

PAM for Industrial Environments

Eliminate PAM complexity. No jump servers. No agents. No cloud dependencies.

The Challenge

The majority of cyber attacks leverage stolen valid credentials for initial intrusion or lateral movement. “Use of stolen credentials” was the top most common attack vector observed in the 2023 Verizon Data Breach Investigation Report. As IT, OT, and Cloud environments become more interconnected, privileged access management (PAM) has become both more urgent and more difficult. Legacy, IT-focused PAM solutions struggle to keep up, requiring complex deployments, agents, jump servers, and heavy-duty firewall changes.

Xage PAM is More Secure and More Scalable

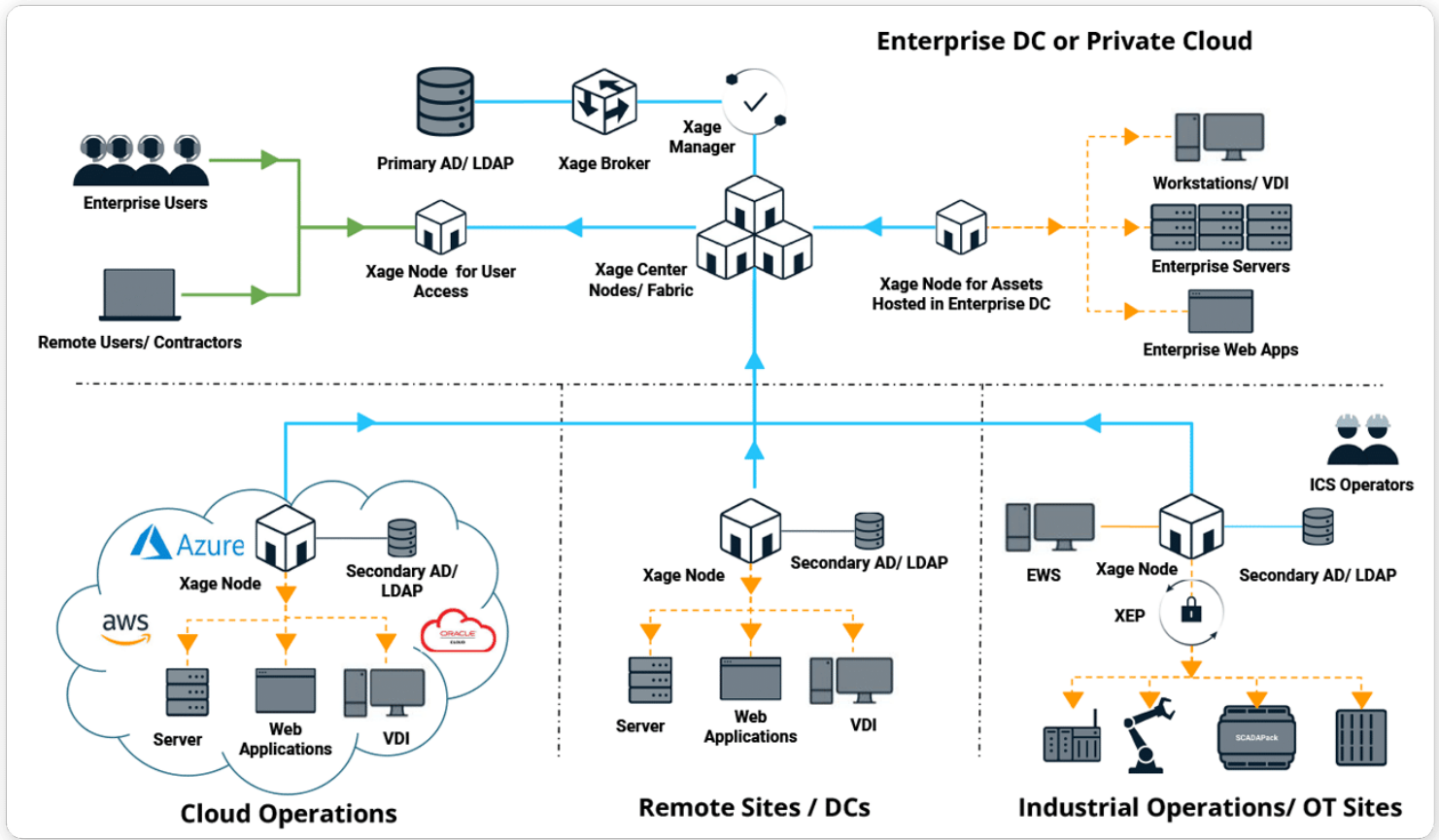
Xage goes beyond what traditional PAM can offer and addresses the modern challenges of distributed, decentralized, and interconnected OT, IT, and Cloud environments. With Xage, you get:

- **Remote Access for distributed sites, easily extending PAM** capabilities to all locations, even those with low bandwidth or loss of network connectivity.
- **Agentless PAM** that supports unmanaged assets or those with no password, or shared default administrative credentials, including PLCs, SCADA, and other OT assets.
- **Support for IT and OT protocols**, including RDP, SSH, Telnet, VNC, HTTP/s, Profinet, Modbus, and more.
- **Distributed password vault** secured by mesh architecture with no single point of failure or compromise.
- **Multi-layer access management** that traditional PAMs can't achieve.
- **Credential Management** with automated time-based or per-session credential rotation, even for legacy assets.
- **Multi-factor authentication and Single-Sign-On for every asset** at every layer, from Cloud/Enterprise IT to OT and DMZ.
- **Record and log every session**, and tie every logged event to an actual identity, even for assets with default administrative credentials.
- **Orchestrate access control across multiple identity providers** and instances across OT and IT.
- **Session collaboration with monitoring & multi-user session control**. with over-the-shoulder shadowing. Terminate sessions on demand or via REST API. Integrate with UEBA, SIEM, XDR, and EDR.
- **Secure File Transfer** with malware scanning and data integrity verification at every step and layer. Granular identity-based access control policy for file transfer and access.



Xage Privilege Access Management

Xage Privileged Access Management (PAM) is delivered Via the Xage Fabric. The Xage Fabric is overlaid on top of your existing environment architecture without requiring any network changes, rip-and-replace, or installation of any endpoint agents or clients. Xage Nodes are deployed as VMs or hardened containers and managed centrally from a browser. Then policy is enforced locally at distributed sites, and even down to individual assets. The Fabric's cybersecurity mesh architecture means there is no single point to hack, making the Fabric itself secure.



The Xage Fabric Platform is a unique distributed cybersecurity mesh that underpins Xage's Privileged Access Management (PAM) capabilities, also provides Zero Trust Access for Clouds, Zero Trust Network Access (ZTNA), Micro-segmentation, Multi-user Session Collaboration, and OT Zero Trust Remote Access.

Xage's Privileged Access Management (PAM) solution offers a full suite of capabilities:



- **Privileged Account and Session Management (PASM)**
 - Multi-user, multi-device, and concurrent session management
 - Session recording and archiving
 - Session revocations with admin privileges
 - Multi-user session collaboration, session shadowing
 - Single Sign-on with LDAP, SAML and federated access



- **Privilege Elevation and Delegation Management (PEDM)**
 - Policy-based permission control for both devices and accounts
 - Just-in-time & just-enough access
 - Approval based device access management



- **Secrets & Password Management**
 - Account discovery for Windows, Linux, Web Apps, SQL Databases etc. using Xage adapters
 - Distributed Password Vault
 - Manual password reset and verification with the remote systems
 - Automatic password rotation based on set schedules
 - Password management

Xage Universal PAM Adapter Framework

Xage offers a novel agentless approach for remote accounts and passwords discovery and management via its universal adapter framework, which can be configured, extended, and modified to work with any 3rd party system or application. Using Xage’s universal adapter framework, even new adapters can be written quickly to support new use-cases, workflows easily.

Under the hood, each adapter uses target platform complaint scripts to perform the following tasks:

1. **Accounts discovery**
2. **Password rotation**
3. **Password checkout**
4. **Password reset**

The adapter’s functionality can be easily and quickly extended to perform other custom tasks or to even automate multi-step workflows.

Xage customers have given us rave reviews across our PAM, ZTNA, and CPS protection product categories on Gartner Peer Insights.

Xage Customer Reviews

Zero Trust Network Access (ZTNA)	★★★★★	(4.6)
CPS Protection Platforms	★★★★★	(5.0)
Privileged Access Management (PAM)	★★★★★	(4.8)



© 2024 Gartner, Inc. Gartner® and Peer Insights™ are trademarks of Gartner, Inc. and/or its affiliates. All rights reserved. Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences, and should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.

