ZERO TRUST REMOTE ACCESS

Defend industrial operations from escalating threats and boost productivity

Industrial organizations are at an inflection point. Preventing costly disruptions and defending against escalating cyber threats dramatically elevates the need to modernize cybersecurity. Furthermore, staying competitive and complying with mandates continues to fuel digital transformation efforts. Meeting these requirements makes secure remote access to once-isolated operational assets more vital than ever.

The benefits of remote connectivity for operators, vendors, and supply chain partners are significant. However, increased connectivity leaves Industrial Control Systems (ICS) and Operational Technology (OT) assets vulnerable to cyberattacks. This exposure jeopardizes operational and productivity gains.

Shortcomings of IT-centric Remote Access Solutions

Addressing remote access demands – while circumnavigating the unique access control challenges of operational systems – frequently leads to an overreliance on IT-centric solutions. As a result, many industrial environments end up with a mix of disjointed access methods to enable remote connectivity to OT assets:

- **Traditional VPNs** are widely deployed but often provide all-or-nothing access when relied on for remote connectivity to critical infrastructure environments. If a remote user's credentials are compromised, attackers can gain unfettered access to OT assets.
- **Firewall rulesets and network ACLs** are cumbersome and complex to manage. Opening firewall ports expose vulnerable remote access protocols, like RDP, increasing the risk of ransomware, spoofing, and other cyberattacks. Additionally, most firewalls lack fluency in common OT protocols making fine-grained access policies difficult.
- **Jump servers and Privilege Access Management (PAM) tools** are a complicated and costly necessity to address a lack of granular policy enforcement or native device security controls. In most cases, PAM solutions cannot extend protection down to at-risk OT assets, like Programmable Logic Controllers (PLCs), diluting the full benefits of a least-privilege security model.
- **IT-centric Zero Trust Network Access (ZTNA) solutions** are an improvement over traditional VPNs for IT network access yet lack the necessary capabilities to maintain defense-in-depth across OT security layers. These solutions cannot enact granular control of access to the diversity of OT devices found in industrial environments.

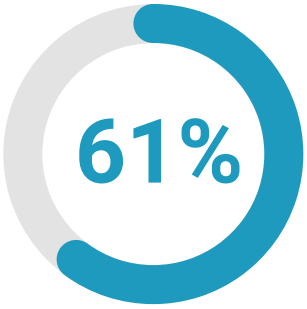
Operational environments that rely on a patchwork of point solutions suffer a suboptimal remote access experience. A poor experience impacts productivity and endangers operational safety. Additionally, disjointed access methods create the ideal conditions for cyberattacks and failed regulatory compliance.

Modernizing Secure Remote Access with Zero Trust

Operational leaders can no longer afford to settle for all-or-nothing, reactive, or disjointed remote access. Instead, industrial organizations must shift to a unified approach that delivers granular and just-in-time access controlled down to the asset level.

Adopting a zero trust approach eliminates remote access friction while adding protection that blocks most attacks before they can begin.

The benefits of a zero trust-based approach are evident. However, not all approaches are the same. It is important to pursue a secure remote access strategy that **reduces complexity** and **accelerates cyber-hardening** while **eliminating the need to rip and replace**.



61% of senior operational leaders agree reactive strategies are not enough to prevent breaches

Wakefield Research (June 2022)

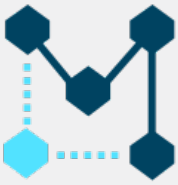
Attributes of a Zero Trust-based Approach

Identity-Driven Access

Shifts from a network-centric to an identity-centric remote access policy model, with each identity forming its own perimeter.

Continuous Verification

Strengthens cybersecurity posture by eliminating all-or-nothing access regardless of the maturity – or lack thereof – of native controls.



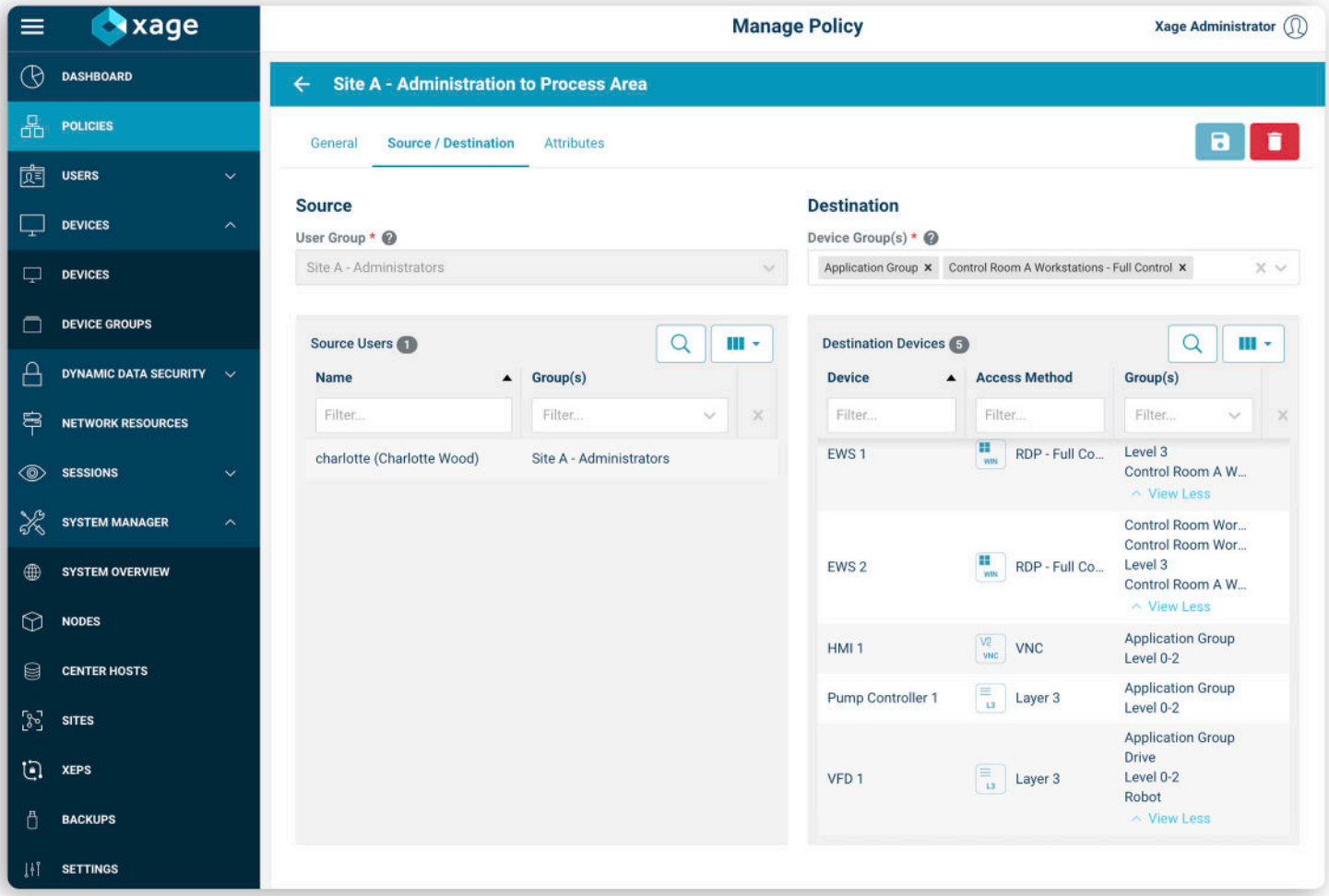
Least Privilege

Reduces vulnerable attack surface area – providing just enough access for just enough time – to accelerate cyber-hardening without disruption.

Xage Zero Trust Remote Access

Xage accelerates the adoption of a zero trust remote access approach for industrial environments.

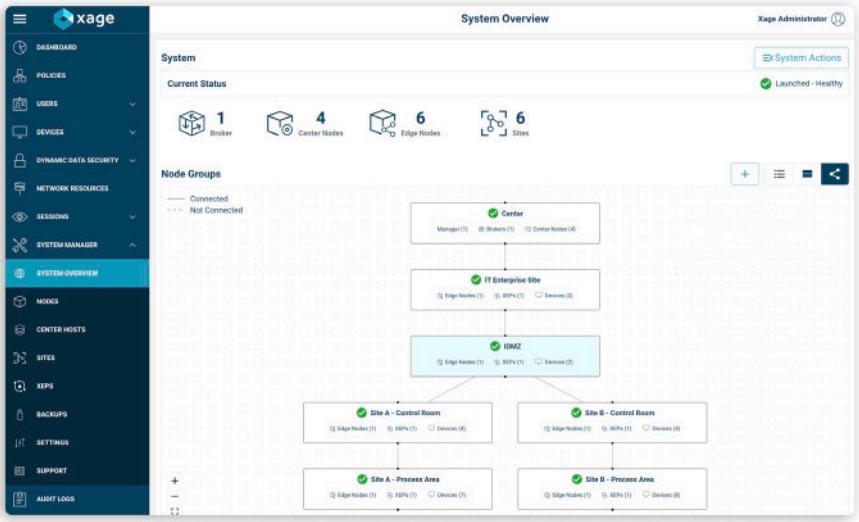
With Xage Zero Trust Remote Access, security and operational teams can easily create and enforce granular, identity-driven access policies between operational assets and remote users and applications.



The tamperproof, resilient, and highly available Xage Fabric can be deployed as an overlay across your existing OT, IT, and Cloud infrastructure. This unique mesh architecture removes the need to rip and replace your current investments or suffer disruptive operational changes to protect all digital interactions between users and assets.

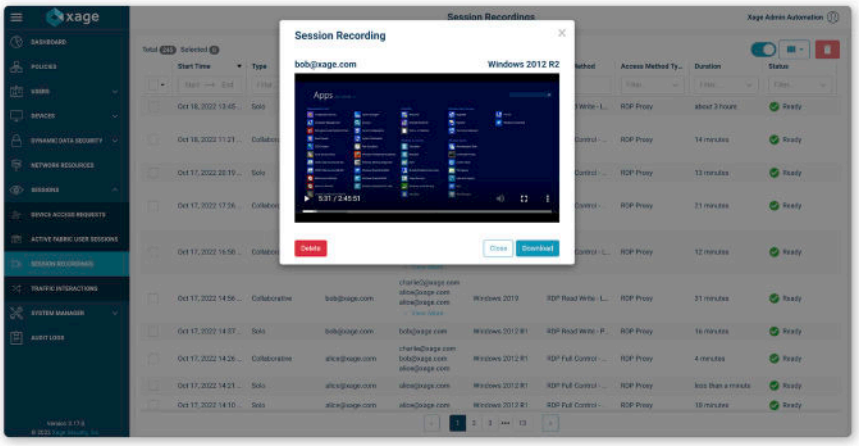
The Xage Fabric simplifies and secures remote access to and through your OT-IT DMZ. You no longer need to open multiple firewall ports for remote connectivity via common protocols – such as SSH, VNC, RDP, HTTPS, PROFINET, Modbus, or others – safeguarding your at-risk assets without impacting productivity.

Xage bolsters defense-in-depth and supports Purdue Model best practices with secure traversal of multiple network layers. The Xage Fabric multi-hop mesh eliminates direct interaction with protected OT assets, enabling session and protocol termination at each layer. These defenses further mitigate the risk of vulnerable protocol exploitation and IP spoofing by attackers.



Xage makes it easy to cyber-harden virtually any cyber-physical system. Regardless of the maturity of native device capabilities, you can add advanced security controls, like Multi-Factor Authentication, point-in-time access approval workflows, and role-based access controls.

Xage provides a single pane of glass for managing and monitoring all remote activity. Detailed reporting and audit trails – including user session recordings, identity-based logging, and user and asset identity traceability – offer unmatched visibility for incident response and demonstrating regulatory compliance.



Key Benefits

Unified Access Policy Management
Say goodbye to managing separate tools for different segments of your operations environment. Xage Policy Manager enables you to centrally create and enforce unified, granular identity-driven remote access control policies across all your operational assets and remote users.

Simplified Secure Access Experience
Whether you are a remote operator, a third-party maintenance vendor, or a supply chain partner, you'll have the same experience. The web-based Xage portal delivers friction-free remote access in seconds instead of days or weeks. There's no need for end-point agents, VPN or SASE configurations, cloud-based proxies, additional software, or having to ship out pre-configured laptops to third parties.

Seamlessly Modernize and Elevate Security Controls
Embrace cybersecurity best practices by adding new layers of security controls to virtually any device. With Xage, you can enact Multi-Factor Authentication (MFA) with support for SAML 2.0, enable Single Sign-On (SSO), implement advanced secrets management, and more – regardless of the maturity of native device capabilities.

Enable Session Collaboration Across Any Remote Access Protocol
Boost operator productivity, maintain separation of duties, or speed up technical support with session collaboration across any remote connectivity protocol, including RDP, VNC, and SSH. Xage makes it easy to securely invite other users to active remote sessions with full or view-only control without separate tools or a clunky user experience – even for air-gapped and private on-premises networks.

Protect File Transfers Across Layers
Enable flexible file sharing across Cloud, IT, and OT environments without fear of malicious software or compromised file integrity. Xage simplifies secure file transfers to and from any asset, preventing vulnerable USB and SMB file transfers. There is no need for added agents or client software to ensure end-to-end file authenticity and confidentiality. Integrated malware scanning and granular filtering safeguard critical OT files and data assets without impeding operational productivity.

Full Visibility and Control of Remote Sessions
Gain peace of mind with unmatched monitoring of all remote access activity. Xage identity-driven access unlocks context-rich visibility, including identity-based logging, auditing, traceability, and session recording. You'll always know who is accessing which assets, even if the devices lack unique user accounts, without additional agents or software installed throughout your OT environment.

Mitigate the Risks of Malware and Uncover Anomalous Behaviors
Proactively block cyber risks before they can wreak havoc across your industrial environment. Xage not only reduces vulnerable attack surface area with dynamic, granular access policies, but you can also detect and block a wide range of threats – insecure network protocols, unusual interactions between assets, malicious software, and more.

Comply with Industry and Regulatory Mandates
Rapidly meet and exceed compliance requirements and industry standards, such as NERC-CIP, IEC 62443, and TSA Cybersecurity Directives. Xage's proven zero trust defense-in-depth capabilities offer pragmatic controls to improve your industrial cybersecurity posture immediately without costly tradeoffs or disruptive changes.

Choice of Deployment Model
Be operational in less time with the flexibility to choose on-premises or cloud-based deployment options. The Xage cloud solution delivers hosted secure remote access accessible for faster deployment.

Experience the Xage Difference

Attributes	Xage Fabric	VPN	Jump Server	ZTNA
Identity-based, Least Privilege Access				
Asset-level Access Control				
Identity-Aware Access Logging				
Secure Data Transfer				
Multi-Hop Session Termination				
Multi-Factor Authentication				
End-to-End Encryption				
Session Recording				
Credential Management and Rotation				
Real-time Session Collaboration				

Customer Spotlight

One of the largest steel manufacturers in the world with dozens of plants in the United States and operations in Mexico, Brazil, and throughout Central and South America. The company has a vast footprint that requires in-depth coordination and planning to maintain security.

At the outset of the pandemic, the steel producer's personnel needed to log in remotely to manufacturing sites to maintain production. The company began to trial TeamViewer as a solution for access to their OT environments but quickly ran into limitations. Then they turned to Xage Zero Trust Remote Access:

- Achieved secure remote access across distributed manufacturing sites with Single Sign-On and MFA
- Cyber-hardened operations and mitigated financial losses resulting from cyberattacks
- Reduced cybersecurity insurance premiums by demonstrating high-security maturity
- Improved productivity from decreased user complexity in operating the solution

Accelerate Your Shift to Proactive Secure Remote Access

Xage Cybersecurity Services deliver expert assessment, design, implementation, and support services to accelerate your adoption of Zero Trust Remote Access.

Our dedicated team of industrial cybersecurity experts brings over 200 years of experience with risk management and regulatory compliance frameworks. This unmatched experience enables Xage and our global services partners to deliver modernized, secure remote access with minimal disruption.