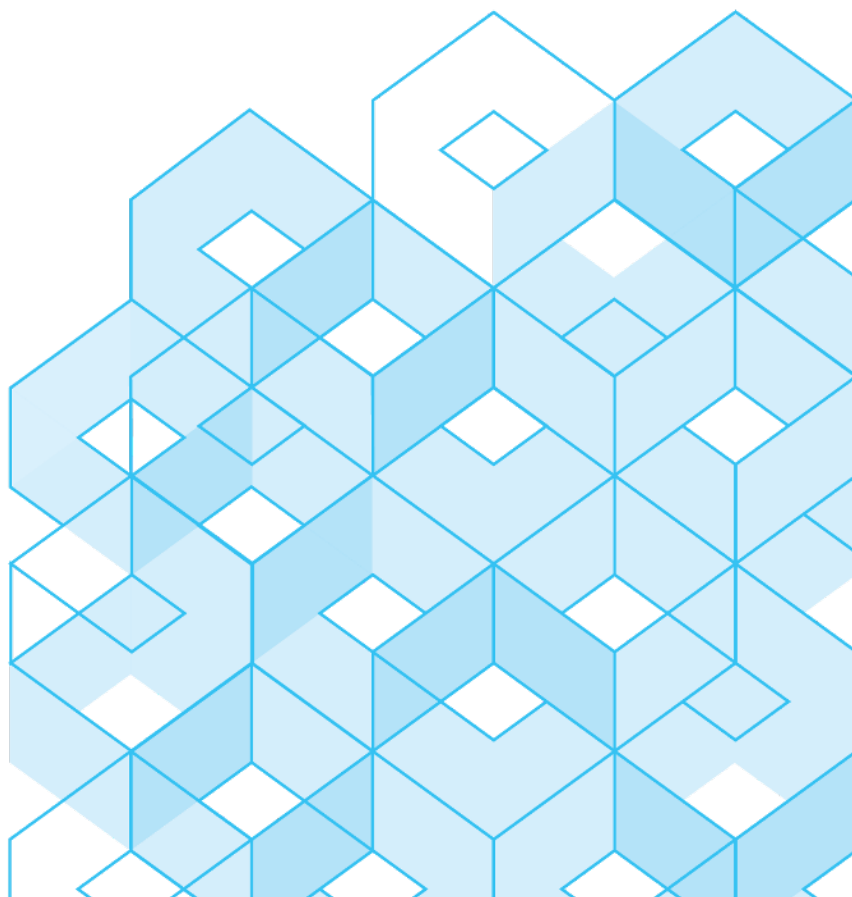




# Complying with the TSA Pipeline Cybersecurity Directives

Updated July, 2023



# Contents

<a href="#"><u>Introduction</u></a>	3
<a href="#"><u>Complying with TSA Cybersecurity Measures</u></a>	5
<a href="#"><u>Documentation to Establish Compliance</u></a>	16
<a href="#"><u>How does the Xage Fabric work?</u></a>	17
<a href="#"><u>Onsite Access Management</u></a>	18
<a href="#"><u>Remote and Onsite Access Management</u></a>	19
<a href="#"><u>Zero-trust Segmentation and Data Security</u></a>	21

# Introduction

To combat the increasing number of cyber attacks targeted at critical infrastructure, the Department of Homeland Security's Transportation Security Administration (TSA) has issued a series of security directives that have been regularly updated from 2021-23 to increase security posture of owners and operators of gas and liquid pipelines in the USA. The TSA guidelines are applicable to operational oil and natural gas and hazardous liquid transmission pipeline systems, natural gas distribution pipeline systems, and liquefied natural gas facility operators.

Most recently, TSA's directive [Security Directive Pipeline-2021-02D](#) was renewed as of July 26, 2023 superseding Security Directive Pipeline-2021-02C, in a continuation of the series of [Pipeline Security Directives](#) first published in July 2021. The renewed security directive takes a performance-based approach to enhancing security, allowing operators to leverage new technologies and be adaptive to changing environments to achieve the ultimate objective of cyber hardening critical Operational Technology (OT) and IT systems.

Highlights of TSA cybersecurity requirements include:

- Implement access control measures, including for local and remote access, to secure and prevent unauthorized access to Critical Cyber Systems<sup>1</sup>.
- Reset memorized secrets (passwords) on schedule or if not feasible provide mitigation measures.
- Limit access to shared accounts and ensure individuals who no longer need access do not have knowledge of the password.
- Enable multi-factor authentication, or other logical and physical security controls to provide risk mitigation commensurate to multi-factor authentication.
- Establish policies and procedures to manage access rights based on the principles of least privilege and separation of duties. If this is not feasible, then provide compensating controls.
- Implement network segmentation policies and controls designed to prevent operational disruption if OT and/or IT systems are compromised.
- Ensure prompt containment of an infected server, asset, or device. Segregate the infected network (or devices) to prevent the spread of the malicious code.
- Implement policies and procedures to prevent, detect, and respond to potential cyber threats.
- Develop a patching process and if not feasible, implement mitigating controls.
- Develop a Cybersecurity Assessment Plan (CAP)" to proactively assess the effectiveness of cybersecurity measures and resolve vulnerabilities.

---

<sup>1</sup> **Critical Cyber System** is defined by the TSA as "any Information or Operational Technology system or data that, if compromised or exploited, could result in operational disruption."

SD02D went into effect on July 26, 2023. The revised security directive still requires owners/operators to submit an implementation plan to TSA for approval within 90 days of the directive's effective date. Additionally, owners/operators are required to submit an assessment plan to TSA within 60 days following the approval of its implementation plan. The July 2023 updates to the directive are focused on testing and auditing of the cybersecurity measures required in the initial versions of the directive. The updates require pipeline operators to:

- Annually submit an updated Cybersecurity Assessment Plan to TSA for review and approval.
- Annually report the results from previous year assessments, with a schedule for assessing and auditing specific cybersecurity measures for effectiveness. TSA requires 100% of an owner/operator's security measures be assessed every three years.
- According to the updated security directive, the five CIRP objectives identified by TSA for pipeline operators are containment, segregation, secure access to critical systems, integrity of backup data, and isolation of IT from OT systems. The directive requires that operators must test at least two of these Cybersecurity Incident Response Plan (CIRP) objectives, and report the findings to TSA each year.

Xage offers owners/operators a holistic approach to meet TSA requirements without having to rely on multiple point solutions. The Xage Fabric cybersecurity mesh approach eliminates the need to "rip and replace" any existing Operational Technology (OT) to rapidly comply with TSA directives. Xage is being deployed now by the owners/operators of U.S. pipelines to comply with TSA requirements, improve security posture, and defend against escalating cyberattacks targeting critical infrastructure.

The Xage zero trust security solution provides the following capabilities to meet the key requirements specified in the TSA security directives:

- **Access and Credential Management:** TSA continues to stress the criticality of access control and credential management. Xage enables granular identity-based access and credential management for all assets– including legacy assets – powered by its patented Xage Fabric. The Xage Fabric seamlessly overlays an operation to impose granular control over all interactions, without any disruptive changes to your assets or operational network.
- **Compensating Controls and Multi-layer MFA:** For the many critical systems that lack their own strong security controls and/or security integrations, the Xage Fabric provides zero trust-based access control with support for multi-layer MFA to deliver the "compensating controls" required in the newest TSA directive. [Xage's multi-layer MFA capability](#) combines zero trust with a defense-in-depth authentication strategy.
- **Secure Zones, Multi-hop Conduits and Asset-centric Segmentation:** TSA requires operational environments to be segmented into zones, interconnected with secure, controlled conduits, to prevent contagion from zone-to-zone in the event of breach. The Xage Fabric acts as a mesh, enabling session and protocol termination at each Xage node. The mesh approach guarantees the security of cross-zone conduits between the nodes and ensures that there is no unauthorized access to assets from outside or within each zone.

# Complying with TSA Cybersecurity Measures

This section provides a detailed explanation of cybersecurity measures specified in the TSA's third directive (SD02C) and the capabilities Xage offers to comply with the TSA's requirements.

Section	Directive Requirement	How Xage Helps You Comply
A	Identify the Owner/Operator's Critical Cyber Systems as defined in Section VII. of this Security Directive.	Xage automatically discovers and categorizes IT and OT assets, as well as all the interactions between assets to identify process and network interdependencies. Xage's asset-centric approach enables the operators to easily identify and designate Critical Cyber Systems (or groups of systems) as protected assets to focus enforcement of security policies on these critical assets. Xage also enables the operators to gradually extend the security protection to the remainder of the assets.
B	Implement network segmentation policies and controls designed to prevent operational disruption to the Operational Technology system if the Information Technology system is compromised or vice versa.  As applied to Critical Cyber Systems, these policies and controls must include:	Xage Fabric provides the technical controls for granular segmentation of all systems across IT and OT. Virtual groups (zones) and interaction policies are created using the Xage Manager and enforced across the deployment using the Xage Fabric. All interactions (user-to-machine, machine-to-machine, app-to-machine) are authenticated and authorized according to policy following zero trust principles. In case of IT system compromise, the impacted IT systems are isolated and OT systems can continue to operate per security policy.
B.1	A list and description of  (a) Information and Operational Technology system interdependencies;  (b) All external connections to the Operational Technology system; and	(a) Xage user interface depicts the network topology and layering of various security zones complying with the Purdue model, visually explaining interdependencies.  (b) Interaction data adds extra visibility and details to interactions between IT and OT assets.

	<p>(c) Zone boundaries, including a description of how Information and Operational Technology systems are defined and organized into logical zones based on criticality, consequence, and operational necessity.</p>	<p>(c) Additionally, asset groups can be organized based on a variety of criteria including criticality, consequence, and necessity as well as function, location, ownership. Each interaction boundary is explicitly defined and enforced through the Xage Fabric.</p>
B.2	<p>An identification and description of measures for securing and defending zone boundaries, that includes security control</p> <p>(a) To prevent unauthorized communications between zones; and</p> <p>(b) To prohibit Operational Technology system services from traversing the Information Technology system, unless the content of the Operational Technology system is encrypted while in transit.</p>	<p>Xage enables granular control of all interactions between user, device, machine, and app across IT and OT sites. Xage Fabric acts as a multi-hop mesh, providing session and protocol termination at each zone via a Xage node. This mesh approach guarantees the security of cross-zone conduits between the nodes and ensures that there is no unauthorized access to assets from outside or within each zone.</p>
C	<p>Implement access control measures, including for local and remote access, to secure and prevent unauthorized access to Critical Cyber Systems.</p> <p>These measures must incorporate the following policies, procedures, and controls:</p>	<p>Xage Fabric combines zero trust principles and defense-in-depth to enact granular access control for all assets at all locations across OT, IT, and Cloud. This includes legacy and new assets, such as apps, workstations, servers, PLCs, RTUs, meters, and sensors. Xage deploys as an overlay with no clients, no agents, and no network changes. The distributed architecture of the Xage Fabric enables granular access control for remote (North-South) and local interactions (East-West) alike even when sites lose network connectivity.</p>
C.1	<p>Identification and authentication policies and procedures designed to prevent unauthorized access to Critical Cyber Systems that include</p>	<p>Xage enables identity-based authentication, authorization, and enforcement for all interactions. This includes interactions with assets that do not have built-in authentication controls, such as passwords, keys, or other credentials.</p>

	<p>(a) A schedule for memorized secret authenticator resets; and</p> <p>(b) Documented and defined mitigation measures for components of Critical Cyber Systems that will not have passwords reset in accordance with the schedule required by the preceding subparagraph (C.1.a) and a timeframe to complete these mitigations.</p>	<p>(a) Xage Fabric rotates asset (app, machine, device) credentials on a per session, schedule, or on demand basis.</p> <p>(b) Xage Fabric provides compensating and commensurate controls to deliver identity-based authentication to assets that do not have credentials (memorized secrets). Xage controls all asset access on a per policy basis and prevents all unauthorized access by utilizing overlay authentication proxy and filtering approaches.</p>
C.2	<p>Multi-factor authentication, or other logical and physical security controls that supplement password authentication to provide risk mitigation commensurate to multi-factor authentication. If an Owner/Operator does not apply multi-factor authentication for access to industrial control workstations in control rooms regulated under 49 CFR parts 192 or 195, the Owner/Operator shall specify what compensating controls are used to manage access.</p>	<p>Xage Fabric enables multi-layer MFA on a per organization, site, and asset (app, machine, workstation, server, device) basis for access to both IT and OT systems. Multi-layer MFA can be enacted on OT assets such as PLCs, RTUs, workstations, servers, meters, and sensors that do not have built-in MFA support. Xage acts as an overlay delivering MFA for any asset interaction satisfying commensurate and compensating control requirements.</p> <p>Xage's unique approach is specifically designed for operational environments with multi-layer Purdue Model deployments combining zero trust with defense-in-depth to protect against emerging threats such as "MFA bombing" attacks.</p>
C.3	<p>Policies and procedures to manage access rights based on the principles of least privilege and separation of duties. Where not technically feasible to apply these principles, the policies and procedures must describe the compensating controls that the Owner/Operator will apply.</p>	<p>With Xage, access is granted based on identity, role, and policy, to accelerate the implementation of the "least privilege concept." Xage Fabric enables secure access management with multiple factor authentication (MFA) to any asset including workstations, apps, RTUs, PLCs, meters, and sensors, even if they don't have passwords or keys.</p>
C.4	<p>Enforcement of standards that limit availability and use of shared accounts to those that are critical for operations,</p>	<p>Xage enables managed identity-based access for both local and remote interactions with assets such as workstations, HMIs, PLCs, RTUs,</p>

	<p>and then only if absolutely necessary.</p> <p>When the Owner/Operator uses shared accounts for operational purposes, the policies and procedures must ensure</p> <p>(a) Access to shared accounts is limited through account management that uses principles of least privilege and separation of duties; and</p> <p>(b) Individuals who no longer need access do not have knowledge of the password necessary to access the shared account.</p>	<p>applications, and servers. Individual accounts and credentials for all assets under management are automatically created and rotated, where possible, eliminating the need for shared accounts</p> <p>(a) For assets that only support static accounts, Xage automatically rotates credentials on those assets and stores them in a tamper proof vault. Access to the rotated credentials is controlled on the principles of least privilege and requires MFA using the user's unique managed identity.</p> <p>(b) Xage automatically rotates credentials on a per session, on-demand, or regular scheduled basis, limiting their use. As soon as the user or group is removed from the access policy, the user or group no longer has access to the asset or the credential.</p>
C.5	<p>Schedule for review of existing domain trust relationships to ensure their necessity and policies to manage domain trusts</p>	<p>Xage Fabric manages users and asset access policies spread across multiple Identity Providers (IdPs), including support for multiple Microsoft Active Directory (AD) instances across IT and OT environments. As part of the multi-layer authentication approach, the Xage Fabric can use separate ADs (and domains) for each layer of IT and OT while automating the management of users, groups, and credentials (creation, deletion, modification of accounts, groups, and credentials) across multiple ADs.</p>
D	<p>Implement continuous monitoring and detection policies and procedures that are designed to prevent, detect, and respond to cybersecurity threats and anomalies affecting Critical Cyber Systems.</p> <p>These measures must include:</p>	<p>Xage Fabric continuously discovers and monitors IT and OT assets – including Critical Cyber Systems – and interactions between assets to identify potential anomalous behavior.</p> <p>Xage's identity-based, zero trust security model proactively protects critical infrastructure by dramatically reducing the vulnerable attack surface. Granular and real-time zero trust access policies also reduce the frequency of alerts and eliminate noise. Identity-driven access</p>



		management adds unmatched context to OT activity log data, e.g. excessive failed login attempts, spraying attacks, flooding attacks, stolen credential use, and more. This identity-enriched forensic evidence streamlines root cause analysis and speeds incident response.
D.1	<p>Capabilities to:</p> <p>(a) Prevent malicious email, such as spam and phishing emails, from adversely impacting operations;</p> <p>(b) Prohibit ingress and egress communications with known or suspected malicious Internet Protocol addresses;</p> <p>(c) Control impact of known or suspected malicious web domains or web applications, such as by preventing users and devices from accessing malicious websites;</p> <p>(d) Block and prevent unauthorized code, including macro scripts, from executing; and</p>	<p>(a) Xage complements email security solutions adding a layer of protection. By regularly rotating asset and user credentials and enforcing multi-layer MFA for all interactions, Xage prevents malicious use of stolen/phished accounts and credentials.</p> <p>(b) Malicious protocols are identified and automatically blocked for all interactions including user-to-machine and machine-to-machine in both North-South and East-West. Only protocols specifically allowed per security policy permitted to ingress and egress.</p> <p>(c) Xage protects against initial pivoting, command and control, and other tactics that use known or suspected web domains to carry out exploits. Malicious web applications often exploit shared user accounts. Xage prevents such exploits by creating session specific credentials with OTP, thus obsoleting the need to use shared credentials. Xage ensures every interaction between user-to-device and between device-to-device is strictly authorized based on policies.</p> <p>(d) Xage also protects from the impact of any unauthorized code running on the customer's host/VMs by disallowing any unauthorized request to the Xage protected devices. Additionally, Xage's distributed ledger technology is tamper-proof from any unauthorized code, including macro scripts, from executing.</p> <p>(e) Xage mandates that every authorized</p>

	<p>(e) Monitor and/or block connections from known or suspected malicious command and control servers (such as Tor exit nodes, and other anonymization services).</p>	<p>connection goes through its encrypted tunnels and enforces protocol termination at each hop. The Xage Fabric use of proxy services ensures that all connections and sessions always stay within its encrypted tunnels. Additionally, Xage uses AES-256 encryption standard to encrypt all data between devices. The secured and authorized network segmentation Xage provides – along with encrypted data protection – removes any possibilities for Tor exit nodes or other anonymization services to infiltrate or exfiltrate critical data in/out and to cause any damage.</p>
D.2	<p>Procedures to:</p> <p>(a) Audit unauthorized access to internet domains and addresses;</p> <p>(b) Document and audit any communications between the Operational Technology system and an external system that deviates from the Owner/Operator's identified baseline of communications;</p> <p>(c) Identify and respond to execution of unauthorized code, including macro scripts; and ·</p> <p>(d) Implement capabilities (such as Security, Orchestration, Automation, and Response) to define, prioritize, and drive standardized incident response activities.</p>	<p>(a) Xage restricts and logs any unauthorized access to IT/OT assets at ingress and egress. Restrictions are enforced through user defined policies.</p> <p>(b) Xage enables asset-centric segmentation by defining an identity-centric perimeter around an OT asset or group of assets. This enables owners/operators to isolate OT systems from external systems. Any communication between external systems and OT systems is strictly policy-driven and every interaction is audit logged and reported with details.</p> <p>(c) Xage includes integrated malware scanning for any file transfer. Xage automatically blocks malware initiated by malicious macros before they impact the endpoint. Xage also blocks any unauthorized asset access via code or macro scripts and logs unauthorized access attempts.</p> <p>(d) Xage aids incident investigation and forensics with identity-enabled interaction recordings and logs. By providing a unique identity to each user and asset and enforcing the use of managed identities, Xage creates identity-enriched audit trails for investigations</p>

		<p>and forensics. Xage integrates with Security Incident and Event Management (SIEM) solutions to provide identity-enabled visibility into events and interactions. Xage offers a centralized management platform with a single pane of glass for monitoring, management, and policy definition. Policy enforcement is distributed across the Xage Fabric for automatic and dynamic control over all interactions for simplified incident response.</p> <p>(e) Additionally, Xage products and services can help verify the integrity of backup data to ensure effective and speedy recovery in cases where certain systems must be restored.</p>
D.3	<p>Logging policies that:</p> <p>(a) Require continuous collection and analyzing of data for potential intrusions and anomalous behavior; and</p> <p>(b) Ensure data is maintained for sufficient periods to allow for effective investigation of cybersecurity incidents.</p>	<p>(a) Xage Fabric continuously discovers assets and monitors interactions between assets. Xage enforces access control per defined policy with any policy violations, potential intrusions, and anomalous behavior logged, reported, and proactively blocked.</p> <p>(b) All audit logs and recordings are maintained for a customizable time period by the system.</p>
D.4	<p>Mitigation measures or manual controls to ensure industrial control systems can be isolated when a cybersecurity incident in the Information Technology system creates risk to the safety and reliability of the Operational Technology system.</p>	<p>Xage Fabric ensures that OT systems can safely operate even when IT assets are compromised with security controls to isolate individual systems and groups of systems.</p>
E	<p>Reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers, and firmware on Critical Cyber Systems consistent with</p>	<p>Xage partners and integrates with multiple vulnerability management and patch management solutions to identify assets, vulnerabilities, and securely deliver patches to any asset in multi-layer networks.</p>

	the Owner/Operator's risk-based methodology. These measures must include	
E.1	A patch management strategy that ensures all critical security patches and updates on Critical Cyber Systems are current.	Xage's consulting and professional services team works with the customer to develop a vulnerability and patch management strategy optimized for the types of assets, interactions, vulnerabilities, and risk mitigation objectives.
E.2	<p>This strategy required by paragraph E.1 must include:</p> <p>(a) The risk methodology for categorizing and determining criticality of patches and updates, and an implementation timeline based on categorization and criticality; and</p> <p>(b) Prioritization of all security patches and updates on CISA's Known Exploited Vulnerabilities Catalog.</p>	<p>(a) Xage works with the customer to develop a schedule for system updates and patches that aligns with criticality of patches and maintenance schedules to achieve desired availability and security objectives. Additionally, Xage offers compensating controls to protect unpatched systems to keep operations running.</p> <p>(b) Xage works with the customers to reconcile and prioritize asset inventories against the Cybersecurity and Infrastructure Security Agency (CISA) Known Exploited Vulnerabilities Catalog.</p>
E.3	If the Owner/Operator cannot apply patches and updates on specific Operational Technology systems without causing a severe degradation of operational capability to meet necessary capacity, the patch management strategy must include a description and timeline of additional mitigations that address the risk created by not installing the patch or update	Xage Fabric can limit or eliminate the exposure of vulnerable systems and protocols ensuring the necessary protection measures to keep operations running. Xage understands some OT systems are hard to or cannot be patched. Xage Fabric delivers compensating controls to protect these systems through zero trust based granular access control and malware scanning (overlay endpoint protection).
F	Develop and maintain a Cybersecurity Incident Response Plan	Xage provides the security controls for an effective Cybersecurity Incident Response program including ability to identify, investigate, and mitigate incidents across IT and OT environments.

F.1	<p>Owner/Operators must have an up-to-date Cybersecurity Incident Response Plan for the Critical Cyber System that includes measures to reduce the risk of operational disruption, or the risk of other significant impacts on necessary capacity, should their pipeline or facility experience a cybersecurity incident.</p> <p>The Cybersecurity Incident Response Plan must provide specific measures sufficient to ensure the following objectives, as applicable:</p> <p>(a) Prompt containment of the infected server or device.</p> <p>(b) Segregation of the infected network (or devices) to ensure malicious code does not spread by, as necessary -</p> <ol style="list-style-type: none"> <li>I. Segregating (removing from the network) the infected device(s);</li> <li>II. Segregating any other devices that shared a network with the infected device(s);</li> <li>III. Preserving volatile memory by collecting a forensic memory image of affected device(s) before powering off or moving; and</li> <li>IV. Isolating and securing all infected and potentially infected devices, making sure to clearly label any equipment that has been affected by malicious code.</li> </ol>	<p>Xage Fabric helps you achieve Cybersecurity Incident Response objectives in the following ways:</p> <p>(a) Xage enables dynamic isolation and containment of threats by providing identity context with distributed controls through the Xage Fabric to streamline incident response.</p> <p>(b) In case of an incident, users and devices can be rapidly isolated anywhere Fabric Nodes are deployed, including remote sites, by utilizing the Xage Management Tools or programmatically via REST APIs.</p> <ol style="list-style-type: none"> <li>I. Xage Fabric operationalizes the zero-trust principle of controlling all interactions based on the identity of the asset (machines). When the asset is isolated due an infection, all interactions from the asset including peer-to-peer interactions are blocked.</li> <li>II. When an infected computer is isolated, remaining unaffected assets in the group continue to interact as per policy to ensure high availability in the operational environment.</li> <li>III. Infected systems can be isolated remotely using the Xage Fabric. Through granular controls for all asset interactions, systems can be isolated with a simple policy update and enforced throughout the environment. Labels and</li> </ol>
-----	---	---

	<p>(d) Established capability and governance for isolating the Information and Operational Technology systems in the event of a cybersecurity incident that results or could result in operational disruption.</p> <p>(e) Exercises to test the effectiveness of procedures, and personnel responsible for implementing measures, in this Cybersecurity Incident Response Plan, no less than annually.</p>	<p>annotations are applied through the Xage Fabric for all isolated assets.</p> <p>(d) Xage Fabric provides security controls on a per asset and asset group basis for each part of the operation. Policies are defined centrally and enforced across the operation through a distributed mesh architecture. Additionally, with the multiple site admin capability, administrators can define and enforce asset policies for their respective sites and systems without the potential of disrupting others. In the event of IT and OT isolation, the Xage Fabric continues to operate without interruption.</p> <p>(e) Xage Fabric can be switched between monitoring and enforcement modes allowing testing procedures without risking operational disruption. The effectiveness of access management policies is indicated through detailed logs, audit trails, and visual representations.</p>
G	Develop a Cybersecurity Assessment Plan for proactively assessing and auditing cybersecurity measures.	Xage partners with customers to develop Assessment Plans and Programs based on a detailed review of existing cybersecurity controls and identified gaps with TSA guidelines. Xage also assists customers with implementation of required cybersecurity measures to meet the TSA requirements and provides periodic, proactive assessments to ensure compliance.
G.1	The Owner/Operator must develop a Cybersecurity Assessment Plan for proactively assessing Critical Cyber Systems to ascertain the effectiveness of cybersecurity measures and to identify and resolve device, network, and/or system vulnerabilities.	Xage verifies device authenticity in the field, based on owner, manufacturer, location, and device fingerprints. Xage Fabric tracks assets and enrolls legitimate devices in the multi-vendor trust system, which helps the owner/operator identify and resolve device, network and system vulnerabilities with precision and speed.
G.2	The Cybersecurity Assessment Plan required by Section III.G.1 must	Xage partners with customers to complete stand-alone or periodic cybersecurity assessments which include:

	<p>(a) Assess the effectiveness of the Owner/Operator's TSA-approved Cybersecurity Implementation Plan;</p> <p>(b) Include an architectural design review at least once every two years that includes verification and validation of network traffic and system log review and analysis to identify cybersecurity vulnerabilities related to network design, configuration, and inter-connectivity to internal and external systems; and</p> <p>(c) Incorporate other assessment capabilities, such as penetration testing of Information Technology systems and the use of "red" and "purple" team (adversarial perspective) testing.</p>	<p>(a) <b>Current Cybersecurity Profile Assessment</b> to measure compliance with TSA guidelines. This includes a review of existing access policies, asset inventories, and interaction logs and events. Xage explicitly tests the effectiveness of implemented cybersecurity policies and control measures.</p> <p>(b) <b>Target Cybersecurity Profile Development</b> Services aimed at helping owners/operators to comply with TSA guidelines. This includes architecture, design, development and update of cybersecurity policies, processes (such as assessment plans) and procedures with implementation of technical security controls.</p> <p>(c) Periodic/on-going cybersecurity gap analysis, compliance reviews, and assessments to help owners/operators stay up to date with evolving TSA requirements.</p>
--	--	--

# Documentation to Establish Compliance

Directive Requirement	Xage Capability
<p>The Owner/Operator must make records necessary to establish compliance with the requirements of this Security Directive available to TSA upon request for inspection and/or copying.</p> <p>(a) Hardware/software asset inventory, including supervisory control, and data acquisition systems.</p> <p>(b) Firewall rules.</p> <p>(c) Network diagrams, switch and router configurations, architecture diagrams, publicly mutable internet protocol addresses, and Virtual Local Area Networks.</p> <p>(d) Policy, procedural, and other documents that informed the development, and documented implementation of, the Owner/Operator's Cybersecurity Implementation Plan, Cybersecurity Incident Response Plan, Cybersecurity Assessment Plan, and assessment or audit results.</p> <p>(e) Data providing a "snapshot" of activity on and between Information and Operational Technology systems, such as:</p> <ul style="list-style-type: none"> <li>• Log files;</li> <li>• A capture of network traffic (i.e., packet capture (PCAPs)), not to exceed a period of twenty-four hours, as identified and directed by TSA;</li> <li>• "East-West Traffic" of Operational Technology systems/sites/environments within the scope of this Security Directive's requirements; and</li> <li>• "North-South Traffic" between Information and Operational Technology systems, and the perimeter boundaries between them.</li> </ul>	<p>Xage Fabric automatically collects the required information to establish compliance, as applicable and appropriate. This information includes:</p> <p>(a) full asset inventories and interaction maps</p> <p>(b) policies demonstrating allowed asset interactions.</p> <p>(c) segmentation policies and optionally related architectural and network diagrams as part of a consulting and services engagement</p> <p>(d) procedural requirements and implementation details as well as test results are documented and provided to customers as part of Xage services engagement</p> <p>(e) identity-enabled network logs for East-West and North-South interactions with audit logs and session recordings.</p>







# How does the Xage Fabric work?

The Xage Fabric uses a mesh-protected distributed architecture for delivering security services to any location, IT, OT, and Cloud. The following security services are provided by the Xage Fabric:

- **Identity and Access Management (IAM)** for all interactions including user-to-machine (or app), machine-to-machine, app-to-machine as well as end-to-end data encryption and access control with per-asset credentials rotation (including PLCs/RTUs), strong authentication, and MFA.
- **Zero Trust Secure Remote Access** with file transfer, malware scanning, and multi-party capabilities to any asset at any location including IT, Cloud, DMZ, and operational Purdue Model environments.
- **Zero Trust Data Exchange** provides end-to-end, granular data access management, authenticity, integrity, and confidentiality from the OT edge to IT/Cloud and to the ecosystem, enabling objective and trusted data sharing across multiple parties.

The Xage Fabric is composed of the following components:

 <b>Xage Node</b>	Xage Nodes (XNs) form the mesh-protected fabric by connecting to each other using secure tunnels to direct access and transfer data. Xage Nodes provide authentication, authorization, and enforcement for all interactions. XNs rotate asset (app, machine, device) credentials on a per session basis. Xage Nodes also provide tamper-proof storage of access policy information, credentials, and operational data. Xage Nodes can be deployed as VM appliances or hardware appliances.
 <b>Xage Broker</b>	Xage Broker (XB) connects the Xage Fabric with central services such as Active Directory or LDAP systems. XB synchronizes accounts, credentials, policies and shared data between centralized services, Xage Manager, and distributed Xage Nodes. Xage Broker runs as a VM alongside Xage Manager.
 <b>Xage Manager</b>	Xage Manager (XM) enables security policies to be defined centrally and then replicated and enforced across the Xage Fabric. Xage Manager also provides overall Xage Fabric system deployment, upgrade, configuration, monitoring, reporting and fault management capabilities. Xage Manager can be hosted and managed by Xage with Xage Cloud or hosted as a VM on-premises.
 <b>Xage Enforcement Point</b>	Xage Enforcement Points (XEPs) provide protocol-agnostic access filtering plus dynamic data security with authenticity, integrity, and encryption. XEPs are an optional component of the Xage Fabric designed to protect assets that do not have built-in security controls and provide in-transit data encryption where needed. XEPs ship as an appliance and are deployed in line at the asset locations, typically in front of switches. A single XEP can support multiple assets and multiple asset types per deployment location.

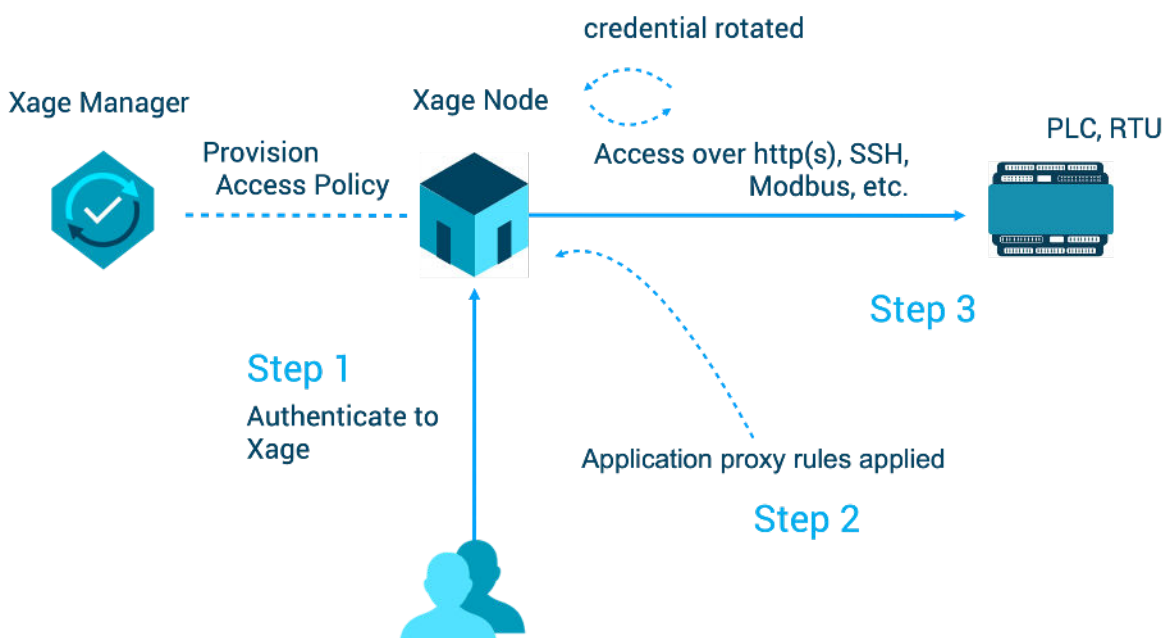
## Onsite Access Management

Typical Xage Fabric deployment for onsite access management contains a Xage Node deployed within a site and Xage Enforcement Points in front of groups of assets, such as PLCs/RTUs. Xage Broker and Xage Manager can also be deployed within the same site typically on the same machine.

This architecture provides zero trust access management and file transfer for onsite users and assets that are network reachable through the Xage Node. A Xage Node has a built-in authentication proxy for apps, servers, devices, and workstations. Authentication with Xage Nodes is performed over a secure HTTPS connection with multi-factor authentication (MFA) support for asset access. Xage Fabric nodes manage credentials for all assets including OT assets such as PLCs/RTUs by rotating credentials using native protocols (such as Modbus) on a per session basis. Users interacting with the Xage Fabric use their managed accounts and credentials (integration with multiple AD servers is supported) and often do not even need to know actual asset credentials rotated by the Xage Fabric.

XEPs work the Xage Node to enforce network filtering rules dynamically based on policy. Once an interaction is authenticated and authorized with a Xage Node, access policy is applied on the XEP to control access to allowed assets. XEPs are protocol agnostic and work with a variety of Layer 3 and Layer 2 industrial protocols. XEPs operate at Layer 2 and are transparent in the network eliminating the need for network configuration changes.

Diagram 1: Zero trust access and credential rotation for OT assets

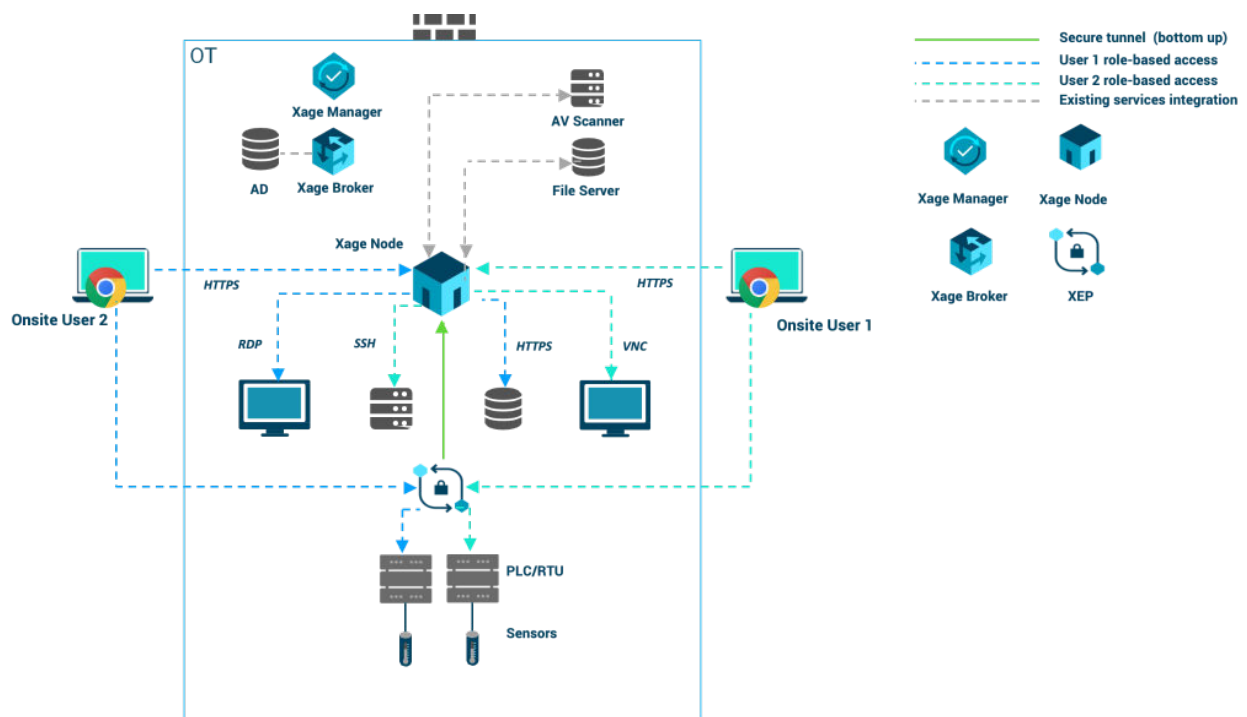


Each Xage Enforcement Point can support multiple devices and device types. XEPs are deployed:

- Inline upstream of switches - protecting access to groups of assets or zones from all other assets
- Inline individual devices - protecting access to individual devices from all other assets
- Inline downstream of onsite workstations - protecting access to devices from workstations

File Transfer capability is supported through the same Xage Node with integrated support for pluggable malware scanners (via ICAP). Full identity-enabled audit trails and detailed screen recordings are provided for all interactions.

Diagram 2: Onsite Access Management



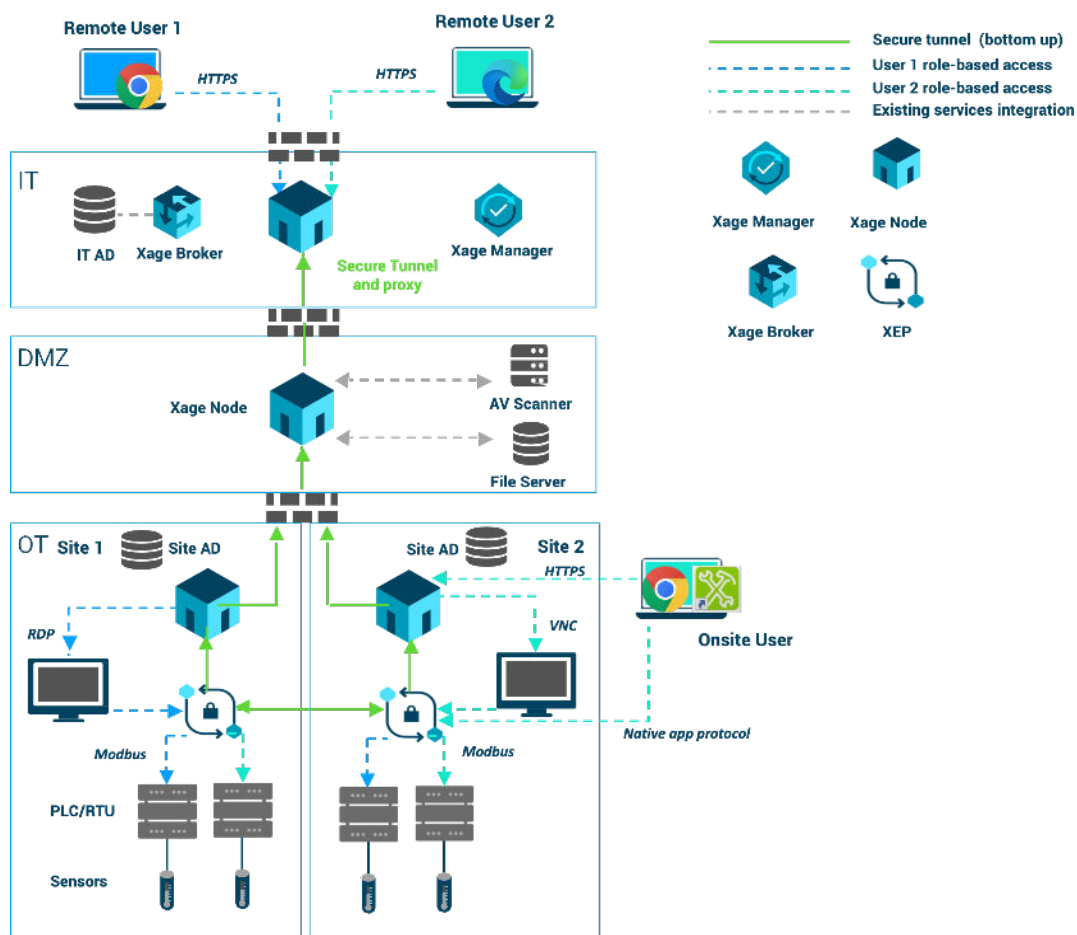
## Remote and Onsite Access Management

Operational environments commonly have a DMZ between OT (more trusted) and IT (less trusted) networks adhering to security best practices. In this architecture, all remote connections are terminated in the DMZ, scanned, and new authenticated sessions are established to OT assets. The Xage Fabric can be extended using multiple nodes in a multi-hop architecture to support remote user access as well. Each Xage Node proxies and relays the remote user interaction. Access is provided with a secure (HTTPS) browser session enabling vulnerable protocols such as RDP/VNC to be terminated inside the OT environment and never exposed.

Xage Zero Trust Remote Access provides granular identity, role, and policy-based access to individual assets. Xage Nodes establish secure IPsec tunnels automatically originating from trusted segments (OT sites) to less trusted segments (DMZ), and not the other way around. Tunnels between nodes filter interactions automatically based on authentication and authorization, reducing the reliance on firewalls and related management burden. Onsite access management can still be provided via the onsite Xage Node. Xage supports onsite access even when network connectivity to other Xage Nodes or Xage Manager and Broker are unavailable.

File Transfer services with support for pluggable malware scanners utilizing the ICAP protocol are provided via the Xage Fabric. The Xage Fabric provides a repository for transferred files with granular role-based filtering, file type filtering and malware scanning. A file repository for each user to upload and download files is available at any location (accessible via the browser) where the Xage Fabric can be reached. Xage recommends that file transfer services are deployed on the Xage Node in the DMZ to allow files to be scanned before they are transferred into more trusted environments. However, it is possible to deploy file transfer services at any Xage Node locations.

Diagram 3: Remote and Onsite Access Management



## Zero-trust Segmentation and Data Security

The Xage Fabric enables granular, zero trust segmentation. Groups of assets can be defined in the Xage Manager on per site, function, or Purdue Model layer basis. Once XNs and XEPs are deployed in various locations, the zero-trust segmentation is enforced for all interactions, vertical (North-South) and horizontal (East-West), without requiring complex VLANs and firewall rules. These segmentations can be dynamically changed by simply adjusting the policy on the Xage Manager. Furthermore, enforcement occurs on individual asset identity and interactions basis. Not just site-to-site and zone-to-zone, but rather which asset in site 1 to another asset in site 1 or site 2, and so on.

All interactions are controlled and protected by the XEP IPsec tunneling capabilities using AES 256 encryption.

Diagram 4: Asset grouping and access segmentation

