networks, active discovery of accounts on those assets, and integration with third-party active discovery tools to enrich asset and identity data without disrupting sensitive Process Control systems. Xage combines this information—assets, users, permissions, and interaction patterns—to build risk profiles that drive adaptive access controls, dynamically adjusting privileges or sessions based on observed behavior and risk signals. This approach aligns with OT constraints by avoiding aggressive scanning, while still delivering the visibility needed for risk-based access decisions and supporting SIEM, SOAR, and IDS workflows with accurate, low-noise data.
2.2.1.OT	Implement Connection Policy for OT Environments	Device	Target	The DoW Enterprise refines policy, standards and requirements for connection policies. Policy, standards, and requirements should specifically state how often compliance audits are conducted to ensure all NPEs meet minimum security standards. DoW Components implement and enforce compliance-based network authorization for the Operational IT environment, but only for the Process Control environment, as appropriate.	1. DoW Enterprise policy, standards, and requirements for connection policies are refined and documented. 2. Refined policies clearly dictate the frequency and scope of compliance audits to meet minimum security standards. 3. DoW Components implement and enforce compliance-based network authorization, specifically for the Process Control environment as appropriate. 4. Compliance enforcement is risk-based, prioritizing the Operational IT and Process Control environments as appropriate.	P	Xage centralizes and enforces connection policies across Operational IT and Process Control environments, applying compliance-based network authorization where appropriate without disrupting OT operations. Xage integrates with compliance management tools to provide risk-based access for assets. Xage also provides detailed logs and telemetry that support scheduled compliance audits and verification processes defined by DoW policy, ensuring NPEs maintain required security standards while preserving the separation and safety constraints of Process Control systems.

2.3.1.OT	Configuration Monitoring and Control Tools for OT Environments	Device	Target	DoW Components procure and implement configuration monitoring and control solutions for the Operational IT environment. Configuration control should ensure configuration files (e.g., ladder logic) for the Process Control environment are not altered, downloaded, or uploaded except by authorized individuals.	1. Configuration monitoring and control solutions are implemented for the Operational IT environment 2. Process Control environment configuration control solution prevents altering, downloading, or uploading unauthorized configuration files.	P	Xage provides secure, policy-controlled file transfer capabilities that ensure configuration files—including ladder logic and other OT-specific artifacts—are only accessed or modified by authorized individuals. All file movements, in or out or East-West, are authenticated, integrity-checked, and scanned for malware, preventing altered or unauthorized files from being uploaded or downloaded.
2.3.2.OT	Integrate AV Tools for OT Environments	Device	Target	DoW Components procure and implement approved anti-virus and anti-malware solutions for supported Operational IT NPEs. NPEs without anti-virus or anti-malware solutions must be protected with mitigating controls.	1. Anti-virus and anti-malware is implemented on Operational IT NPEs 2. NPEs without anti-virus or anti-malware must be protected with other mitigating controls.	P	Most OT assets such as PLCs and RTUs cannot support anti-virus or anti-malware agents, so Xage provides an agentless protective layer by proxying and filtering all connections to these devices. Xage applies overlay malware scanning to files and data streams before they reach the asset and integrates with multiple ICAP-compatible malware scanning solutions to ensure only clean, authorized content is allowed through. This delivers strong mitigating controls for NPEs that cannot host traditional endpoint protection, enhancing Operational IT and Process Control security without impacting sensitive OT equipment.
2.3.3.OT	OT Device Security Stack with C2C	Device	Advanced	DoW Components working with DoW Enterprise review current C2C policies applicability to the OT Environment. DoW Components shall prioritize applying security solutions and configurations for OT devices enabling C2C policies where possible in the OT Environment.	1. DoW Components, in collaboration with the DoW Enterprise, have reviewed current C2C policies to determine their applicability to the OT environment. 2. Based on the review, DoW Components prioritize the implementation of security solutions and configurations for OT devices that enable C2C policies, where feasible. 3. OT devices prioritized for C2C implementation have an acceptable security stack adaptation to support those policies.	P	Xage supports the application of C2C policies in OT environments by ensuring that simply connecting to a network does not grant access to any assets. Users must still authenticate and be authorized through the Xage Fabric before performing any action and then only to certain assets and operations per policy. For devices including legacy OT devices that cannot authenticate when joining a network Xage strictly limits their scope of allowable interactions based on centrally defined policy. The Xage Fabric can also detect or block devices that unexpectedly change MAC or IP addresses, reducing spoofing risks and ensuring that only verified entities can operate within the environment.
2.4.1.OT	NPE Deny by Default Policy	Device	Target	DoW Components block all unauthorized remote and local NPE access to resources, including serial communications and console access, via technical or procedural controls. Identified and authorized NPEs are provided risk-based, methodical access.	1. Unauthorized remote and local NPE access and connections are blocked. 2. Physical controls are implemented to secure local NPE access.	Y	Xage enforces strict deny-by-default access for all NPEs through its Xage Enforcement Point (XEP), which discovers and controls every interaction according to centrally defined policy. Whether communication is local or network-based, XEP mediates and authorizes each request, ensuring that only identified and approved NPEs receive access and only at the level justified by risk and operational need. Furthermore, Xage also controls access to the NPEs themselves whether from users or other NPEs. This provides comprehensive technical control over NPE access while maintaining the safety and reliability required in OT environments.
2.4.2.OT	Managed and Limited BYOD support for OT Environments	Device	Target	Only Government Furnished Equipment (GFE) is permitted to connect to an OT Environment. GFE is provided by the system owner and any required software is scanned and approved before deployment for use in the OT environment. If non-GFE is required, and properly authorized by command authority, to connect to the OT Environment, it must follow the approved deviation process, which explicitly identifies risk tolerance levels based on situational circumstance.	1. Only GFE is permitted to connect, manage, configure, or maintain NPE in the OT environment. 2. Software deployed on GFE is scanned and approved before use in the OT environment. 3. Any non-GFE requiring connection to the OT environment must follow an approved deviation process, explicitly identifying risk tolerance levels based on situational circumstance and requiring command authorization	Y	Xage identifies all assets connecting to the OT environment, including endpoints, and ensures that only Government Furnished Equipment meeting required posture checks is allowed access. Xage supports flexible integration with native GFE posture check tools as well. All connectivity is mediated through Xage's proxies and zero trust containment points requiring successful authentication before any interaction occurs. Management and industrial protocol access is conducted through a secure browser interface, preventing direct device exposure and ensuring that only approved, policy-defined applications are available to each user. Xage's granular control over interactions and device posture enforcement also supports deviation processes for properly authorized non-GFE by tightly constraining access based on risk tolerance and operational context.

2.4.3.OT	Managed Non-OT Assets	Device	Target	DoW Components shall require non-OT assets are managed and meet standard baseline checks before authorization or connection to the OT Environment.	1. Only non-OT assets that meet mandated configuration standards allowed to access resources or connect in the OT Environment.	Y	Xage performs posture checks on every non-OT endpoint before allowing any connections verifying software version, malware scan results, user identity, location, and other baseline criteria. Endpoints never interact directly with OT assets; all activity is proxied through Xage, providing full session termination and protocol breaks for inspection and control. Even after authorization, interactions are tightly limited to the specific assets and actions defined by policy, ensuring that all non-OT systems accessing OT resources remain secure, constrained, and fully monitored.
2.5.1.OT	Implement Vulnerability and Patch Management Tools for OT Environments	Device	Target	OT Environments must maintain minimum government approved compliance standards and patching as well as be maintained to current approved configuration profiles. Any systems outside of these standards require authorization from the DoW Component through a risk based assessment approach. Periodic reassessments for compliance are performed for all devices in use. At the Process Control level, special care must be given to mitigate vulnerabilities without a patch source, while protecting safety, operational functionality, and process reliability. Similarly, risk-based testing must be performed and accepted prior to patching.	1. OT Environments are maintained to current approved compliance standards, patching levels, and configuration profiles. 2. Periodic reassessments are performed for all devices to verify ongoing compliance. 3. For Process Control environments, a risk-based approach is used to mitigate vulnerabilities, particularly where patch sources are unavailable, prioritizing process reliability.	P	Many OT assets cannot be patched directly or immediately because updates are often unavailable or would require downtime that risks mission-critical operations. Xage addresses this challenge with virtual patching, shielding vulnerable assets from exploits by enforcing identity-based access controls, protocol mediation, and overlay scanning without modifying the device or interrupting operations. This allows OT environments to maintain compliance and mitigate vulnerabilities even when traditional patching is not feasible. Xage enables risk-based decisions for systems that fall outside approved configuration or patch baselines while maintaining safety and operational reliability at the Process Control level.
2.6.1.OT	Implement UEDM for OT Environments	Device	Target	DoW Components will procure and implement a UEDM solution, wherever applicable, for all identified devices. This shall include explicit configuration profiles per device.	1. UEDM solution is implemented, incorporating the requirements for configuration, vulnerability, and patch management.	P	Xage works alongside UEDM by supplying rich interaction, audit, policy, and governance data that enhances endpoint visibility and compliance monitoring. Every access request, session, and action mediated by Xage is logged with full identity and contextual detail, giving the UEDM platform deeper insight into how devices and users interact with OT assets. At the same time, Xage can consume data from UEDM such as device configuration state, software version, vulnerabilities, or detected anomalies to dynamically adjust access policies, enforce deny-by-default decisions, or trigger step-up authentication. This bi-directional integration ensures that endpoint security status directly informs access decisions, while UEDM benefits from Xage's granular, identity-driven activity data to strengthen monitoring, governance, and enforcement across OT environments.
2.6.2.OT	OT Device Configuration Management	Device	Target	DoW Components sets standards and policies for the device inventory and secure configuration, in conjunction with the UEDM solution and asset management tools, to enable automated configuration management control. Automated solutions for configuring devices are used only after analyzing the risk to operations.	1. Standards and policies are defined for OT device management for the Operational IT and Process Control environments. 2. Automated configuration management is enabled.	N	Xage works in conjuction with UEDM and Configuration Management solution by supplying inventory information, providing secure access, and insuring integrity of the data.
2.7.1.OT	Implement Endpoint Detection & Response (EDR) Tools for OT Environments	Device	Target	DoW Components procure and implement EDR solution(s) within the Operational IT, and Process Control environments as appropriate. DoW Components conduct system analysis to determine the potential automated responses within both the Operational IT and Process Control environments prioritizing safety, process reliability, and mission.	1. EDR solutions are implemented for both Operational IT and Process Control environments, following system analysis to determine and prioritize automated responses.	P	Most OT assets cannot support traditional EDR agents, so Xage complements EDR deployments by providing an overlay fabric that enforces access control, performs malware scanning, and enables automated response actions without requiring agents on the devices themselves. Xage proxies, filters, and mediates all interactions with OT assets, allowing it to block malicious activity, terminate risky sessions, or adjust privileges dynamically based on detected threats. Xage integrates with a variety of EDR and malware scanning vendors to provide overlay detection and response for any asset.

2.7.2.OT	Implement Extended Detection & Response (XDR) Tools for OT Environments	Device	Advanced	DoW Components procure and implement XDR solution(s) to all possible devices, and integration with other solutions where possible. EDR continues coverage 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 OT and/or Enterprise SIEM solution.	1. XDR solution is implemented for both Operational IT and Process Control environments 2. The maximum number of services and applications are covered by the XDR solution 3. Basic analytics from the XDR are sent to the OT and/or Enterprise SIEM.	P	Xage complements XDR deployments by supplying identity-rich interaction data, session telemetry, and policy context that extend detection and response capabilities into OT environments where agents cannot be deployed. While XDR solutions cover as many devices, services, and applications as technically feasible, Xage provides an overlay control point for the OT assets that cannot run agents, mediating all access and enabling automated response actions such as session termination, privilege reduction, or access denial. Xage also integrates with major XDR, EDR, and malware scanning vendors, feeding them high-fidelity activity data and consuming their threat intelligence to strengthen real-time access decisions. This combined approach ensures comprehensive visibility and coordinated analytics across the XDR stack, which then feeds into OT and Enterprise SIEM systems for broader detection, correlation, and response.
3.1.1.OT	OT Application and Code Inventory	Applications and Workload	Target	DoW Components create an inventory of all applications. Software applications include those in use within the Operational IT environment, as well as those in use within the Enterprise IT applications when they interoperate with the Operational IT environment, including open source, commercial, and/or in-house solutions. Each Component tracks and documents the application supportability, hosted location (e.g., cloud, on-premise, hybrid), and other important data (e.g., name, version, team responsible, licensing and support, mapped dependencies).	1. All applications within the Operational IT environment, and the Enterprise IT and which interoperate with the Operational IT environment, are identified, categorized, tracked, and documented.	P	Xage's proxy architecture enables granular, identity-based access to both web-based and native applications running on workstations or servers across Enterprise, Operational, and Process environments. Xage can granularly limit access based on identity, role, or attributes to a specific native or web application on any workstation or server, ensuring only authorized users can interact with it. This visibility and control can also be extended to generate an application inventory, supporting Component efforts to document versions, locations, supportability, and dependencies.
3.1.2.OT	OT Application Control	Applications and Workload	Target	Application control solutions are applied to inventoried applications (e.g., SCADA software, control software, controller IDEs, etc.), to prevent unauthorized modifications.	1. Application control solutions are implemented on inventoried applications	P	Xage fingerprints and isolates applications used to interact with OT assets such as SCADA software, control applications, and controller IDEs and ensures that all interaction to and from these applications is performed in approved, policy-governed ways. Through its secure access proxy, Xage identifies exactly which application a user is invoking, restricts access to only those applications authorized for a given role (even when other apps are present on workstations), and prevents unapproved tools or modified executables from being used. By isolating application interactions from the underlying OT network and enforcing deny-by-default policies, Xage helps ensure that critical OT software cannot be misused
3.2.1.OT	Build OT DevOps Capability Factory Pt. 1	Applications and Workload	Target	The DoW Enterprise provide guidance for DevOps or DevSecOps processes, CI/CD, and Infrastructure as Code (IaC) pipelines in the Operational IT environments, and where appropriate for the Process Control applications. For DoW Components that have application development processes the guidance is applied.	1. The DoW Enterprise provides guidance for DevOps or DevSecOps processes, CI/CD, and IaC pipelines for Operational IT environments, and where appropriate for Process Control applications, to be applied by DoW Components with existing application development processes.	Y	Xage suppots integration with DevOps/DevSec processes, CI/CD and Infrastructure as Code pipleine. Xage software is fully containerized, provides full APIs, itegrates with IdPs using SAML/LDAP, supports syslog and event management.

3.2.2.OT	Build OT DevOps Capability Factory Pt. 2	Applications and Workload	Target	DoW Components that have capability development processes extend to use approved DevOps or DevSecOps processes, CI/CD, and IaC pipelines to develop new capabilities in the OT environment, as appropriate. DevOps or DevSecOps processes are also used to update existing capabilities. Continual validation functions are integrated into the CI/CD pipelines and DevSecOps processes are integrated with existing capabilities.	1. Engineering teams within the OT environment follow DevOps or DevSecOps, CI/CD, and IaC pipeline process patterns for development and deployment.	Y	Xage suppots integration with DevOps/DevSec processes, CI/CD and Infrastructure as Code pipleine. Xage software is fully containerized, provides full APIs, itegrates with IdPs using SAML/LDAP, supports syslog and event management.
3.2.3.OT	Standardized OT Application Security and XBOM Inventory	Applications and Workload	Advanced	All delivered applications and capabilities must apply approved security practices during development and ensure all security features are operable during execution. Additionally, an approved XBOM solution inventories utilized capability and application delivery.	1. All delivered applications and capabilities apply approved security practices during development 2. All security features are operable during execution 3. An approved XBOM solution inventories utilized software solutions.	Y	Xage Fabric is IEC 62443 and FIPS 140-2 certified. Xage implements Secure Development Life Cycle (SDLC) certified per IEC 62443 and validates all software components for authetiicit and integrity. Xage is also ISO 27001 certified for the enterprise.
3.3.1.OT	OT Vulnerability Management Program Pt. 1	Applications and Workload	Target	DoW Components work with the DoW Enterprise to establish and manage an OT Vulnerability Management program. OT Vulnerability Management teams shall collaborate with a related Enterprise IT Vulnerability Management team. Vulnerability management for the OT environment shall incorporate vulnerability scope and risk to mission in prioritization decisions. Vulnerability sources can be delivered from any trusted agent, and must be consumed as an interoperable product.	1. OT Vulnerability Management program is established and managed by the DoW Component, in collaboration with the DoW Enterprise. 2. The OT Vulnerability Management program prioritizes vulnerabilities based on risk to mission and consumes vulnerability data from interoperable sources.	P	Most OT assets cannot be patched easily because updates are often unavailable or would require downtime that risks mission-critical operations. Xage addresses this challenge with virtual patching, shielding vulnerable assets from exploits by enforcing identity-based access controls, protocol mediation, and overlay scanning without modifying the device or interrupting operations. This allows OT environments to maintain compliance and mitigate vulnerabilities even when traditional patching is not feasible. Xage enables risk-based decisions for systems that fall outside approved configuration or patch baselines while maintaining safety and operational reliability at the Process Control level.
3.3.2.OT	OT Vulnerability Management Program Pt. 2	Applications and Workload	Target	Standard processes are established at the DoW Enterprise level for reporting and managing the disclosure of vulnerabilities in DoW maintained or operated OT environments, for disclosure both publicly and privately. DoW Components expand the OT Vulnerability Management program to track and manage open public, controlled public, PAI and CAI, and DoW internally derived vulnerability sources.	1. Enterprise-wide processes for managing disclosure of vulnerabilities for OT environments 2. DoW Components have expanded the vulnerability management program to track and manage open public, controlled public, PAI and CAI, and DoW internally derived vulnerability sources.	P	Most OT assets cannot be patched easily because updates are often unavailable or would require downtime that risks mission-critical operations. Xage addresses this challenge with virtual patching, shielding vulnerable assets from exploits by enforcing identity-based access controls, protocol mediation, and overlay scanning without modifying the device or interrupting operations. This allows OT environments to maintain compliance and mitigate vulnerabilities even when traditional patching is not feasible. Xage enables risk-based decisions for systems that fall outside approved configuration or patch baselines while maintaining safety and operational reliability at the Process Control level.
3.3.3.OT	Binaries, Code, and Hardware Configurations for OT Environments	Applications and Workload	Target	The DoW Components manage and document approved binaries, code, and hardware configurations for the Operational IT and Process Control environments, and code reviews are conducted. Secure and reliable configuration management processes and procedures are established and adopted (e.g., to enable reverting to known-good backups). These approaches include supplier sourcing risk management, supply chain risk management, and industry standard vulnerability management.	1. Approved binaries, code, and hardware configuration developed across the OT environment are managed and documented.	P	Xage Fabric is IEC 62443 and FIPS 140-2 certified. Xage implements Secure Development Life Cycle (SDLC) certified per IEC 62443 and validates all software components for authenticity and integrity. Xage is also ISO 27001 certified for the enterprise. Furthermore, Xage can enable integrity verification of any files including binaries and configuration as part of our Xage file transfer and secure data exchange capabilities.

3.4.1.OT	Access Control for OT Environments Pt. 1	Applications and Workload	Target	All applications and capabilities must support a full ABAC solution. Applications, services, and devices unable to utilize ABAC are identified for future decommissioning.	1. All applications and capabilities support a full ABAC solution. 2. Applications, services, and devices unable to utilize ABAC are identified for future decommissioning.	Y	Xage supports ABAC requirements by enforcing attribute-based decisions at every access point and layering ABAC controls on top of applications, services, and devices that lack native ABAC capabilities. Through its proxy and enforcement fabric, Xage evaluates user, device, environmental, and behavioral attributes before permitting any interaction, effectively extending ABAC governance to legacy OT systems without requiring their replacement or modification. This preserves existing investments while still enabling full ABAC policy enforcement, and also helps identify applications that may require future modernization.
3.4.2.OT	Access Control for OT Environments Pt. 2	Applications and Workload	Target	Access control must be enforced using digital policy with full attribution utilizing ABAC following established policies. Applications, services, and devices unable to utilize ABAC are either decommissioned or accepted using a risk-based methodical approach.	1. Policy enforcements is implemented for all possible applications, services, and devices in the Operational IT environment 2. Applications, services, and devices unable to utilize ABAC are either decommissioned or accepted using a risk-based approach.	Y	Xage enforces digital access control with full attribution by capturing and validating every identity, device posture, environmental factor, and behavioral signal involved in an access request. Each interaction whether from a user, service, or NPE is tied to a verifiable identity, enriched with attributes such as role, location, device compliance state, application used, time, and risk indicators. This allows Xage to apply precise ABAC decisions at the proxy and mediation layer, ensuring that access is granted only when all required attributes align with policy. By layering this ABAC enforcement onto applications, services, and devices that lack native attribute support, Xage preserves existing OT investments while still delivering complete attribution and policy-driven control.
3.4.3.OT	Access Control for OT Environments Pt. 3	Applications and Workload	Advanced	Confidence scoring is introduced across the attributes to create a more advanced method of authorization decision making in an automated fashion. High-Privileged OT attributes are identified for the Confidence scoring.	1. Confidence scoring is introduced and implemented to High-Privileged OT attributes.	Y	Xage supports confidence-based authorization through its adaptive access framework, which continuously evaluates risk using a rich set of attributes—including identity, role, location, behavior, time of access, device posture, and asset-specific risk factors. Xage calculates dynamic confidence levels for every interaction by combining internal signals with optional external threat or asset data, allowing authorization decisions to adjust automatically as conditions change. High-privileged OT actions such as controller access or access from engineering tools carry greater weight in this model, triggering stricter controls, step-up authentication, or session restrictions when confidence decreases. This creates a sophisticated, automated authorization process that aligns Zero Trust with the safety and reliability needs of OT environments.
3.4.4.OT	Access Control for OT Environments Pt. 4	Applications and Workload	Advanced	Apply confidence scoring to all DAAS, PEs, and NPEs in the OT environment.	1. Confidence scoring is applied to all DAAS, PEs, and NPEs in the OT environment.	P	Xage adaptive access framework with confidence/risk analysis applies as on overlay DAAS, PEs, and NPEs in OT environment.
4.1.1.OT	OT Data Tagging Governance	Data	Target	The DoW Enterprise establishes governing body(s) for establishing controlled terminology (data and metadata), file formats, and communication protocols, which are used to ensure interoperability across communities. Data at the DoW Component level should be categorized and analyzed to align with the controlled terminology, ensuring input from appropriate Information Owners for correct alignment. DoW Components will also determine data tagging structure and maps based on workflow process, with a focus on risk of operational impact. OT environment must include a characterization method for all data.	1. A governing body is established to define and maintain controlled terminology, file formats, and communication protocols for interoperable data transmission, querying, and storage across communities. 2. DoW Component categorizes and analyzes their data to align with the established controlled terminology. 3. DoW Component determines and implements data tagging structures and maps based on workflow processes and operational risk, including a characterization method for all data in the OT environment. 4. Exemptions for data tagging have been submitted by the DoW Component with justification.	N	Xage can provide this capability via integration wih partners

4.2.1.OT	Define OT Data Tagging Patterns	Data	Target	Data tagging mandates for data within the OT environment is defined based on workflow process data types in 4.1.1.OT. The DoW Enterprise works with DoW Components to establish data tagging, labeling, and classification patterns based on industry best practices. Patterns are agreed upon, for both Operational IT data tagging and Process Control data tagging (which may be system specific), documented, and implemented in portions of the OT environment for which tagging does not interfere with critical processes.	1. Data tagging mandates for OT data are defined based on workflow process data types. 2. Data tagging, labeling, and classification patterns are established across DoW Components, instituting industry best practices and does not interfere with critical processes.	N	Xage can provide this capability via integration wih partners
4.2.2.OT	OT Data Sharing Interoperability Patterns	Data	Target	The DoW Enterprise, collaborating with the DoW Components, develops interoperability patterns that are compliant with the established policy used for each operating mode of the OT environment. DoW Components develop methods for data sharing outside of the OT environment, considerations for secure data exchange between different Impact Levels, and including protection mechanisms for managing all OT data.	1. Interoperability patterns, compliant with established policy, are in place for data protection technologies across all operating modes of the OT environment. 2. Methods and protection mechanisms for data sharing outside of the OT environment are developed.	Y	Xage's Zero Trust Data Exchange (ZTDE) supports these interoperability and data-sharing requirements by enforcing granular, identity-driven controls not only on user and asset interactions but also on how data itself is accessed, moved, and consumed. ZTDE allows data to be governed at the topic or object level, effectively giving each data stream or dataset its own "data identity" that defines who or what may interact with it and under what conditions. This enables strict separation across domains and impact levels while providing secure pathways for data sharing outside the OT environment.
4.2.3.OT	Document OT Storage Architecture	Data	Target	The DoW Enterprise works with DoW Components to establish storage architecture patterns and guidance, taking into consideration the data that is produced within the Operational IT and Process Control environments. DoW Components develop logical and physical architectural diagram for all storage methods. DoW Components assess their existing data storage strategies and technologies to determine the suitability for implementing storage architectures.	1. Storage architecture patterns and guidance are established by the DoW Enterprise in collaboration with the DoW Component. 2. Storage architecture considers OT-specific data requirements, both for the Operational IT environment (e.g., server configurations, network device configurations, etc.), and Process Control environment (e.g., controller logic, device configurations, PLC project files, etc.). 3. Logical and physical architectural diagrams are developed for all storage methods used by the DoW Component. 4. DoW Component assesses their existing data storage strategies and technologies to determine suitability for implementing established storage architecture patterns, including consideration of Software Defined Storage where appropriate.	Y	Xage abstracts data storage across the OT environment by mediating all interactions through the Xage Fabric, which creates controlled repositories for each user or NPE and enforces granular access and sharing policies. Instead of allowing users or systems to access OT storage directly especially via insecure protocols like SMB Xage proxies and governs every interaction, ensuring that configuration files, controller logic, PLC project files, and other OT data are handled according to established storage architecture patterns. This eliminates direct exposure of storage systems, enforces strict segmentation, and provides consistent policy enforcement regardless of where data resides. By centralizing control of data access while supporting distributed OT storage requirements, Xage helps DoW Components align their existing storage strategies with the enterprise-defined architecture, including future transitions toward software-defined storage models.
4.3.1.OT	Implement OT Data Tagging Tools	Data	Target	DoW Components procure and implement a data tagging solution based on the standard from activity 4.2.1.OT. A framework is established for periodic re-assessment of system risk and vulnerability. Tagging solution may leverage native capabilities of the Process Control protocols.	1. Data tagging solution is procured and implemented 2. Periodic evaluation of the system risk and vulnerabilities is performed to adjust data tagging to evolving threat landscape. E53:E55	N	Xage can provide this capability via integration wih partners.
4.3.2.OT	Data Tagging	Data	Target	DoW Components use the tagging standards developed in 4.2.1.OT to apply tags (manual or automated) using local labeling to meet minimum essential metadata criteria to enable ZT functionalities. Data tagging solution migrates over time to attribute-based pattern marking.	1. Manual and/or automated data tagging begins according to the standards established.	N	Xage can provide this capability via integration wih partners

4.4.1.OT	DLP Analytics	Data	Target	DoW Components establish DLP types (e.g., Network, Endpoint, On-Premises, etc.) and recognition patterns based on data tagging solution in Activity 4.3.1.OT. A DLP analytics process is established to investigate loss type from logs, and determine severity, impact, policy enforcement, and mitigation response.	1. DLP types, recognition patterns, and analytics process are established 2. DLP analytics process enables policy enforcement for how sensitive data is handled and shared, and enables monitoring and detection of data loss events.	P	Xage can integrates with variety of DLP solutions to provide overlay data loss prevention as data moves within and across environments utilizing the Xage Fabric.
4.4.2.OT	Establish DRM Processes	Data	Target	DoW Components establish a DRM processes, which leverage PBAC to control information use, to include information use beyond the OT environment Formal Boundary. The framework includes the development of DRM-specific use cases to better outline solution coverage.	1. DRM processes that leverage PBAC are established 2. DRM-specific use cases are developed in framework.	N	Xage does not provide this capability at this time.
4.4.3.OT	OT File Prioritization and Monitoring	Data	Target	DoW Components identify files within the Operational IT and Process Control environments that require file monitoring and protection (e.g., controller configuration files, plant schematics, network diagrams), and establish a prioritization process for ranking severity of impact for each file type and use case. Data owners utilize File Monitoring tools to monitor, in priority order, the identified files.	1. Data and files of critical classification are actively being monitored 2. Data owners utilize File Monitoring tools to monitor files in order of established priority 3. Basic Integration is in place with monitoring system such as the SIEM.	P	Xage controls access to critical OT files such as controller configurations, plant schematics, and network diagrams based on user identity, role, and attributes, ensuring only authorized individuals can upload and download them. It also governs where these files can be transferred, preventing unauthorized movement or exposure. Xage continuously monitors and logs all access attempts to identified files, providing the visibility needed for file monitoring and protection efforts and supporting prioritization based on the impact of each file type.
4.4.4.OT	OT File Monitoring Interoperability	Data	Target	File monitoring artifacts and logs must have a standard, machine-readable formats to enable interoperability with other tools (e.g., DLP, DRM, and UEBA tools), in alignment with activity 6.6.1.OT.	1. Data and files of all regulated classifications are actively being monitored 2. A standard, machine-readable format is utilized for file monitoring artifacts and logs.	P	Xage produces file monitoring artifacts and logs in standard, machine-readable formats that can be easily integrated with DLP, DRM, UEBA, and other security tools.
4.4.5.OT	Inventory Databases	Data	Target	DoW Components identify, enumerate, and document databases within the OT Operational Environment.	1. Databases are identified and documented within the OT Operational Environment.	Y	Xage identifies and inventories databases within the OT environment by discovering data stores and enumerating the accounts associated with them. This provides DoW Components with an accurate, continuously updated view of database assets and their accounts and interactions. Furthermore, Xage can also discover internal data structure and tables in the those databases.
4.4.6.OT	Database Activity Monitoring and Response	Data	Target	DoW Components procure, implement, and utilize Database Monitoring solutions, as appropriate, with either in-band or out-of-band solutions. Initial data monitored shall include regulated data types (e.g., CUI, PII, PHI) as appropriate for the mission environment. Logs and analytics from the database monitoring solution are fed to the SIEM. Additional data attributes are identified and used to extend the monitoring of databases as applicable.	1. Databases within the OT environment (e. g. data at rest, data exchange, transaction monitoring) is monitored. 2. Monitoring analytics is sent to SIEM. 3. Additional data attributes are identified and incorporated into database monitoring to enhance detection capabilities. 4. Along with in-band monitoring, out-of-band monitoring solutions are considered and possibly utilized.	P	Xage can monitor and control access to database data at a granular level—governing how users, LLMs, and AI agents interact with sensitive information and preventing unauthorized access to regulated data such as CUI, PII, or PHI. All database access requests are mediated through Xage's identity-driven policies, ensuring that only approved entities can query or retrieve protected content. Xage also integrates with external DLP solutions to extend monitoring and protection, while exporting detailed logs to SIEM platforms for comprehensive analytics and compliance reporting.
4.5.1.OT	Implement DRM and DLP Pt. 1	Data	Target	OT environment will manage DRM and DLP to the outer edge of the OT environment formal boundary as determined by the DoW Component. The consumer of the artifact(s) is expected to maintain the DRM agreement.	1. DRM and DLP are managed by OT environment to the outer edge of the OT environment formal boundary.	P	Xage integrates with partner DRM and DLP solutions. Xage Fabric deployed as a network overlay with nodes at the edge enables strategic positioning of DRM and DLP at the edges ensuring visbility to all data interactions.
4.5.2.OT	Implement DRM and DLP Pt. 2	Data	Advanced	Atypical DRM behavior or occurrences are documented and reported to DoW Components or Enterprise, to perform outlier analysis and refinement of DRM rule sets. Refined rule sets utilized by DLP.	1. Outlier analysis and refinement of DRM rule sets is performed and documented against atypical DRM behavior and/or occurrences 2. DLP used with refined rule sets.	P	Xage integrates with partner DRM and DLP solutions. Xage Fabric deployed as a network overlay with nodes at the edge enables strategic positioning of DRM and DLP at the edges ensuring visbility to all data interactions.

4.5.3.OT	DRM Response Pt. 1	Data	Target	Create data tags for response characterization, and create response process driven by newly established tags.	1. Data tags are created for DRM response characterization 2. DRM response process is driven by newly established tags.	N	Xage does not provide data tagging capability
4.5.4.OT	DRM Response Pt. 2	Data	Advanced	DoW Components implement data tags for data within databases applicable to the mission environment. Data is encrypted according to policy based on data tags.	1. Data repositories are protected using DRM. 2. Data is encrypted using data tags.	N	Xage does not provide data tagging capability, but can integrate with a partner solution to provide access control to data based on tags.
4.6.1.OT	DLP Deployment	Data	Target	Newly identified attributes can be established to improve DLP outcomes. The DLP enforcement points can be controlled to the OT environment formal boundary with a combination of PBAC, DRM, and DLP, and then beyond the boundary via agreement. DLP is initially implemented with “monitor-only” and/or “learning” mode, to test outcomes with limiting impact on operations. Collaboration with cyber functions should occur with respect to any observed data loss activity.	1. DLP enforcement points are established and controlled to the OT environment formal boundary, deployed with DLP tools, and initially configured in monitor mode with standardized logging. 2. A process is established for identifying and incorporating new data attributes to improve DLP effectiveness. 3. Observed data loss activity triggers collaboration with cyber functions for investigation and response. 4. Mechanisms for extending DLP enforcement beyond the OT boundary via agreements are defined.	P	Xage integrates with partner DLP solutions. Xage Fabric deployed as a network overlay with nodes at the edge enables strategic positioning of DRM and DLP at the edges ensuring visbility to all data interactions.
4.6.2.OT	DLP Operations	Data	Target	DLP solution is transitioned from testing to operations. DLP and zero trust tagging should be complimentary to achieve full access control and data loss prevention to the formal boundary. The operational model must also prescribe formalized agreements for zero trust and DLP behaviors beyond the formal boundary as determined by the DoW Component.	1. DLP solution is transitioned from testing to operations mode. 2. Tagging is integrated to achieve full access control and data loss prevention to the formal boundary. 3. Formalized agreements are established to govern zero trust and DLP behaviors beyond the formal boundary.	P	Xage integrates with partner DLP solutions. Xage Fabric deployed as a network overlay with nodes at the edge enables strategic positioning of DRM and DLP at the edges ensuring visbility to all data interactions.
4.7.1.OT	Manage DAAS Access with Storage Policy	Data	Target	Governance mechanisms ensure that DoW Component DAAS access policy is sufficient for Zero Trust outcomes aligned with activity 4.2.3.OT.	1. Attribute-based DAAS policy is developed with DoW Enterprise and organizational level support.	Y	Xage provides the enforcement layer needed for an attribute-based Data-Access-as-a-Service (DAAS) policy by allowing data access rules to be driven by identity, role, device posture, environment, data sensitivity, and other attributes defined at the DoW Enterprise or Component level. Once an attribute-based DAAS policy is established, Xage can apply it uniformly across Operational IT and Process Control environments, ensuring that data access is granted only when all required attributes align with enterprise policy. Because Xage mediates and authenticates all data interactions through its fabric, it becomes a natural enforcement point for DAAS, enabling consistent, centrally governed, attribute-based access to OT data without requiring changes to underlying systems.
5.1.1.OT	OT Granular Access Rules and Policies Pt. 1	Network	Target	The DoW Enterprise works with DoW Components to create granular access rules and policies, technical and procedural, in the Operational IT environment, and within the Enterprise IT environment when services are provided to the OT environment. Associated ConOps shall be developed to align with the access rules and policies. DoW Components will implement these access rules and policies into existing solutions to improve initial risk levels and ensure future interoperability.	1. Granular access rules and policies are established for the Operational IT environment, and for the Enterprise IT environment when applicable 2. ConOps are developed 3. Access rules and policies are implemented.	Y	Xage allows administrators to create granular, enforceable policies for both Operational IT and applicable Enterprise IT environments. Xage can also translate existing ConOps rules into enforceable policies. Xage Visibility 2 Policy (V2P) Studio plays a central role in this process by providing a single interface to discover assets, visualize interactions, and create precise access rules that reflect operational workflows. Once defined, these policies are consistently applied through Xage’s distributed enforcement fabric, ensuring that only authorized interactions occur across all sites.

5.1.2.OT	OT Granular Access Rules and Policies Pt. 2	Network	Target	Data flow patterns are defined. DoW Components apply data tagging patterns to enable granular access to the OT environment, as appropriate.	1. Data flow patterns are defined, which cover both persistent and ephemeral data. 2. Data tagging patterns are applied.	Y	Xage enforces defined data flow patterns by controlling access at the individual interaction level, applying identity- and policy-based decisions to any data source or system in the OT environment. Each data request whether from a user, service, or NPE is evaluated against granular access rules, ensuring that only authorized entities can initiate or receive specific data flows. This approach provides precise control over OT data movement and maintains strict separation between systems and domains.
5.2.1.OT	Define OT Communication Pathway APIs	Network	Target	When SDN or alternate communication pathways are specified, the DoW Enterprise works with the DoW Components to identify the necessary APIs and other programmatic interfaces. Automated policy management through APIs should be tested before deployment, to minimize risk to OT operations.	1. Necessary APIs and other programmatic interfaces for specified communication pathways (including SDN) are identified and tested prior to deployment to minimize risk to OT operations.	Y	Xage uses an SDN-style architecture for access control and segmentation, combining centralized policy management with distributed controllers and enforcement points that operate safely within OT environments. All policy creation, updates, and enforcement can be driven programmatically through APIs, enabling seamless integration with existing workflows and minimizing operational risk during deployment. Xage also exports interaction data and analytics through APIs, providing visibility and validation for approved communication pathways while ensuring that only authorized traffic is permitted.
5.2.2.OT	Implement OT Programmable Infrastructure	Network	Target	DoW Components implement the programmable communication pathways to enable automation tasks in the Operational IT environment, as appropriate. Segmentation Gateways and Authentication Decision Points are integrated into the SDN or alternative networking infrastructure. All components of each programmable pathway shall output their logs into a standardized repository (e.g., SIEM, Log Analytics, syslog) for monitoring and alerting.	1. Programmable communication pathways are implemented in the Operational IT environment. 2. Segmentation Gateways and Authentication Decision Points are integrated into SDN. 3. Logs are output into standardized repository.	Y	Xage acts as both the segmentation gateway and the authentication decision point within its SDN-style architecture. Xage's distributed enforcement fabric controls and authenticates every pathway based on identity and policy, enabling safe automation without exposing OT systems to unmanaged traffic. All enforcement points generate detailed, standardized logs that can be forwarded to SIEM, Log Analytics, syslog, or other repositories for monitoring and alerting, ensuring complete visibility and alignment with DoW logging requirements.
5.2.3.OT	Information Flow Mapping Across OT Planes	Network	Target	Develop detailed information flow map inclusive of all planes and actions (e.g., data, control, management planes). Analytics and NetFlow from the updated infrastructure is automatically fed into operations centers and analytics tools.	1. Detailed information flow map is developed. 2. Analytics are automatically fed to operations centers and analytic tools.	Y	Xage helps create a detailed information flow map across data, control, and management planes by passively discovering assets, mapping their communication patterns, and identifying all associated users and NPEs. Its distributed enforcement points continuously collect flow and interaction telemetry, which can be exported as NetFlow-like analytics into operations centers and security analytics tools.
5.3.1.OT	OT Plane Segmentation	Network	Target	DoW Components implement plane segmentation (e.g., control, data, management planes) using traditional tiered and/or service-based architectures, as it applies to connected devices and systems within the Enterprise IT, Operational IT, and Process Control environments. Proxy and/or enforcement checks are integrated with communication pathways based the access policies defined in 5.1.1.OT and 5.1.2.OT.	1. Traditional tiered and/or service-based plane segmentation is implemented. 2. Enforcement checks of attributes, behavior, or other data using behavioral analytics engines are established.	Y	Xage provides segmentation across control, data, and management planes by mediating all communication through distributed enforcement points and proxies, applying identity- and policy-based checks to every interaction. These controls ensure that access to each plane is restricted according to defined segmentation policies and enforced consistently across Enterprise IT, Operational IT, and Process Control environments. Furthermore, Xage provides multi-layer segmentation across these domains, creating isolation at every layer to deliver true defense-in-depth and prevent unauthorized movement between tiers or services.

5.3.2.OT	B/C/P/S Segmentation	Network	Target	DoW Components implement B/C/P/S segmentation using logical zones, limiting lateral movement across missions and geographically separated DoW Components. Proxy and/or enforcement checks are integrated with the communication pathways based on the defined access policies.	1. Segmentation is implemented across base, camp, post and stations using logical zones to limit lateral movement. 2. Attribute and behavior based enforcement checks are implemented to enforce defined access policies across the base, camp, post, and stations.	Y	Xage implements segmentation across bases, camps, posts, and stations by establishing logical zones with tightly controlled conduits between them, preventing unauthorized lateral movement. Its fabric with centralized management and distributed enforcement overaly across all locations and applies attribute and behavior-based checks to every request, ensuring that movement between zones occurs only under defined policy. Xage also provides granular, asset-level segmentation within each zone, controlling interactions down to individual devices and services offering granular lateral movement protection. This combination of zoned architecture, controlled conduits, and fine-grained enforcement delivers strong, consistent segmentation and lateral movement protection across all locations.
5.4.1.OT	Implement Micro Segmentation	Network	Target	DoW Components implement Micro segmentation communication pathways into the Operational IT and Process Control environments, enabling basic segmentation of network addresses, VLANs, devices, endpoints, services, ports, and protocols. Basic automation is accepted for IT systems for policy changes, including API decision-making. OT systems will queue and notify proposed changes for human approval. Virtual hosting environments also implement Micro segmentation at the host/container level.	1. Micro segmentation is implemented in the OT environment. 2. Automated policy changes are enabled following human approval.	Y	Xage delivers microsegmentation across Operational IT and Process Control environments by enforcing identity and policy-based controls on every communication pathway, regardless of network address, VLAN, device type, endpoint, service, port, or protocol. Its distributed enforcement points act as secure policy enforcers, mediating each interaction and ensuring that devices and services can only communicate per policy and only through explicitly authorized conduits. Xage supports automation through API-driven policy updates as well as human-approval processes to maintain safety and operational continuity.
5.4.2.OT	Application and Device Micro Segmentation	Network	Target	DoW Components apply Micro segmentation communication pathways for all information flow, including logical network zones (e.g., VLANs, IP subnets), roles, attributes and conditional-based access control for all PEs, NPEs, and endpoints, privileged access management services for network resources, and policy-based control on API access, as appropriate.	1. Micro segmentation is implemented across all information flow, utilizing role, attribute, and condition-based access controls for PEs, NPEs, and endpoints, privileged access management services for network resources, policy-based control on API access, and logical network zones.	Y	Xage combines Privileged Access Management (PAM), secure access, and microsegmentation into a single, scalable solution that applies role, attribute, and condition-based controls across all information flows. Every interaction whether from a PE, NPE, endpoint, or service is mediated through Xage's identity-driven fabric, which restricts access to network resources, APIs, workstations, servers, PLCs/RTUs, SCADA systems and others on per policy basis. Xage utilizes multiple enforcment methods including proxies, filtering, and direct account and credential management to control access to any assets. This integrated approach delivers fine-grained microsegmentation and priviledges access management for any asset or interaction type across Operational IT and Process Control environments.
5.4.3.OT	Protect OT Data In Transit	Network	Target	DoW Components shall use protection of data in transit per policy, and include common use cases.	1. Data is protected in transit per policy through the OT environment.	Y	Xage adds policy-driven overlay encryption and integrity validation to protect data in transit for any user-to-machine or machine-to-machine interaction across OT environments and between security levels. Xage Enforcement Points (XEPs), deployed in front of individual OT assets or groups of assets, transparently encrypt traffic and verify integrity using secure tunnels established between XEPs. Policies can enforce encryption on a per-device basis or across asset groups, ensuring consistent, flexible protection of OT data in transit regardless of protocol or network limitations

6.1.1.OT	Policy Inventory and Development	Automation and Orchestration	Target	DoW Enterprise works with DoW Components to catalog and inventory existing access control policies and standards across OT system environments, including role-based access controls and policies dictating operational availability and Disaster Recovery Plans/Business Continuity Plans. Policies and standards are updated as needed.	1. Policies have been collected in reference to applicable compliance and risk 2. Policies have been reviewed and updated as needed.	Y	Xage serves as an overlay that enables consistent role-based access control for all interactions with applications, machines, devices, and data across OT and IT environments. Policies can be centrally created, inventoried, and managed within Xage, ensuring they are applied uniformly across Enterprise, Operational, and Process Control environments as well as remote sites. This unified policy framework simplifies alignment with existing standards, supports updates as requirements evolve, and ensures that access controls reflect organizational availability, continuity, and disaster recovery needs.
6.1.2.OT	Attribute-Driven Access Profiles	Automation and Orchestration	Target	DoW Components support DoW Enterprise in establishing rules, which are prioritized over local rules, as appropriate. DoW Components develop attribute-driven access profile rules for mission/task and DAAS, using appropriate cross-pillar data.	1. Enterprise rules are established. 2. Component scoped, attribute-driven profile(s) are created for mission/task and DAAS	Y	Xage's centralized policy management and distributed enforcement architecture allows enterprise-level access rules to take precedence over local rules and ensures they are applied consistently across all sites. Attribute-driven access profiles for missions, tasks, and DAAS can be defined centrally and enforced automatically through the Xage Fabric. Xage also enables unified management of identities, accounts, credentials, and policies for any asset, including legacy OT systems, providing consistent, enterprise-prioritized control regardless of the environment or device type.
6.1.3.OT	Enterprise Security Profile for OT Environments Pt. 1	Automation and Orchestration	Target	DoW Components establish minimum attributes to drive security and privacy policies. DoW Components create rules to ensure security, privacy, and integrity is aligned and in compliance with Enterprise policy.	1. Minimum attributes are established to drive security and privacy policies 2. Rules are created to ensure alignment with Enterprise policy.	Y	Xage supports this requirement by enforcing access decisions based on a defined set of minimum attributes—such as identity, role, device posture, location, time, and behavioral signals—that drive both security and privacy policies. Administrators can create centralized rules that apply these attributes consistently across all environments, ensuring that security, privacy, and data integrity requirements remain aligned with Enterprise policy. Xage's distributed enforcement fabric then applies these rules uniformly at every access point, maintaining compliance while protecting OT operations.
6.1.4.OT	Enterprise Security Profile for OT Environments Pt. 2	Automation and Orchestration	Advanced	DoW Components implement all security and privacy rules to ensure sufficient policy coverage.	1. All security and privacy rules are implemented to ensure sufficient policy coverage.	Y	Xage provides multiple enforcement methods such as authentication proxy, protocol filtering, ovelay encryption and integrity verification, and account and credential management to ensure that security and privacy policies are applied consistently across all assets, including legacy OT systems that cannot be modified.
6.2.1.OT	Process Automation Analysis	Automation and Orchestration	Target	DoW Components identify, enumerate, and document all operational processes and procedures that can be executed both manually and in an automated fashion, and identify candidates for automation.	1. Automatable operational processes and procedures are identified 2. All operational processes and procedures are enumerated.	P	Xage provides an inventory of access interactions and policies whether manual or automated.
6.2.2.OT	Tool Interoperability for OT Environments	Automation and Orchestration	Advanced	DoW Enterprise works with DoW Components to establish and prioritize baseline integration and interoperability between applicable SOAR, SIEM, and other security solutions within OT environments. Where possible, environment integration shall be done with DoW Enterprise solutions and policy services, while maintaining a human in the loop capability.	1. Baseline integration and interoperability between applicable SOAR, SIEM, and other security solutions within OT environments is established 2. Prioritization of integration efforts is completed, based on risk and operational impact. 3. Integration with DoW Enterprise solutions and policy services is prioritized and implemented where feasible.	Y	Xage integrates seamlessly with SIEM, SOAR, and other security platforms by providing standardized, machine-readable logs and real-time telemetry from every interaction across OT environments. Its API-driven architecture allows organizations to prioritize integrations based on risk and operational impact, while fully supporting enterprise-wide policy and security services. Xage also adds human-in-the-loop controls for sensitive operations through just-in-time and just-enough access, including command-level restrictions, ensuring that high-risk activities receive appropriate oversight and are executed safely.

6.3.1.OT	Implement OT Data Tagging and Classification Tools	Automation and Orchestration	Advanced	DoW Components evaluate data-driven analytic approaches, such as Machine Learning solutions or equivalent capabilities, as needed to increase capability for orchestrated workflows and risk management processes. Solutions are tested with existing tagged and classified data repositories to establish baselines with a supervised approach to continually improve analysis.	1. Implemented data tagging and classification tools are integrated with analytic tools, utilizing existing tagged and classified data repositories. 2. A supervised learning approach is established to establish baselines and continually improve the accuracy and effectiveness of data-driven analysis.	P	Xage enables access policies and enforcement decisions to be driven by insights from deployed analytic tools operating on tagged and classified data. As analytics solutions generate signals such as risk scores, anomalies, or sensitivity indicators, Xage can incorporate these into its real-time policy engine to adjust access, require additional authorization, or restrict sensitive operations.
6.5.1.OT	OT Response Automation Analysis	Automation and Orchestration	Target	Identify and enumerate all workflow processes that are potential optimization candidates, to improve response automation using advanced analysis techniques. Manual tasks are assessed for possible automation, or partial automation that maintains a human-in-the-loop. Remaining manual processes are documented for exception and are periodically revaluated for possible automation.	1. All workflow processes are identified and enumerated. 2. Manual processes are assessed for automation. 3. Remaining manual processes are documented for exception and are periodically revaluated for possible automation.	P	Xage provides an inventory of access interactions and policies whether manual or automated. As well as identifies which access workflows have human-in-the-loop controls.
6.5.2.OT	Implement SOAR Tools in OT Environment	Automation and Orchestration	Target	DoW Components work with DoW Enterprise to develop a standard set of requirements for OT SOAR solutions to operate in OT environments. DoW Components use approved requirements to procure and implement SOAR solutions in the OT environment, while maintaining a human in the loop capability to prevent mission impact or risk of life.	1. Develop requirements for SOAR tool 2. Procure SOAR tools.	N	Xage partners and integrates seamlessly with SOAR tools through its APIs and standardized data exports, enabling automated workflows, incident response actions, and policy-driven remediation.
6.5.3.OT	IAC within OT Environments	Automation and Orchestration	Advanced	DoW Components review existing manual and automated processes to prioritize Infrastructure as Code (IAC) development for automation within the OT Environment.	1. When possible IAC principles are applied to automate workflow capabilities 2. Manual processes are automated when possible.	Y	Xage integrates resource authorizations with a CI/CD pipeline through its "Policy as Code" approach. Because all access policies in Xage can be managed via API, they can be defined in text files (like YAML or JSON) and stored in a code repository such as Git. When an administrator needs to change an authorization, they simply update the policy file and commit it. The CI/CD pipeline automatically detects this change, runs tests, and then uses the Xage API to programmatically push the new or updated authorization rule into the production environment.
6.6.1.OT	API Patterns for OT Environments Pt. 1	Automation and Orchestration	Target	The DoW Enterprise works with DoW Components to establish an API standard (or equivalent automated interchange mechanism) which outlines the approved patterns and protocols for tooling inclusive of the OT environment. The standard should prioritize ensuring the safety, reliability, and resilience of the OT Environment with the diverse OT componentry implemented.	1. API standard is established for tooling.	Y	Xage API's are pupose built for the OT environments making security controls available consistently across any asset even legacy assets. Xage API's are also designed for security, safety, and high availability.
6.6.2.OT	Tool Compliance Analysis for OT Environments	Automation and Orchestration	Target	Automation and orchestration tooling and solutions are reviewed to identify existing APIs that they provide. These APIs are analyzed for compliance with existing API machine-readable patterns and protocols established by DoW Enterprise, or the necessary modifications are documented to achieve alignment.	1. Existing APIs within automation and orchestration tooling are assessed for compliance with established DoW Enterprise API standards. 2. Non-compliant APIs are documented with necessary modifications to achieve alignment with DoW Enterprise standards.	Y	Xage API's are pupose built for the OT environments making security controls available consistently across any asset even legacy assets. Xage API's are also designed for security, safety, and high availability.

6.6.3.OT	API Patterns for OT Environments Pt. 2	Automation and Orchestration	Target	DoW Components ensure that all applications and services implement API protocols as appropriate. Enterprise and/or Operational IT environments shall prioritize interoperation with APIs. Applications and services that are unable to interoperate are scheduled for eventual retirement, and alternative equivalent capability solutions for operational gaps must be identified.	1. API calls and schemas are implemented at prioritized areas within the OT environment 2. Applications and services that cannot meet standardization are marked for eventual retirement 3. Alternative equivalent capability solutions are identified.	Y	Xage enables secure, policy-driven access control through APIs for any asset—including legacy OT systems that lack native API support. By mediating all interactions through its enforcement fabric, Xage exposes standardized, API-based control points that allow Enterprise and Operational IT environments to interoperate without requiring changes to underlying devices. This allows organizations to modernize their access architecture while continuing to use legacy applications and services safely.
6.6.4.OT	API Patterns for OT Environments Pt. 3	Automation and Orchestration	Advanced	DoW Components ensure that all applications and services implement API protocols. Applications and services that were marked for retirement are decommissioned. If decommissioning presents an operational gap, an alternative must be implemented.	1. All applications and services implement the standard API calls and schemas. 2. Applications and services that cannot meet API standardization requirements are either retired or replaced with alternative solutions.	Y	Xage enables secure, policy-driven access control through APIs for any asset—including legacy OT systems that lack native API support. By mediating all interactions through its enforcement fabric, Xage exposes standardized, API-based control points that allow Enterprise and Operational IT environments to interoperate without requiring changes to underlying devices. This allows organizations to modernize their access architecture while continuing to use legacy applications and services safely.
6.7.1.OT	Incident Response Guidance for OT Environments Pt. 1	Automation and Orchestration	Target	DoW Enterprise works with DoW Components to establish cybersecurity incident response guidance utilizing threat feeds from 7.5.1.OT. DoW Components establish appropriate incident response processes for OT environments based on each environment's standard operating procedures.	1. Threat events are identified. 2. Incident response workflows for threat events are developed. 3. DoW Component establishes and documents OT-specific incident response processes, aligned with the Enterprise guidance and their existing standard operating procedures.	P	Xage helps identify potential malicious activity through granular visibility into all user, NPE, and system interactions, and it can supply high-fidelity telemetry to external threat detection tools for deeper analysis including logs, session recordings, and transcripts. When threat events are detected, Xage supports incident response workflows by enforcing automated mitigation actions such as isolating affected assets, terminating risky sessions, or blocking unauthorized communication pathways to prevent contagion from spreading across the OT environment.
6.7.2.OT	Incident Response Guidance for OT Environments Pt. 2	Automation and Orchestration	Advanced	DoW Components identify and establish extended incident response guidance for advanced response types in alignment with 7.2.3.OT. This includes developing and incorporating incident response playbooks for any event to support OT engineers and security managers. Enrichment data sources are used for existing workflows to identify emerging, evolving, and advanced threat events.	1. Guidance for advanced threat events are developed; Advanced Threat events are identified 2. Enrichment data is utilized for advanced incident response.	P	Xage helps identify potential malicious activity through granular visibility into all user, NPE, and system interactions, and it can supply high-fidelity telemetry to external threat detection tools for deeper analysis. When threat events are detected, Xage supports incident response workflows by enforcing automated mitigation actions such as isolating affected assets, terminating risky sessions, or blocking unauthorized communication pathways to prevent contagion from spreading across the OT environment.
7.1.1.OT	Scale Considerations for OT Environments	Visibility and Analytics	Target	DoW Components are required to analyze current OT infrastructure and resource capabilities and capacities for adopting zero trust functionality, and project a growth curve aligned with planned mission needs. The team works with existing Continuity of Operations teams to ensure continuous mission support.	1. Future scaling needs are determined for current conditions, as well as for mission growth and emergencies.	Y	Xage acts as an overlay that delivers Zero Trust security without requiring changes or upgrades to existing OT assets. It discovers assets, identifies their interactions, and applies granular identity-based access controls including MFA, microsegmentation, continuous session monitoring, and privileged access management to enforce Zero Trust principles across the environment. By layering these controls on top of existing systems, Xage enables secure modernization at scale while preserving operational continuity and supporting mission-driven growth. Xage's distributed architecture scales horizontally as demand increases across the entire Enteperise, Operational, and OT footprints without creatings any bottlenecks or single points of failure.

7.1.2.OT	Log Parsing in OT Environments	Visibility and Analytics	Target	DoW Components identify and prioritize collection of all log, event, alert, and flow sources in the Operational IT and Process Control environments within the OT environment, and for data flow to the Enterprise IT and external environments. DoW Components and DoW Enterprise, with vendor support, map existing vendor log content and create a DoW Enterprise machine consumable pattern. The established DoW Enterprise pattern is provided as a contract element for vendor capability alignment.	1. Rules developed for each log format. 2. All log, event, alert, and flow sources are identified in the OT environment and are collected and mapped.	Y	Xage provides identity-enabled visibility across Operational IT and Process Control environments by generating detailed logs on users, machines, devices, applications, and data interactions including session recordings and command-level activity. These logs offer deep insight into operational behavior and can be exported via APIs or syslog in standardized, machine-readable formats that align with DoW Enterprise logging patterns. This ensures Xage's telemetry can be integrated seamlessly into enterprise-wide log collection, analysis, and vendor alignment efforts.
7.1.3.OT	Log Analysis in OT Environments	Visibility and Analytics	Target	DoW Components work with DoW Enterprise to develop common behaviors, and identifies and prioritizes behaviors based on all relevant documented processes, including distinct operating modes. Ensure log data has sufficient attributes to analyze the behavior model.	1. Common behaviors are developed or identified, and are prioritized based on all relevant documented processes. 2. Log data has sufficient attributes to analyze behavior model~~.~~	P	Xage performs its own behavioral analysis to support adaptive access decisions and also provides detailed, attribute-rich activity logs to external analytics systems. This ensures behavior models have the necessary data for accurate analysis while enabling coordinated detection and response across operating modes.
7.2.1.OT	OT Infrastructure Incident Response Isolation	Visibility and Analytics	Target	DoW Components will ensure that the interconnections between Enterprise IT, Operational IT, and Process Control infrastructure are designed to be disconnected physically or logically during a detected incident to prevent any further intrusion or damage. The infrastructure must prevent reconnection until the incident is cleared. A controlled recovery procedure for testing and validation is used during reconnection to maintain system integrity and reduce the risk of recurring issues.	1. Enterprise IT, Operational IT, and Process Control infrastructure can be physically or logically disconnected in a safe and reliable manner, and this capability is regularly tested and validated to ensure effectiveness during incident response. 2. Controlled recovery procedure testing and validation process to maintain system integrity is used.	Y	Xage provides granular isolation capabilities across environments, sites, systems, and individual devices, allowing interconnections between Enterprise IT, Operational IT, and Process Control infrastructure to be logically disconnected during an incident. Isolation can be triggered directly from Xage's central management system, ensuring rapid containment and preventing reconnection until the incident is cleared. Before enforcing isolation policies, Xage supports monitoring modes that reveal dependencies and communication paths, enabling controlled testing and validation so recovery procedures maintain system integrity and prevent recurring issues.
7.2.2.OT	Threat Alerting for OT Environments Pt. 1	Visibility and Analytics	Target	DoW Components procure and implement a SIEM solution, or integrate, with an Enterprise SIEM. Data feeds are ingested, identified from the CTI program established in 7.5.1.OT, to develop rules and alerts for the OT environment.	1. SIEM solution is procured and implemented for OT environment. 2. Data feeds are ingested. 3. Rules and alerts are developed for the OT environment.	P	Xage integrates with SIEM solutions by providing standardized, identity-rich logs and telemetry that support rule creation and alerting for OT environments. Xage also tamperproofs its audit logs with the Fabric, to prevent an attacker from covering their tracks by changing or deleting logs.
7.2.3.OT	Threat Alerting for OT Environments Pt. 2	Visibility and Analytics	Target	DoW Components expand threat alerting and develop deviation anomaly rules to detect advanced threats utilizing the data feeds established in 7.2.2.OT.	1. Threat alerting is expanded by incorporating data feeds resulting in a measurable increase in the number of detected threat indicators. 2. Deviation anomaly rules are developed and implemented to detect advanced threats and reduce false positive rates.	P	Xage enhances threat alerting by supplying detailed access and behavior telemetry that increases detectable indicators and supports the development of anomaly-based rules to identify advanced threats while reducing false positives.
7.2.4.OT	Threat Alerting for OT Environments Pt. 3	Visibility and Analytics	Advanced	Threat Alerting is expanded to include advanced data sources, such as UEBA and UAM. These advanced data sources are used to develop and improve anomalous and pattern activity detections and event triggers.	1. Identify Triggering Anomalous Events 2. Implement Triggering Policy. 3. Anomalous and pattern activity detections are developed and continuously improved using data from UEBA and UAM, resulting in a reduction in undetected threats.	P	Xage provides rich UAM data and behavior signals that can feed into UEBA and other analytics tools, enhancing anomalous activity detection and improving the accuracy of threat alerts and event triggers.

7.2.5.OT	OT Asset ID and Alert Correlation	Visibility and Analytics	Target	All PEs and NPEs in SIEM are identified and correlated to alerts in order to provide security teams with accurately detailed information and asset IDs. Event visualization indicates which asset ID is affected by detected event.	1. All PEs and NPEs within the SIEM are identified and correlated to alerts, providing security teams with accurately detailed information and asset IDs. 2. Event visualization clearly indicates the affected asset ID for each detected event. 3. Automated responses are developed based on asset ID, enabling faster and more targeted incident response.	Y	Xage can export its asset inventory with unique asset IDs and associated events directly to SIEM platforms, ensuring accurate correlation for both PEs and NPEs. It also provides detailed visibility into interactions between assets and users, allowing security teams to quickly understand which systems are affected during an event and how activity is related across the environment.
7.2.6.OT	OT Baselines	Visibility and Analytics	Target	DoW Components develop a subject/attribute baseline approach based off of typical patterns and behaviors from activity 7.3.2.OT.	1. Subject/attribute baseline are established.	P	Xage provides the baseline activity data needed to establish typical behavior patterns, along with indicators of potential malicious activity such as excessive login attempts, time-travel behavior, repeated policy violations, and detected or blocked malware.
7.3.1.OT	Implement Analytics Tools for OT Environments	Visibility and Analytics	Target	DoW Enterprise works with DoW Components to develop and provide minimum requirements for Analytics Tools capabilities to analyze all data. Any analytic tools under consideration by DoW Components for implementation shall be subject to these requirements.	1. Minimum requirements for analytic tools are developed.	Y	Xage can work with DoW to support this requirement
7.3.2.OT	Establish OT Baseline Behavior	Visibility and Analytics	Target	DoW Components utilize analytics tools developed for OT environments to analyze baseline operational behavior patterns across the entire OT environment, and to identify patterns and deviations from the normal baseline.	1. Analytics tools are utilized to establish baseline behavioral patterns for OT environment, and deviations from these baselines are identified and investigated to proactively detect anomalous activity and potential threats. 2. UEBA capabilities improve the accuracy of threat detection by reducing false positives and identifying previously undetected malicious activity.	P	Xage supplies the granular, identity-linked data needed for analytics tools and UEBA systems to build accurate behavioral baselines in OT environments. This includes detailed logs on user actions, NPE activity, device posture, session behavior, command execution, policy violations, access patterns, and attempted or blocked interactions. Xage also supports adaptive access by continuously evaluating these signals in real time—adjusting privileges, requiring step-up authentication, or terminating sessions when behavior deviates from expected norms. Xage also provides a converged visibility to protection policy and enforcment workflows - not only detecting actual interaction patterns, but using those observation to create policies to support desired, but block undesired, interactions.
7.4.1.OT	OT Environment Baseline and Profiling	Visibility and Analytics	Target	DoW Components, utilizing the developed OT baselines, create threat profiles to assess the level of risk of deviations from normal baseline. Threat profiles should be used for prioritization of events and integrated into access profile rules developed for system triage.	1. Threat profiles are developed to assess level of risk. 2. Events are prioritized based on developed threat profiles.	P	Xage identifies risky behaviors and deviations from normal patterns and also integrates with partner analytics tools by supplying identity-enabled activity data from the OT environment. This rich telemetr covering users, NPEs, assets, commands, and policy violations supports the creation of accurate threat profiles and helps prioritize events. These profiles can then be incorporated into Xage's access rules for automated triage and adaptive enforcement.
7.5.1.OT	OT Cyber Threat Intelligence Program Pt. 1	Visibility and Analytics	Target	The DoW Enterprise works with DoW Components to develop an OT CTI program. The CTI program identifies and integrates common data feeds with an OT SIEM solution for improved alerting and response. Integrations with enforcement points are created to monitor CTI-driven data alerting and response for the Enterprise IT, Operational IT, and the Process Control environments.	1. An OT-focused CTI program is established, defining processes for identifying, analyzing, and disseminating threat intelligence. 2. The CTI program integrates relevant data feeds into the SIEM solution that is deployed in the OT environment. 3. CTI-driven data alerting and response are integrated with enforcement points across Enterprise IT, Operational IT, and Process Control environments.	P	Xage supports OT CTI programs by integrating with SIEM and threat intelligence feeds and by serving as an enforcement point that can act on CTI-driven alerts across Enterprise IT, Operational IT, and Process Control environments. Xage provides identity-rich telemetry to enhance CTI analysis and can automatically enforce containment or access restrictions based on threat intelligence signals. As a member of CISA's JCDC, Xage also contributes to and benefits from collaborative cybersecurity insights, strengthening its ability to support DoW alerting and response.

7.5.2.OT	OT Cyber Threat Intelligence Program Pt. 2	Visibility and Analytics	Advanced	DoW Components expand their CTI program to develop a community of interest that includes identified stakeholders. Authenticated, private, and controlled CTI data feeds are integrated into the OT SIEM solution and utilized by the appropriate PEPs.	1. The OT CTI program is expanded to include authenticated, private, and controlled CTI data feeds 2. A CTI community of interest is established, identifying and engaging key stakeholders.	P	Xage supports the expansion of OT CTI programs by enabling secure collection of identity- and activity-based telemetry from isolated environments without exposing them to direct external connections. This allows authenticated, private CTI feeds to be integrated safely while maintaining OT isolation. Xage's centralized management also helps engage stakeholders by providing shared visibility into OT security posture and activity data.