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.

Xage XPAM vs. Traditional PAM

Condensed capability comparison and enterprise-wide access architecture

	Xage	Traditional PAM
Easy Deployment for Multiple Sites	Nodes inherit policy, user and credential data across sites - including self-hosted deployments.	Manual per-site setup; deployments often do not stay synchronized.
Single Sign-On	SSO reaches individual systems and assets with managed device/endpoint identity.	SSO often stops short of legacy OT assets, leaving manual logins and clunky integrations.
Multifactor Authentication	Layered MFA across IT, OT, DMZ and cloud with site-specific IdP support.	MFA is typically applied at first login only; site-specific IdP needs add complexity and cost.
East-West Lateral Movement Control	Policy-based M2M controls reduce target discovery, lateral movement and malware spread.	Can authenticate M2M connections but cannot enforce granular machine-to-machine paths.
Full Support for On-Premises Deployment	Distributed on-prem deployment works securely with limited or intermittent connectivity.	Cloud-first designs make on-premises support an afterthought for operational environments.
Rapid Deployment	Deploy in as little as one day with no agents, firewall rule updates or network changes.	Often requires software installation, firewall changes and allow-list updates, causing delays.
DDIL Environments	Distributed nodes function independently in disrupted, disconnected, intermittent and low-bandwidth environments.	Centralized vault designs struggle across multiple distributed or disconnected sites.

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