xage SECURITY

Xage Extended Privileged Access Management

A high-value PAM that quickly achieves complete deployment and protection, is simple to use, and extends coverage across the whole enterprise and every asset, including semi-privileged assets, multi-cloud and hybrid environments, and even the operational edge.

Legacy PAM solutions are not providing enough value for the cost, eating up budgets while not giving the full protection necessary for enterprises to stop increasingly sophisticated attackers who are exploiting the complexity of modern environments.

Innovative, Cost-Effective PAM for Simplified Security

Better Total Cost of Ownership

More protection without eating your whole budget.

Eliminate Complexity

Easy to deploy, manage, and use.

Innovative Technology

Its resilient architecture sets Xage apart.

xage SECURITY

What is Extended Privileged Access Management?

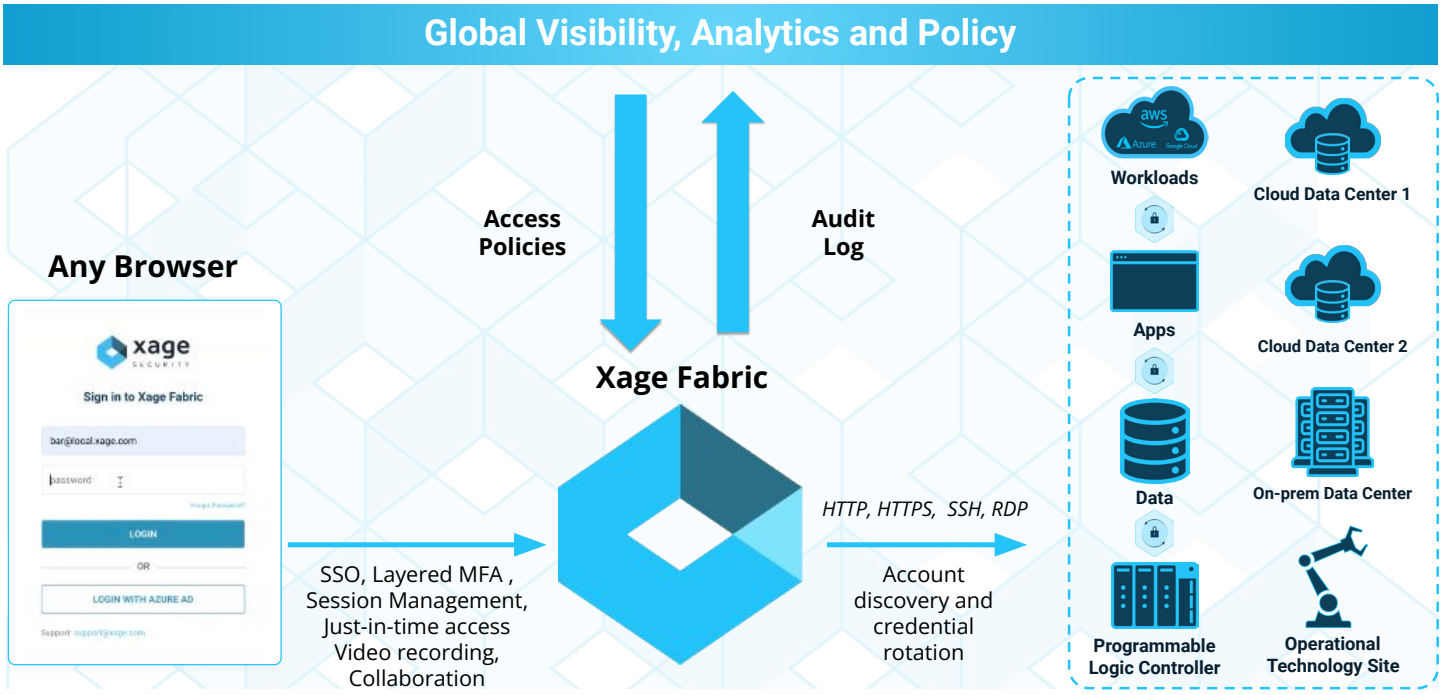
Xage is extending PAM to cover three critical areas where it currently falls short.

We're expanding what counts as privileged. PAM was created because there were certain accounts that, if compromised, gave attackers the keys to the kingdom. But we're increasingly seeing sophisticated attackers exploiting "non-privileged" user accounts in creative ways. These accounts need protection just as much as privileged accounts.

We're expanding to protect more than just accounts. Why do we have separate tools to protect assets (like apps, machines, and devices) vs. accounts? There are many assets within your infrastructure that are capable of interacting with the network, meaning they can be exploited by hackers. They aren't protected by legacy PAM, even though they can represent the same risk as privileged accounts.

We're expanding and simplifying coverage. Xage works across IT, operational technology (OT), and cloud and it's the same solution whether in the cloud or onsite.

XPAM Architecture



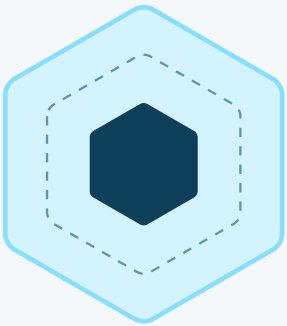
Simple to deploy and scales horizontally

PAM That Won't Eat Your Whole Budget

Xage's unique architecture provides better security that gives protection starting on day one and protects more: privileged accounts, regular users (and other identities), and everything in between. It also protects assets, devices, and environments like OT that aren't covered by legacy PAM.

Xage XPAM gives better protection without eating your entire security budget and comes with a highly responsive customer support team.

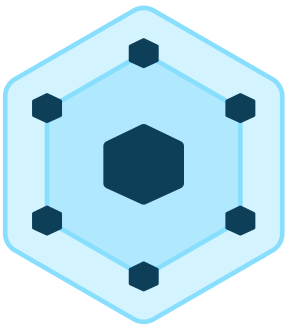
A PAM Approach That Flips the Script



Most PAM requires complex setup (identifying privileged accounts and defining policies) before protection starts. The Xage Fabric immediately acts as a layer between users and what they're accessing.

Its simplicity means it has a lower total cost of ownership and you don't have to wait on the endless cycles of account discovery and management to see real protection. Xage XPAM has clear pricing you can understand and a single solution that works across on-premises and cloud—giving comprehensive PAM, MFA, SSO, and session management.

Innovative Architecture Improves Security and Is Easier to Use



Xage has a unique and modern resilient architecture that enables it to provide security that's both easier to use and harder for adversaries to compromise.

Control of credentials and policy enforcement in Xage is decentralized, with a quantum-proof credential vault. Its more modern and resilient architecture means better protection of all credentials. Legacy PAM has a centralized vault which, if compromised, is game over.

xage SECURITY

Key Differentiators

Xage provides the fastest time-to-value. Xage allows customers to realize the full value of PAM rapidly across their entire enterprise and get more value for their money. Unlike legacy PAM, Xage's simplicity will ease management burden and delight users—meaning better security.

Protection on day one. Xage immediately creates a layer between users and assets, managing access. You don't have to wait to discover every privileged account and define every policy before your environment is protected.

No single point of security failure. Control of credentials and policy enforcement in Xage is decentralized and extremely secure. Nodes check in with each other and use consensus to validate the authenticity of the request. Xage XPAM will continue to enforce policies even if connectivity is lost to the cloud or central site.

Better for multiple, self-managed sites. Deploying Xage across multiple sites, whether on-premises, public & hybrid cloud, and even OT sites is fast and easy since each node automatically inherits policy, user, and credential data from other nodes.

Secure zones. Xage allows you to create deeper layers of higher security. It provides session termination between layers with additional validation using a multi-layer MFA process. So you can protect and isolate secure datacenters or sensitive resources like vaults, databases, or OT assets from less-secure or internet-connected infrastructure.

About Xage Security

Xage Security is a global leader in zero trust access and protection on a mission to pioneer a secure tomorrow. Control access and prevent attacks in the cloud, in the data center, at the remote operational edge anywhere on Earth, and even in orbit with the Xage Fabric Platform. Xage is easy to manage and can be deployed in a day, giving users easy and secure access to the assets they need from anywhere, while preventing advanced adversaries and insider threats at every stage of the attack chain. Learn why organizations like the U.S. Space Force, PETRONAS, and Kinder Morgan choose Xage at xage.com.

xage SECURITY