xage SECURITY

Privileged Access Management (PAM) for Interconnected IT, OT, and Cloud

No jump servers. No agents. Eliminate complexity.

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:

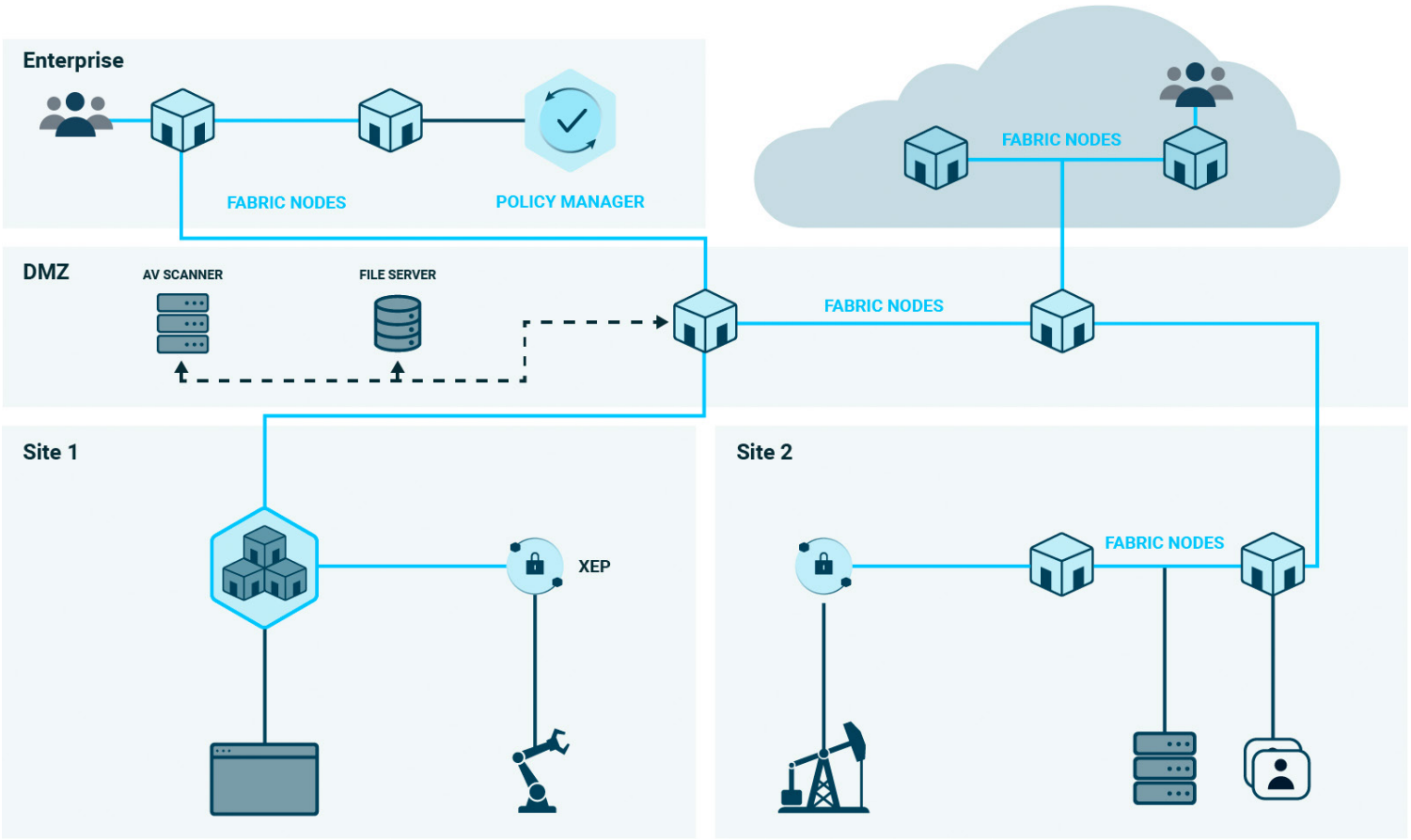
- **Agentless PAM** that supports unmanaged assets or those with no password, or shared default administrative credentials, including PLCs, SCADA, and other OT assets.
- **Support for IT and OT protocols:** RDP, SSH, Telnet, VNC, HTTP/s, Profinet, Modbus, and more.
- **Remote Access for distributed sites, easily extending PAM** capabilities to all locations, even those with low bandwidth or loss of network connectivity.
- **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, 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 SECURITY

Xage Privileged Access Management 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 supports Privileged Access Management, Identity-based Access Management, Zero Trust Remote Access, Zero Trust Data Exchange, and many other security use cases.

Xage Protects

34M+
Megawatt Hours Transported Daily

1M+
Assets and Identities Globally

1,000s
Operational Sites Globally

xage SECURITY