xage SECURITY

SECURE REMOTE ACCESS AND DATA TRANSFER

OT, IT, AND CLOUD

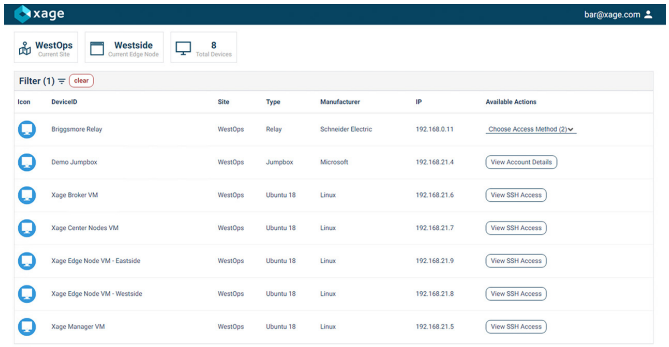
Today's industrial enterprises and operations involve complex interactions between field, control center, enterprise, and cloud. These interactions include machines and apps from a variety of vendors, often with little to no security functionality or built-in access enforcement. Additionally, access is required for people who are not part of the core organization, such as vendors, system integrators, and contractors.

In the last two years, digital attacks targeting industrial control systems (ICS), critical infrastructure, and operational technology have increased by 2000%. Attackers are targeting both applications and the underlying infrastructure (e.g. windows server applications, network equipment, industrial control systems). Malware is armed with state of the art worm-like capabilities that can easily bypass traditional security controls such as firewalls, VPNs, and Jump Boxes, and spread across IT, OT, and cloud environments.

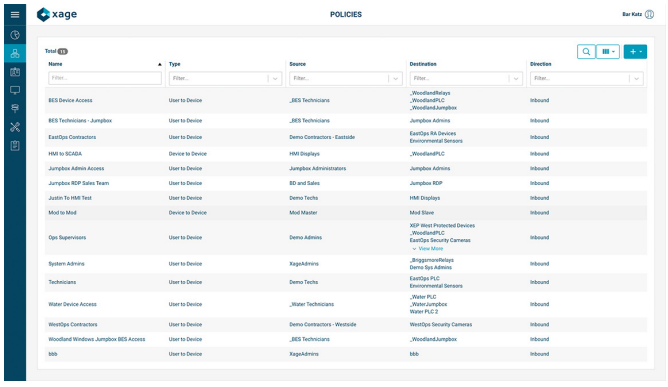
While attackers evolve rapidly, OT admins find it difficult to catch up and manage legacy security controls which are not fit to adapt. This not only requires lots of their precious time, but is also an error prone task to undertake. Users, on the other hand, have to adjust their usage to fit legacy architecture, resulting in cumbersome and complex workflows.

It has become clear that the current isolation and trust-based security approaches using Firewalls, DMZ, Jump Boxes and VPNs, have become too complex, vulnerable to exploit, and difficult to manage for today's industrial enterprises and operations.

Fabric Portal



Xage Manager



xage

Remote Access Challenges

Remote access enables process automation and optimization by ensuring that remote users and applications can effectively interact with assets distributed across the operation. However, it comes with challenges.

Ensuring granular control of remote interactions for applications, users, and machines across a complex environment with large numbers of assets is a daunting task, especially when most assets don't have any built-in security controls. Furthermore, access often needs to be granted on a temporary basis, varies based on asset, includes the need to transfer data (e.g files) and may involve third party users and applications. OT environments need a new solution that is manageable, scalable, and truly secure.

The Xage Security Fabric provides a zero-trust identity-based remote access solution for users, applications, and machines, across the field, control center, datacenter, and cloud environments. A zero trust access (ZTA) model uses identity as the perimeter, and rather than automatically assuming trust for any entity that can gain network-segment access, sets a standard that no trust should be assumed for machines, apps, or users until their identity is authenticated and their access authorized per the security policy. This approach utilizes identities and credentials to create a secure environment, and even so, grants authorization to only a limited set of interactions, and only for the required duration.

The Xage Fabric was designed specifically for OT/IoT environments and enables organizations to unlock the benefits of secure remote access without changing their underlying architecture or assets. Xage Fabric enables effective access control throughout the operation for remote, local, and 3rd party users and applications from any location, without a single point of failure, and even during intermittent connectivity.

Xage Fabric Secure Remote Access and Data Transfer

The Xage Fabric greatly simplifies access management by providing a single system to manage and enforce access security policies. The Fabric strengthens an organization's security posture by providing state of the art authentication and authorization capabilities to both modern and legacy OT environments, with strong passwords, MFA, etc. In addition, since all OT access is controlled and logged in the tamperproof Fabric, it provides visibility into all the OT interactions (user, app, machine).

Starting at the edge of the OT field environment, Xage extends into enterprise IT, the cloud, and all interactions across them. The Fabric creates holistic security from edge to cloud, with sophisticated policy learning and management capabilities built in, enabling truly secure remote access into the OT environment.

Diagram 1 - Xage Fabric unified access management for applications, machines, and data

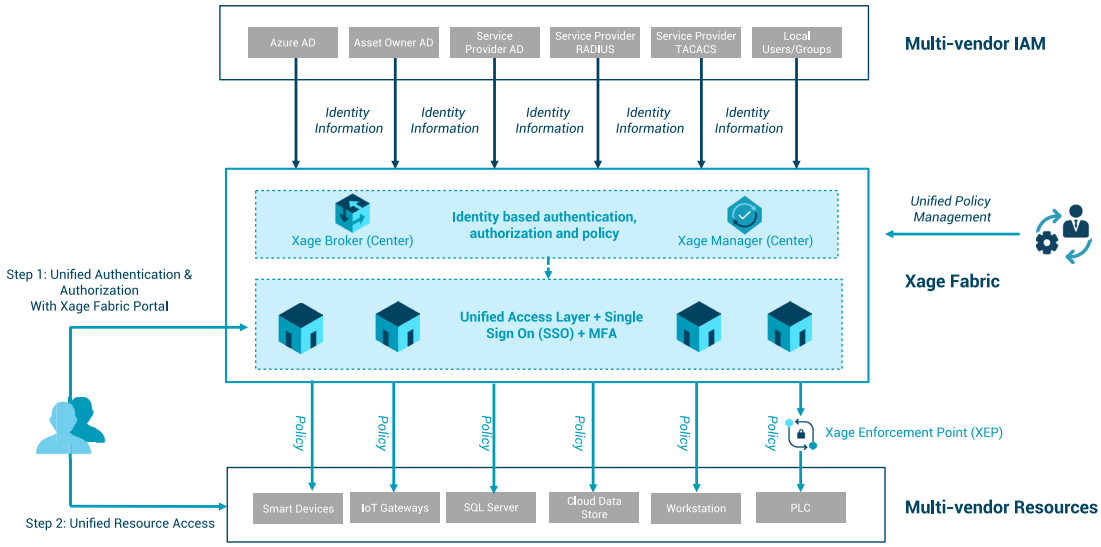


Diagram 2 -
Xage Fabric on-prem deployment for remote access

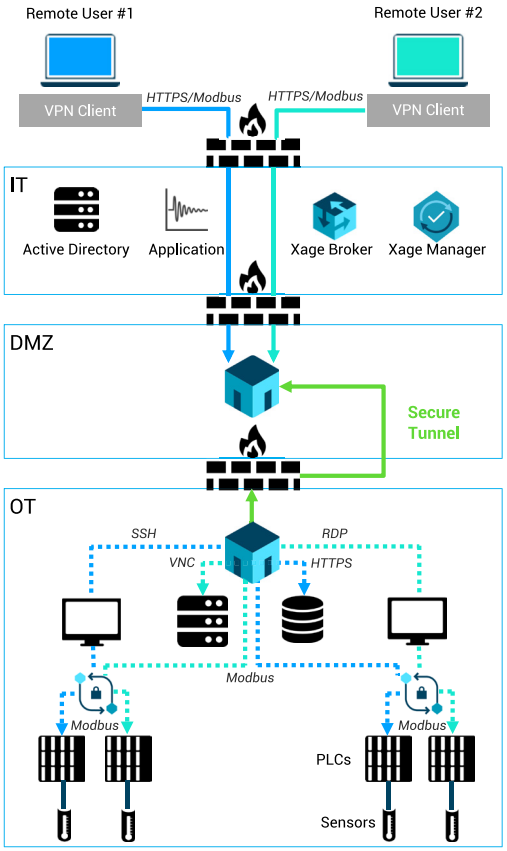
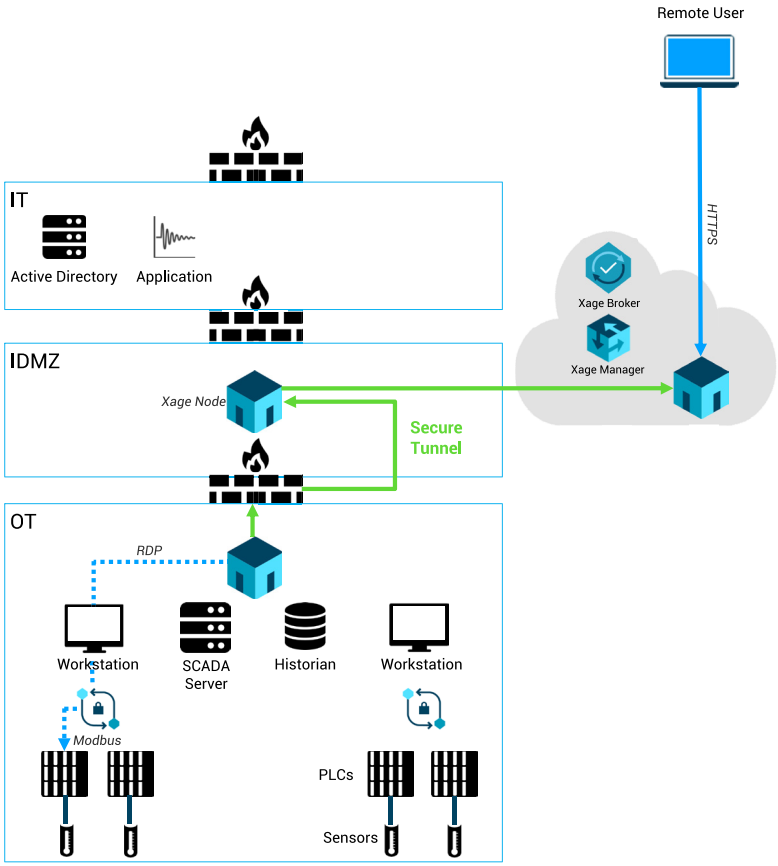


Diagram 3 -
Xage Fabric cloud deployment for remote access



The Xage Fabric enables secure remote access to OT, IT, and cloud environments and provides fine-grained identity based access control to field, enterprise, and cloud assets. Utilizing the Xage Fabric simplifies the access management and, in certain scenarios, replaces existing security controls (e.g. firewalls, VPN, Jump Boxes, Remote Desktop Gateways and Reverse Proxies) to facilitate secure remote access, thus reducing operating costs.

Xage Fabric adds security controls to assets where they are lacking or utilizes existing security controls to automatically and dynamically manage access. From creating or removing identity-based accounts on workstations and applications, all the way to managing firewall rules, port forwarding and VPN tunnels. Xage not only improves the operational security posture, but also improves operational efficiency by eliminating existing complexity and unifying access management.

In addition, Xage Fabric supports secure data (e.g. ML data, program files, logs) transfer across different operation trust zones, enterprise, and the cloud while adhering to the principles of the Purdue model. Secure data transfer utilizes the same secure tunnels used for remote access, with access control capabilities that can limit datafile type, size, content, location, originator, and destination.

Xage Fabric ensures datafile authenticity and integrity by storing the fingerprint (cryptographic hash) inside the Fabric as metadata. Using the hash, it is possible to verify file integrity and authenticity end-to-end (e.g. verify PLC program file hash against the hash in the Xage Fabric at any given time - to ensure it was not modified or tampered with).

Xage Fabric Secure Remote Access Benefits

- Secure access through OT DMZ using Xage Fabric proxy capabilities for various protocols (e.g. SSH, HTTP/S, RDP, Modbus, etc.)
- Ubiquitous Xage Security Fabric portal (in the field and in the cloud) for user and application access using identity and role-based authentication with Single Sign-on (SSO) and Multi-Factor Authentication (MFA)
- Granular identity and role-based remote access to specific assets (not just trust zones) per security policy automatically orchestrated end-to-end, and with no account, asset, or firewall changes required
- Protocol, session, and encryption termination at the Xage Fabric node, such that direct communication with protected assets is never allowed
- Access control (e.g. permitting only certain operations from certain users, based on identity) and monitoring (e.g. recording sessions and actions)
- Tamperproof audit logs for all actions and interactions
- Enables compliance to regulation and standards such as NERC-CIP and IEC 62443
- Single pane of glass for IT/OT access management and monitoring
- Secure file and data transfer into and from OT, enterprise, and cloud environments.
- Greatly simplifies both administration and user experience

Traditional Approach	Xage Approach
Different solutions for access control - remote, local, cloud; user and application; legacy and new.	Single remote access platform for field, control center, data center, and cloud assets and users with Single Sign-On (SSO) and Multi-Factor Authentication (MFA).
Remote access & data acquisition managed in **separate platforms**, complex manual configuration **per asset**.	**Single universal platform** to manage remote access & data acquisition for **all assets**.
Remote access and data acquisition rules are defined **manually**, and are **static**.	Remote access and data acquisition rules are identity-based, created **automatically**, and are **dynamic** (added and removed as needed).
Remote access to trust zones only.	Remote access to individual assets orchestrated and secured end-to-end including workstations, servers, PLCs, and RTUs.
Limited or no access control from native applications to automation equipment (PLCs, RTUs).	Granular identity-based access control to legacy and new automation assets.