xage SECURITY

Extended Privileged Access Management

Expand Privileged Access Protection—Faster, Simpler, and Lower TCO

Agentless, resilient Zero Trust privileged access for IT, data centers, critical infrastructure, and other high-stakes operations. Traditional PAM is often complex, slow to deploy, and dependent on centralized infrastructure. This leaves remote sites, legacy systems, OT, contractors, and disconnected operations reliant on standing privileges, VPNs, and jump servers.

Introducing Xage XPAM

Built on the Xage Fabric Platform, Xage Extended Privileged Access Management (XPAM) closes these gaps with an agentless, distributed architecture that delivers MFA, just-in-time access, session control, credential protection, and auditability without disrupting uptime.

Agentless, Resilient Deployment

Protect distributed environments without endpoint-agent sprawl, jump-server sprawl, or VPN dependency.

Unified Privileged-Access Platform

Consolidate PAM, secure remote access, MFA/SSO, credential management, and session recording.

No Single Point of Security Failure

Continue operating locally even when cloud or central-site connectivity is unavailable.

Lower Total Cost of Ownership

Reduce infrastructure, licensing, and operations associated with fragmented PAM tools.

How XPAM is Different than Traditional PAM

Expands What Counts as Privileged

Protect semi-privileged, third-party, machine, application, and AI identities - not only administrators.

Faster Time to Value

Agentless deployment without network redesign, endpoint agents, or multi-year implementation.

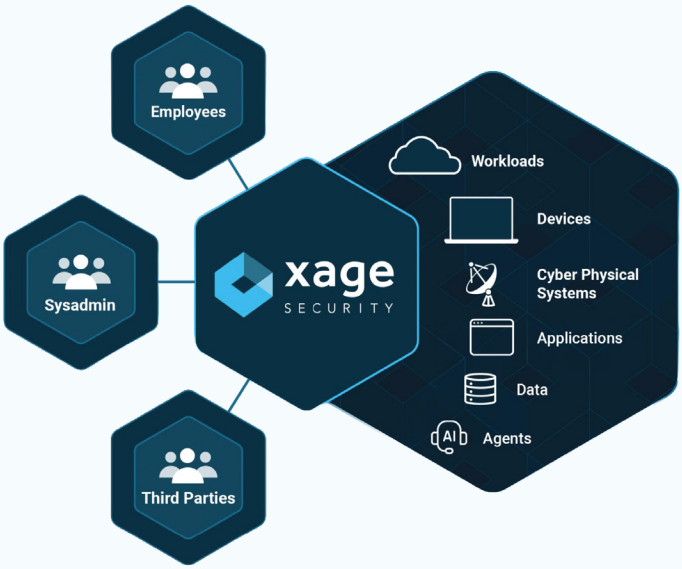
Extends Coverage Everywhere

Apply consistent controls across on-premises IT, cloud, OT, edge, remote sites, and disconnected environments.

Enforces Protection From Day One

Reduce exposure immediately while discovery, credential workflows, and policies continue to mature.

xage SECURITY



Comprehensive Protection

Identity-first controls for human and non-human identities across critical resources. Govern access to applications, devices, workloads, cloud resources, OT assets, and mission-critical systems.

Agentless Overlay Architecture

Deploy faster with an agentless overlay that adds privileged access controls without network redesign, rip-and-replace, or endpoint-agent sprawl.

Resilient by Design

Distributed vaulting and local enforcement remove dependence on a centralized control point.

Core XPAM Capabilities

Feature	Description	Benefit	Business Outcome
Just-in-Time Access	Enforces least privilege and JIT access for users, machines, and AI.	**Reduces Standing Privileges**	Limits attack surface, stops credential abuse and lateral movement.
Distributed Vaulting	Distributes credentials and policy enforcement across the Xage Fabric.	**High Availability**	No single point of failure; operations continue during disconnected states.
Agentless Overlay	Enforces access without network redesign, endpoint agents, or VPNs.	**Accelerated Value**	Lowers total cost of ownership and speeds up deployment significantly.
Session Isolation & Control	Secures access via HTTP, HTTPS, SSH, RDP with layered MFA and recording.	**Enhanced Oversight**	Provides audit-ready evidence and allows safe credential rotation in legacy environments.
Extended Coverage	Governs access for third-parties, IT, OT, cloud resources, and AI identities.	**Universal Protection**	Consistent privileged access controls across all hybrid and edge environments.
Day-One Protection	Enforces privileged access immediately while discovery, credential workflows, and policies mature.	**Immediate Security**	Stops waiting for every account to be discovered and perfected before enforcing security.
Secure Zones	Applies layered validation and session termination between security layers.	**Asset Isolation**	Isolates and protects data centers, vaults, databases, OT assets, and high-value systems.
Centralized Visibility & Auditing	Consolidates audit logs, evidence, analytics, and policy management into a single view.	**Simplified Compliance**	Streamlines compliance reporting and enables continuous monitoring of access risks.
Account Discovery	Identifies privileged-access control gaps and unmanaged identities.	**Blind Spot Reduction**	Brings shadow IT and unmanaged accounts under strict centralized governance.

Learn more at www.xage.com/xpam

xage SECURITY