Xage XPAM vs. Traditional PAM

Extended Privileged Access Management (XPAM)

Controlling access to critical assets and preventing the abuse of privileged accounts is more urgent, and also more complex than ever. Enterprises face major challenges in bringing necessary privileged access management and asset protection capabilities to every part of the increasingly sprawling and complex environment.

Xage delivers extended privileged access management (XPAM) with no agents and no cloud dependencies—using a distributed architecture that's more secure, easier to deploy, and covers infrastructure that other tools can't. While traditional PAM solutions can take months to deploy, Xage can be deployed in as little as one day, delivering fast time-to-protection and time-to-value.

Xage XPAM Delivers Enterprise-Wide Access Control and Security for the Modern Enterprise

Xage XPAM

Xage XPAM is built on a resilient, distributed cybersecurity mesh. This unique architecture delivers many benefits.

- Easy to deploy and gives protection on day one
- User-friendly so admins won't pursue insecure workarounds
- Protects more: assets, privileged accounts, regular users, applications, and machine identities

Xage enables granular and automated control of privileged access across your diverse infrastructure. Its unique mesh architecture makes for a vault that's both more secure and works easily across varied, distributed deployments—even self-hosted ones.

Traditional PAM

Traditional PAM depends on a bulky mix of product modules, clients, and jump servers. Choosing traditional PAM has some drawbacks.

- Complex and expensive to manage
- Endless deployment journey that never reaches full protection
- Only protects privileged accounts that it's able to discover

In traditional PAM deployments, a centralized vault holds passwords and is key to authenticating users. This centralization struggles with multiple, distributed self-hosted deployments and makes for a single point of security failure that increases risk.

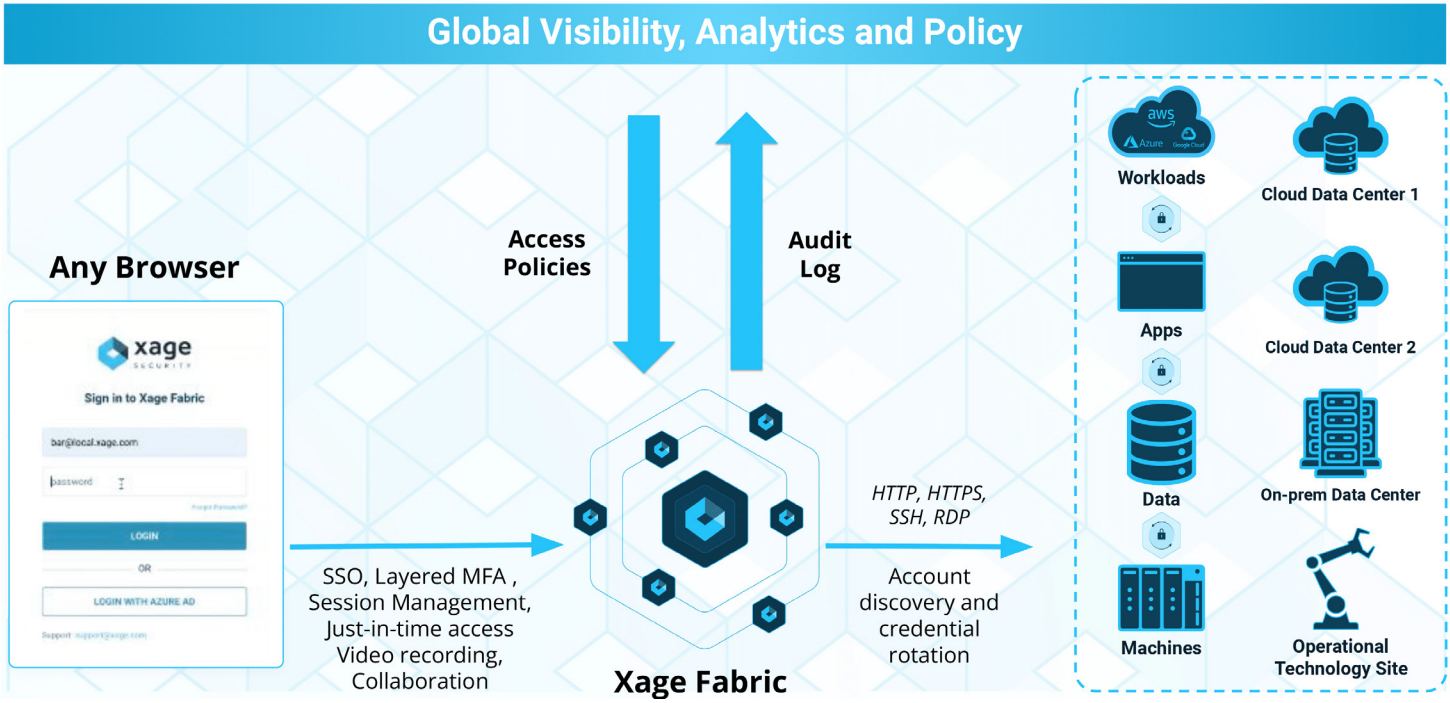
Capability Comparison

	Xage	Traditional PAM
Easy Deployment for Multiple Sites	Deploying Xage across multiple sites is fast and easy since each node automatically inherits policy, user, and credential data from other nodes—even in self-hosted deployments.	Traditional PAM struggles with multiple, self-managed deployments, often resulting in manual setup for every site that won't stay in sync across sites.
Single Sign-On	Xage provides single sign-on access to and protection all the way to individual systems and assets with fully managed device/endpoint identity. Xage users only need to know their Xage access credentials and can securely access individual devices they are allowed to per policy.	Traditional PAM's SSO doesn't extend to the kinds of legacy assets and applications common in operational environments. Users are left using manual logins for OT assets or using clunky integrations to connect, whether remotely or on site.
Multifactor Authentication	Xage, with multiple site specific IdPs, provides layered multifactor authentication across the entire enterprise, from IT to OT to DMZ to the cloud.	Traditional PAM enables MFA at a single layer, when the user first authenticates into their system, which leads to siloed site-specific deployments to meet site-specific IdP requirements leading to very high operational costs.
Machine-to-Machine (East-West) Lateral Movement Control	Xage enables policy-based access control of machine-to-machine communication east-to-west within a network. This prevents malicious target discovery and lateral movement, and the spread of malware.	Traditional PAM can authenticate M2M connections but can't set policies to control machine-to-machine communication or prevent lateral movement within the network.
Full Support for On-Premises Deployment	Xage supports a distributed on-premises deployment that is extremely secure and works even with limited or intermittent connectivity.	Traditional PAM prioritizes cloud deployments, with on-premises options becoming an afterthought. Cloud-hosted PAM has big drawbacks for operational environments which may have limited or intermittent connectivity.

Enterprise-wide Access Control and Security

	Xage	Traditional PAM
Rapid Deployment	Xage can be deployed in a day and begins providing access and protection immediately. Since Xage requires no installation of agents, no firewall rule updates, and no network changes, the deployment is seamless and nondisruptive.	Deploying traditional PAM can require the installation of new software at various points in the environments to be accessed, introducing friction and delays. Deploying traditional PAM may also require updates to firewall rules and allow lists to enable users to access the assets they need to do their jobs.
DDIL Environments	Xage uses a distributed architecture with nodes that can function independently, preventing downtime even in disrupted, disconnected, intermittent and low-bandwidth (DDIL) environments.	Even when self-hosted, traditional PAM centralizes their credential vault, meaning it struggles with DDIL environments when there's more than a single site or location involved.

Xage Delivers Unified Zero Trust Access Across IT, OT, and Cloud



Xage Customer Reviews

While traditional PAM solutions can take months to deploy, Xage can be deployed in as little as one day, delivering fast time-to-protection and time-to-value. Xage has rave reviews from our customers on Gartner Peer Insights across three product categories, all delivered in a single simple solution that can be deployed in a day.

The product more than exceeded our expectations when it came to our privileged access management.

Manager, IT Security and Risk Management – Energy and Utilities (1B - 3B USD)

Gartner Peer Insights™

About Xage Security

Xage 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.