ZERO TRUST FILE TRANSFER

Xage's Zero Trust File Transfer secures and simplifies file sharing across Cloud, IT, and OT environments with granular per user, location, and access control. Each Xage Fabric user can be configured with their own file repository enabling secure file transfer to and from any asset at any location with a Xage Fabric Node.

Zero Trust File Transfer is fully integrated with Zero Trust Access Management which simplifies administration, provides a unified user experience, and enables deployment flexibility with support for multiple DMZ and multi-layer Purdue Model environments. There are no agents or clients that are ever needed with the Xage Fabric; everything is driven through a secure browser connection.

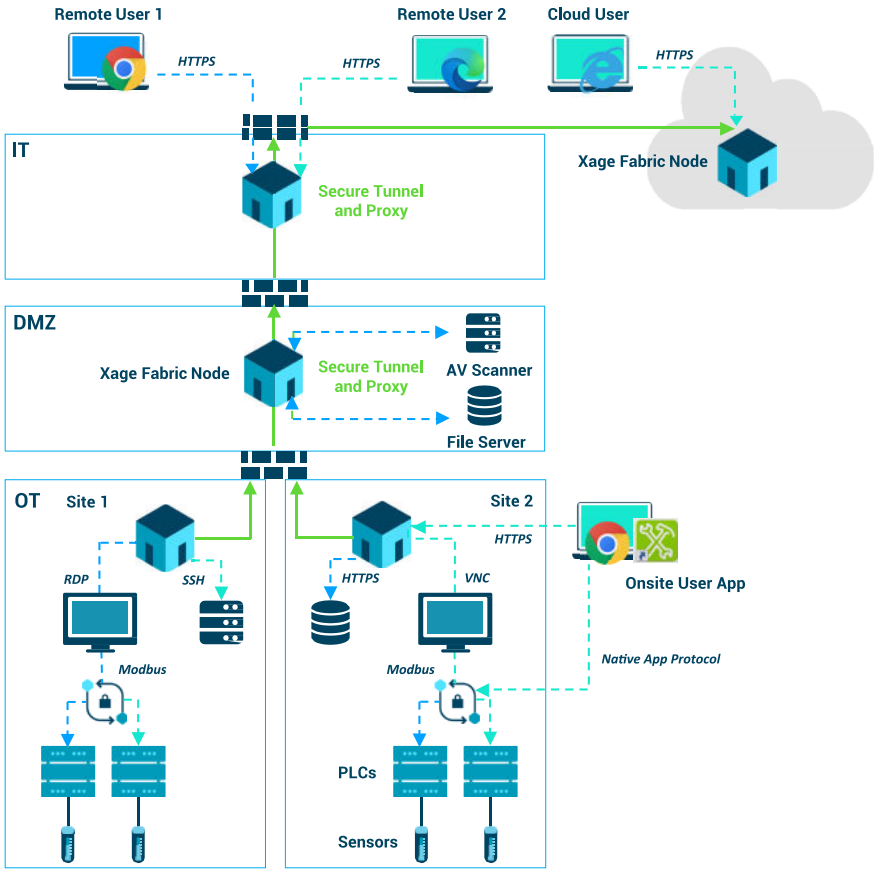
Unlike existing solutions, Xage Fabric ensures file authenticity, integrity, and confidentiality end-to-end and supports pluggable malware scanning and file type filtering at any Fabric Node.

Xage Fabric File Transfer Features and Benefits

- **Secure file transfer and sharing with granular access control across Cloud, IT, and OT**
- **Eliminates vulnerable USB and SMB transfers**
- **Bidirectional (in/out), vertical (remote), horizontal (site-to-site)**
- **Multi-hop support for DMZ and Purdue Model environments**
- **Malware and ransome protection with pluggable malware scanners (ICAP)**
- **Seamlessly integrated and protects existing file servers and storage systems**
- **Multiple file types: PLC programs, ML files, patches, logs, etc.**
- **Filtering based on file type/contents, location, size, etc.**
- **Granular control based on role, asset type, location, direction**
- **End-to-end authenticity, integrity, and confidentiality with AES 256 and Shamir Secrets**
- **Transparent user experience - no agents, no clients, no network changes**
- **Single pane of glass for management with distributed availability**
- **Regulatory compliance: TSA, NERC-CIP, IEC62443**

How does it work?

- Xage Fabric creates a virtual repository for each user with granular policy-driven control over file size, type, location and direction.
- Each user's virtual repository is available wherever Fabric Nodes exist. Xage Fabric automatically transfers files across a multi-hop mesh of Fabric Nodes with session termination, encryption, filtering, and malware scanning (ICAP).
- Each virtual repository can be mapped to an existing physical file server/storage utilizing SMB which is terminated at the immediate Fabric node and never exposed.
- Xage Fabric encrypts files in-transit utilizing reverse (from more trusted to less trusted layers) IPSec tunnels and at-rest utilizing distributed threshold based encryption (Shamir Secret Sharing and AES 256).
- Users interact with their Xage Fabric virtual file repositories over HTTPs with secure browsers utilizing their managed credentials and Multi-Factor Authentication (MFA).
- Administrators define policies through the Xage Manager with single pane of glass across the entire Xage Fabric deployment
- All interactions are logged with tamperproof audit trails



About Xage Security

Xage is the first and only zero trust real-world security company. Powered by the Xage Fabric, the company's Identity & Access Management (IAM), remote access and dynamic data security solutions allow customers to secure, manage and transform operations. With its distributed, scalable and easy-to-operate Fabric, Xage solves the complex digitization challenges of the real-world operations we rely on. Xage customers include leaders in manufacturing, energy O&G, utilities, DoD, logistics and transportation.

Xage Security
445 Sherman Avenue, Suite 200
Palo Alto, CA 94306