xage SECURITY

DATASHEET

# Xage Extended Privileged Access Management

Agentless, resilient Zero Trust privileged access for IT, data centers, critical infrastructure, and other high-stakes environments

Traditional PAM is too complex, too slow to deploy, and too dependent on centralized infrastructure. Across data centers, remote sites, branch offices, legacy environments, contractor workflows, OT, and disconnected operations, these limitations can leave critical access paths unprotected. Standing privileges, VPNs, jump servers, endpoint agents, and discovery-first deployment models add risk and complexity while delaying protection.

Xage Extended Privileged Access Management (XPAM) delivers modern, identity-first Zero Trust protection across users, vendors, machines, applications, AI agents, and critical assets. Its agentless overlay enables organizations to deploy quickly without network redesign or rip-and-replace, while distributed credential vaulting and local policy enforcement eliminate centralized points of failure and maintain protection across IT, cloud, data center, OT, edge, remote, and disconnected environments.

## STRENGTHEN SECURITY

### XAGE'S CORE INNOVATION

**Protection Alongside Discovery—Day 1, Not Day 180:** Traditional PAM and SRA tools protect only the accounts and applications they have been told about. Xage inverts the model: the Fabric inserts an identity-based enforcement layer between every user and every asset from the moment it is deployed. Policies are defined between ALL identities and ALL assets first; account discovery and onboarding follow. Even privileged accounts that are never discovered remain protected — stopping lateral movement, ransomware, and living-off-the-land attacks immediately.

**Quantum-proof Vault With No Single Point of Failure:** Other solutions keep all secrets in one on-prem vault — a single high-value target whose compromise means total privileged access compromise. Xage stores credentials, keys, policies, and session recordings across a distributed, quantum-proof vault using cryptographic secret-sharing and consensus validation across Fabric nodes. No single node holds enough information to be useful to an attacker, and the vault stays available even when a site or the cloud is offline.

**Continuous Oversight of Every Privileged Session**: Beyond initial authentication, Xage enforces MFA at every layer and device, just-in-time access with zero standing privileges, supervised and collaborative sessions, full session recording with smart transcripts, real-time termination, and a tamper-proof, distributed audit ledger for compliance and incident response.

## IMPROVE OPERATIONAL AGILITY

**Data Stays Inside Your Trusted Boundary—With No Cloud Dependency:** Xage XPAM deploys fully on-premises, fully in the cloud, or hybrid. Unlike remote access architectures that route connections through vendor-operated cloud points of presence, the Xage Fabric requires no external cloud component at all. Nodes validate requests by consensus locally, so policy enforcement, credential protection, and session brokering continue uninterrupted in disconnected, intermittent, and low-bandwidth (DDIL) environments — air-gapped plants, offshore platforms, vessels, and remote field sites.

**Deploy in Hours, Protect on Day One:** XPAM deploys as a non-disruptive overlay — no agents on endpoints or targets, no rip-and-replace, and no inbound firewall ports opened toward OT assets. Multi-hop access traverses DMZs and Purdue levels through bottom-up encrypted, signed tunnels, eliminating jump servers and the Windows licensing they carry. Typical deployments are operational in as little as one day, and the horizontally scalable mesh extends across hundreds of sites with policies auto-inherited by new nodes.

**One Platform, One Policy, One License Model:** A single Xage Fabric covers remote privileged access, vaulting, rotation, discovery, session management, MFA/SSO, and file security across IT, OT, and cloud — with simple user-based licensing instead of per-module or per-node pricing.

## ENHANCE USER EXPERIENCE

Agentless, Browser-Based Access: Employees and third-party vendors connect through any browser to RDP, SSH, VNC, HTTP/S, and native applications — no agents, no VPN clients, no software installs. Credential injection means users never see or handle privileged passwords.

Built-In Session Collaboration: Multi-monitor RDP, supervised sessions, real-time session sharing for remote collaboration between operators and vendors, secure managed file transfer with antivirus scanning, and self-service access requests with multi-step approvals.

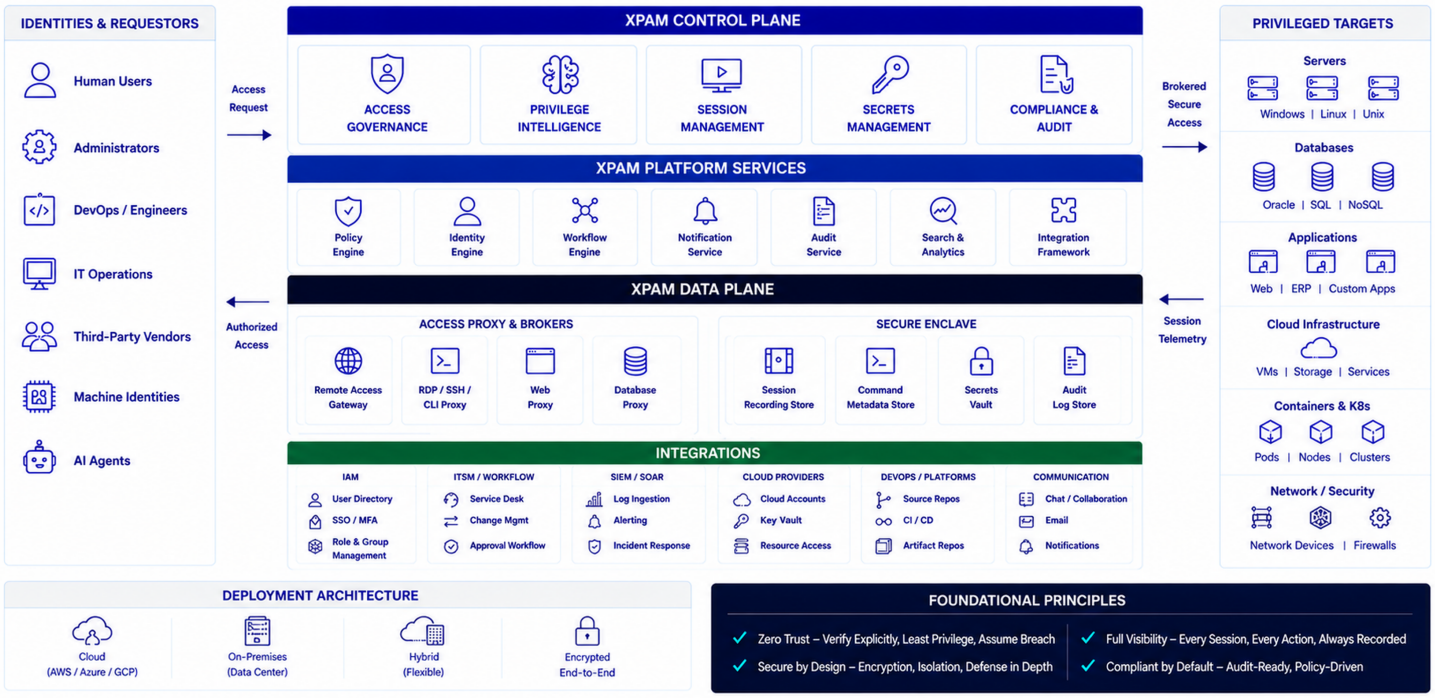
## XAGE XPAM ARCHITECTURE

Xage XPAM delivers a distributed, identity-first Zero Trust architecture for governing privileged access across human users, third parties, machine identities, and AI agents. A unified control plane brings together access governance, privilege intelligence, session management, secrets management, compliance, policy, workflows, analytics, and integrations, while the distributed data plane brokers authorized RDP, SSH, command-line, web, and database access through secure proxies and gateways. Credentials, session recordings, command metadata, and audit logs remain protected within secure enclaves, eliminating the need to expose target systems directly or rely on endpoint agents, VPNs, or extensive network redesign.

Distributed vaulting and local policy enforcement extend consistent controls across servers, databases, applications, cloud infrastructure, containers, network devices, and operational environments. Because enforcement does not depend on a single centralized control point, privileged operations can continue securely through network disconnect or central-site outages.

Combined with MFA, just-in-time access, session isolation and recording, account discovery, centralized visibility, and audit-ready evidence, XPAM provides resilient privileged access protection across IT, data center, critical infrastructure, and high-stakes environments.

# XAGE XPAM Platform Architecture




All Xage capabilities run on the Xage Fabric Platform: a highly available, cyber-resilient distributed cybersecurity mesh providing central management with distributed enforcement. Access policies, credentials, and audit data are protected across the mesh using distributed-ledger technology, Shamir's Secret Sharing, and Federated Byzantine Agreement — creating a tamperproof system that resists vault compromise and session hijacking by design.

| Feature | Technical Description |
|---|---|
| **Xage Manager (XM)** | Single pane of glass where administrators define security policy and deploy, upgrade, configure, and monitor the entire Fabric. |
| **Xage Broker (XB)** | Connects enterprise identity services (Active Directory, LDAP, SAML/OIDC IdPs) to the Fabric, synchronizing accounts, credentials, and policies to distributed nodes. |
| **Core Nodes** | Distributed, redundant storage layer for the quantum-proof vault — secrets are sharded across nodes; no single node is a useful target. |
| **Edge Nodes** | Authenticate, authorize, and enforce at every site and Purdue level — including ICS Layer 2/3 — forming secure multi-hop tunnels with no inbound firewall rules and continuing enforcement even when disconnected from the central site or cloud. |
| **Xage Enforcement Point (XEP)** | Extends MFA and identity-based access control to legacy single-factor and zero-factor devices — PLCs, RTUs, HMIs — without modifying the asset. |

**Distributed security, decentralized enforcement** — central policy with local control, all while keeping data, secrets, and keys inside the organization's trusted boundary with no dependency on a vendor cloud.

## XAGE XPAM: FEATURES & CAPABILITIES

Xage XPAM secures the entire privileged access lifecycle — identity, device, session, account, application, and administration — in one platform.

| Feature | Technical Description |
|---|---|
| **Multi-factor authentication (MFA)** | Layered MFA and passwordless FIDO2 authentication, with login and per-device enforcement on supported deployments. Supported options include FIDO2 security keys, RSA SecurID, and authenticator-app methods. |
| **Single sign-on (SSO)** | SSO across modern, legacy, and cloud applications. SAML SSO for Xage Fabric UI, Xage Manager, and supported applications and CAC/PIV smart-card passthrough for access to RDP targets. |
| **IdP integrations** | Integrates with enterprise directories and identity providers, including Active Directory, LDAP/LDAPS, Entra, Ping, Okta, and SAML 2.0. Orchestrates across multiple AD instances and IdPs simultaneously. |
| **Identity for every entity** | Applies identity to human users, service accounts, and AI agents—controlling machine-to-machine and app-to-machine interactions, not just user logins. |
| **Just-in-time / Zero standing privileges** | Time-bound, on-demand access with multi-step approval workflows; net-new permissions created at session launch and automatically revoked— achieving zero standing privileges across Windows, Linux, and cloud consoles. |
| **Lifecycle management** | Provisioning, deprovisioning, and full life cycle management of privileged accounts for humans and machines. |
| **Dynamic identity-to-account matching** | Exact-, prefix-, and suffix-based rules dynamically associate authenticated identities with the appropriate PAM accounts, reducing manual one-to-one account mappings while preserving credential injection and policy control. |

## ACCOUNTS AND VAULT MANAGEMENT

| Feature | Technical Description |
|---|---|
| **Automated asset-to-account onboarding** | Discover Windows devices from Active Directory, automatically create RDP access methods, discover their privileged accounts, classify them, apply account security policies, and automatically assign discovered accounts to the appropriate vault. |
| **Automated account discovery** | Continuously discover and onboard privileged accounts across Windows, Linux, databases, network and OT systems. |
| **Distributed, quantum-proof vault** | Secrets sharded across Fabric nodes using cryptographic secret sharing. No centralized vault to breach and no single point of failure. Vault remains available even when a site or the cloud is offline. |
| **Delegated vaults + dual control** | Vault Viewer, Contributor, and Manager roles separate account use from account administration. Individual users or user groups can be assigned to vaults, while one- or two-level approval workflows enforce time-bound access with justification and designated approvers |
| **Password rotation & reconciliation** | Policy-driven rotation at the app, account, user, or group level, with automated verification and reconciliation of out-of-sync credentials. |

| Feature | Technical Description |
|---|---|
| **Check-out / check-in** | Seamless privileged account check-out and check-in with exclusive-use controls and full audit. |
| **Credential injection** | Inject vaulted credentials directly into RDP, SSH, web, and native sessions. Users never see or handle privileged passwords. |
| **Out-of-the-box plugins** | AWS, Entra, Windows Local & Domain, Linux, Active Directory, ESXi, Dell iDRAC, PAN firewalls, Windows SQL, Azure SQL, MySQL, PostgreSQL, Nozomi, config files (XML/INI), and more. |
| **Extensible plugin framework** | Build custom discovery, rotation, and checkout plugins for any system, including proprietary legacy devices. |
| **Machine-to-machine credential brokering** | Non-interactive service accounts authenticate to Edge-node PAM APIs using API tokens or mTLS certificates. Policies map service accounts and automation tools to authorized privileged-account groups so pipelines and applications can retrieve vaulted passwords at runtime without embedding credentials in code. |

## SESSION MANAGEMENT & OVERSIGHT

| Feature | Technical Description |
|---|---|
| **Session recording & smart transcripts** | Policy-based video recording of RDP/SSH/web sessions with searchable smart transcripts—find any command executed in any recorded session in seconds. Recordings stored tamper-proof in the distributed Fabric. |
| **Supervised & collaborative access** | Supervisors can monitor, join, and collaborate in active sessions in real time, restrict permitted actions, and terminate any session instantly. |
| **Behavioral analytics (Xage Insights)** | Interactive dashboards for login trends, geolocation of access attempts, most-accessed assets, file transfer activity, MFA coverage, and anomaly detections across the Fabric. |
| **Tamper-proof audit trail and records** | Every user-to-machine and machine-to-machine interaction is logged and stored in the distributed and cryptographically protected fabric, and easily forwarded to any SIEM/SOAR via syslog for monitoring and analysis. |

## SECURE REMOTE ACCESS & FILE SECURITY

| Feature | Technical Description |
|---|---|
| **Agentless, VPN-less access** | Browser-based access to RDP, SSH, VNC, HTTP/S, and native apps with no agents on user or target devices and no VPN. |
| **Secure multi-hop access** | Encrypted, signed tunnels at every hop traverse DMZs and Purdue levels with no inbound firewall ports and no jump servers—defeating IP spoofing and man-in-the-middle attacks. |
| **Third-party / vendor access** | Zero trust onboarding for contractors and OEMs with granular, time-bound, least-privilege access—no standing credentials, no network exposure. |

| Feature | Technical Description |
|---|---|
| **Managed file transfer with malware scanning** | Secure file transfer between users and assets with automatic antivirus scanning (ICAP integration); infected files are deleted and logged — stopping malware and ransomware from spreading into OT. |
| **Multi-monitor & native app support** | Multi-monitor RDP, native RDP/SSH clients, and DevOps CLI access alongside web-based sessions. |
| **Controlled access to web applications** | Captive web proxy supports applications that cannot operate through the standard web proxy, with host allowlisting, HTTP blocking, upload/download controls, credential injection, and event-based session recording. |

## ACCESS POLICY & ENFORCEMENT

| Feature | Technical Description |
|---|---|
| **Granular zero trust policy** | Define and enforce policy at the user, group, asset, account, data, and protocol level—between all identities and all assets, including user-to-machine and machine-to-machine interactions. |
| **Contextual access controls** | Time windows, source IP, device posture, MFA step-up, device certificates, access request and approval workflows. |
| **Action controls in session** | Block or allow clipboard, file upload/download, drive and printer redirection; enforce recording; limit session duration; require supervisor presence. |
| **Asset protection without credentials** | Protect devices that have no account or credential mechanism at all—legacy PLCs, RTUs, sensors—via identity-based network-layer enforcement. No other PAM or SRA tool covers these assets. |

## ADMINISTRATIVE & COMPLIANCE

| Feature | Technical Description |
|---|---|
| **Central management, distributed enforcement** | One Xage Manager governs policy across all sites; Edge Nodes enforce locally and auto-inherit policy as the deployment scales. |
| **Role-based administration** | Granular admin roles (Super Admin, Site Admin, Approver Admin, and more) across the Manager and API. |
| **REST API & integrations** | Full API for automation; syslog log shipping to SIEM/SOAR; ITSM and identity ecosystem integrations. |
| **High availability & resilience** | No single point of failure anywhere in the architecture; continuous operation in disconnected (DDIL) conditions — air-gapped sites, vessels, and remote operations. |
| **Compliance reporting** | Generate on-demand or scheduled reports covering user-device entitlements, pending and approved access requests, scheduled password rotations, device access, and PAM-account use. Notify administrators by email and export reports as PDF or Excel. |

## EXTENDED PAM RESULTS

### Better Security

Day-1 protection for the entire enterprise • No single point of hack or failure • Stops lateral movement, ransomware, and living-off-the-land attacks • Quantum-proof credential protection

### Operational Safety

Granular control of every action on cyber-physical systems • Supervised sessions with real-time termination • Continuous enforcement during outages keeps operations safe

### Maximized Value

Operational in as little as one day • One platform replaces SRA + PAM + jump servers + VPNs • User-based licensing • Documented 400% ROI with 3-month payback at a major critical infrastructure operator

### Compliance, Simplified

IEC 62443-4-1/4-2 certified (SL3) • Supports NERC CIP, NIST CSF / SP 800-82, NIS2, CMMC, ISO 27001 • Tamper-proof audit ledger, JIT access, and recorded sessions out of the box

### Seamless User Experience

Agentless, browser-based access with a single login • Frictionless third-party and BYOD access • Session collaboration between operators and vendors

## ABOUT XAGE SECURITY

Xage Security is the identity protection platform for the modern enterprise, securing privileged access for cyber-physical systems across OT, IT, and cloud. Built on the distributed, quantum-proof Xage Fabric, Xage XPAM is trusted in the world's most demanding environments — including national defense, space operations, and major energy and utility operators — delivering complete privileged access management with day-one protection, no agents, and no single point of failure.

**Visit xage.com to learn more or request a demo.**

xage SECURITY