Zero Trust Access and Security for Manufacturers

Secure assets against cyberattacks while supporting manufacturing process acceleration.

Security shouldn't slow you down, even with increasing cyberattacks on manufacturing hanging in the balance. The industry is modernizing and automating, whether pursuing Industry 4.0 initiatives or broader digital transformation approaches, but these changes bring increased risk. Zero trust cybersecurity can enable the speed and confidence you need to pursue rapid modernization in a highly competitive industry without compromising your security.

Challenges in Securing Manufacturing

Manufacturing has become the industry most targeted by cyberattacks. These attacks can mean costly downtime, ransom payments, lost intellectual property, and other financial losses. In the midst of this onslaught, manufacturing operations and security teams are challenged with ensuring that users (remote or otherwise) and assets are secured throughout the enterprise.

Key challenges:

- Protecting your bottom line while maintaining productivity and ensuring worker safety
- Securing a mix of legacy and modern technology across distributed sites
- Enabling remote access without exposing critical systems to undue risk

Modernizing Operations while Staying Secure

- **STOP ATTACKS**
  Control access based on identity with MFA, protect from vulnerabilities, and block lateral movement to stop escalating cyberattacks.
- **AVOID LOSSES**
  Eliminate risk to avoid astronomical cyber insurance premiums, financial losses, and reputational damage.
- **MAXIMIZE PROFITS**
  Modernization and digitalization must be adopted to meet production demands and maintain and optimize systems without costly downtime.

How Xage is Securing Manufacturing

One of the largest steel manufacturers in the world has 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 organization's personnel needed to log in remotely to manufacturing sites to maintain production. The company began to trial TeamViewer and Citrix as solutions for access to their OT environments but quickly ran into limitations. Then they turned to Xage Security:

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

Key Product Features

- **MFA**
  Provides MFA and multi-layer MFA for defense-in-depth.
- **NATIVE SOFTWARE**
  Supports the remote use of native software like FactoryTalk.
- **DATA TRANSFER**
  Enables secure transmission of data all from siloed, isolated, high-security networks without providing direct access to the sensor that produced it.
- **AUTOMATIC CREDENTIAL ROTATION**
  Secures access while making it easier for users with SSO and automatic credential rotation.

Why Xage?

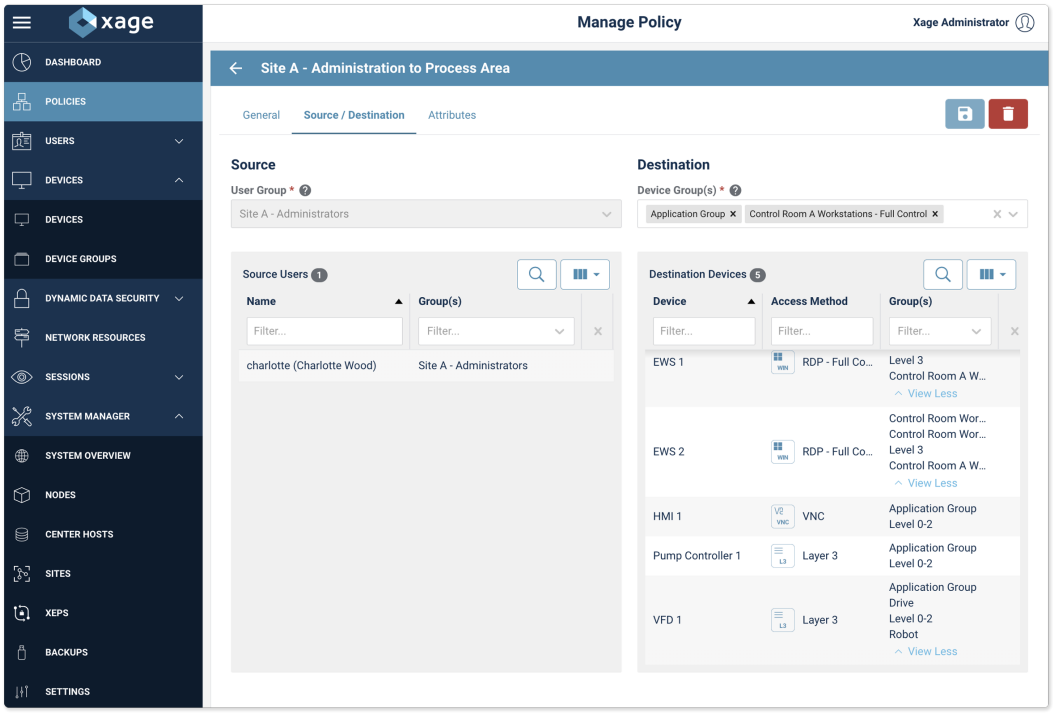
- **Block attacks and gain efficient access management which follows zero trust principles**
- **Secure file sharing—everything from patching to enabling operations to pull machine logs from the process**
- **Gain zero trust remote access that improves productivity without increasing risk**
- **Prevent lateral movement that won't be stopped by existing secure access software—by limiting user privilege**

Xage uses a decentralized mesh architecture and localized enforcement points to manage identities, access, and data transfer. This unique approach makes it easier to deploy and harder to compromise—and means it works even if a site loses connectivity.

xage SECURITY

Identity Management that Follows Zero Trust Principles

Security starts with identity. Xage delivers zero trust identity and access management, securing existing systems and data while enabling secure remote access. With Xage, your security teams can enact granular, just-in-time access control (for users and devices) down to the asset level and protect sensitive data while enabling secure remote access. This blocks malware and attacks from reaching targets on the network, even if credentials are compromised by a phishing attack—and regardless of whether it started in IT, OT, or cloud environments.



Privileged Access Management & Remote Access

Xage provides a unified system for controlling and monitoring access whether remote or not, providing the same level of granular control and tight security for all users and devices. It automatically disables accounts when not in use, taking away what is otherwise a potential tool for attackers living off the land. Access can be monitored with automatic session recording which can even be used as ready-made training materials.

No Single Point to Hack

The Xage Fabric uses a distributed mesh architecture to eliminate connection points with broad access that can be leveraged by attackers. Xage nodes connect directly to assets ensuring attackers can't circumnavigate policies, whether in a flat or segmented network. Unlike alternative ZTNA, PAM, or VPN solutions, granular, protected access to a specific service, app, dataset, or target is easily accomplished within the Xage Fabric.

xage SECURITY

Key Benefits	
Maintain Production Continuity	Pausing production to deal with a cyberattack is too costly for manufacturers. Xage blocks attacks, minimizing their blast radius so that revenue is not disrupted.
No Rip and Replace, Agents, or Additional Software	Xage acts as an overlay, connecting and securely mediating between the assets and systems you already have, protecting legacy assets from cyber-risk, and enabling them to participate fully in integrated digital operations. No need for agents or additional software.
Cyber Harden OT, IT, and Cloud	Simplify strengthening the cyber-physical security posture of your distributed assets and infrastructure resources. Xage eliminates the complexity of implementing credential management, password rotation, and other compensating controls.
Achieve Complete Visibility	Streamline asset inventorying and access activity monitoring while actively blocking cyberattacks such as ransomware. Xage protects every asset and logs every interaction, delivering identity-based access control and data security.
Gain Operational Efficiency	Enable secure remote access to maintain equipment and optimize processes while maintaining operational continuity. Xage simplifies and secures access to and through OT-IT DMZ for maintenance operations. Xage multi-party session viewing enables secure collaboration among local and remote technicians, vendors, and suppliers. It's simple to secure and administer while easily navigated for a frictionless end user experience.
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 needing additional agents or software installed throughout your enterprise IT, OT, and IoT assets.

xage SECURITY