

Xage Extended Privileged Access Management (XPAM) vs. Delinea PAM

CRITERIA	XAGE XPAM	DELINEA
PRIVILEGED ACCESS SECURITY & MANAGEMENT		
Discovery & Time-to-Protection	Instant Agentless Policy Overlay: Governs access immediately upon network placement; no need to wait for full credential discovery/rotation.	Fast Discovery: Rapid directory sync and cloud asset ingestion; quick initial time-to-value for IT environments.
Credential Management & Vaulting	Decentralized / Secretless-First: Eliminates standing credentials; supports dynamic rotation, vaulted secrets, and credential injection without exposing plaintext to users.	SaaS/Hybrid Vault (Secret Server): Cloud-native or on-prem encrypted database; simple secrets management with auto-rotation.
Vault Security	Quantum-resistant cryptography; credentials and policy are fragmented and distributed across the Xage Fabric, so no single node holds a complete secret	AES-based encryption; no public documentation of post-quantum cryptography for secret storage
Resilience	No single point of failure across isolated nodes. 100% Resilient Local Enforcement Nodes sync cryptographically; full authentication and policy enforcement continue during WAN/cloud outages.	HA supported, but the public architecture centers on Secret Server + SQL Server + IIS
Zero Standing Privilege (ZSP) & JIT Access	Native JIT Protocol Proxy: Ephemeral access granted at the protocol/asset level; dynamic role-binding; zero persistent local admin rights.	JIT Infrastructure Access (StrongDM): Ephemeral credentials for databases, k8s, SSH, and cloud consoles via broker.
Third-Party & Remote Vendor Access	Direct Agentless Zero Trust Overlay: Browser-based or native client access to internal assets; no client VPN, no jump hosts, no network-level exposure.	Cloud Web Portal: Identity-aware proxy access for contractors to web, SSH, and RDP targets.
SESSION MANAGEMENT & SECURITY FEATURES		
Session recording	Built-in, agentless	Supported, including browser-based and proxied recordings
Zero Trust Remote Access	Native, included in the same platform	Delivered via Delinea Privileged Remote Access (PRA), a distinct product capability
Session collaboration	Multiple users can join the same session concurrently	Limited multi-user session collaboration
Secure file transfer with malware scanning	Built-in, with AV integration, fingerprinting, and integrity checks	Not natively supported
East-west (machine-to-machine) control	Policy-based control of lateral M2M traffic	Not a core PASM capability
DEPLOYMENT & INFRASTRUCTURE FOOTPRINT		
Architectural Model	Distributed Zero Trust Mesh • Tamper-proof, multi-node consensus • Zero single point of failure	SaaS-Hosted Proxy Broker • Cloud control plane with local brokers • Dependent on external cloud reachability
Deployment model	Software-based; Ubuntu/RedHat VM or virtual appliance	On-prem Secret Server requires Windows Server + IIS + SQL Server; Delinea Platform also offered as SaaS

CRITERIA	XAGE XPAM	DELINEA
DEPLOYMENT & INFRASTRUCTURE FOOTPRINT (CONTINUED)		
Core components	Minimum 2 (Manager + Nodes)	Web/app tier + SQL database minimum; multi-site designs commonly add Distributed Engines, RabbitMQ, and load balancers
Agent requirement	Agentless	Agentless for most remote-access flows; some session-recording and proxy scenarios use connector-style components
Air-gapped/offline support	Fully self-hostable, no cloud dependency, including ZTNA and remote access. 100% operational when WAN, cloud, or central services are disconnected.	On-premises deployment supported for Secret Server; the broader Delinea Platform spans SaaS-delivered services. Dependent on multi-region cloud uptime; loss of internet connectivity locks out local site administrators.
Centralized management	Single console for PAM, ZTNA, MFA, SSO, file transfer, and session collaboration	Multiple products, editions, and consoles across the portfolio (Secret Server, Privilege Manager, PRA, DevOps Secrets Vault)
IDENTITY & ACCESS CONTROL		
AD/LDAP integration	Supported, including multi-level LDAP/LDAPS	Supported
Identity-based micro-segmentation	Supported via Xage enforcement points	Not a core PASM capability
Universal MFA Support	Any System, Protocol, or Legacy Asset Injects Entra ID/Okta/YubiKey MFA in front of legacy Unix, switches, storage, and web tools natively.	SAML/OIDC for Cloud Apps Limited ability to inject MFA directly into legacy protocols and non-web infrastructure.
SCALABILITY & RESILIENCE		
Installation time	Containerized install; operational in hours	Marketed as easy to deploy; on-prem prerequisites (Windows/IIS/SQL) and larger multi-component designs add planning time
Scalability model	Distributed, node-based scaling	Scales via Distributed Engines and central services, following a more conventional client-server pattern
HA model	Built-in fault tolerance via distributed consensus	HA supported, typically via SQL Server clustering/replication alongside web-tier redundancy
Blast Radius Containment	Asset-Layer Isolation Compromise of one node or credential cannot compromise the rest of the estate.	Medium/High Proxy Risk SaaS account hijacking or proxy bypass leaves downstream assets exposed.
LICENSING & TOTAL COST OF OWNERSHIP		
Infrastructure Overhead (TCO)	Zero Appliance Sprawl Eliminates RDP jump boxes, dedicated bastions, hardware appliances, and VPN licensing.	Fragmented Stack Digestion Managing separate engines for Secret Server, StrongDM, Fastpath, and Authomize.
Day-One Protection & Time-to-Value	Immediate (Hours to Days) Agentless overlay wraps any asset with JIT access & MFA instantly, without prior vaulting.	Fast in IT; Nil in Edge/OT Quick directory sync for cloud IT, but leaves unproxied and legacy systems unprotected.
License model	User-based, unlimited assets, single tier	Tiered by edition, with user and feature packs; multiple editions/add-ons modules.
Cost	Lower infrastructure overhead due to a 2-component architecture	Gartner's Oct 2025 PAM Magic Quadrant notes Delinea's PEDM pricing is among the highest evaluated and large-enterprise pricing runs above the market average; some requirements still need PowerShell customization
USER EXPERIENCE		
Admin experience	Single console, unified workflows	Gartner notes customers commend usability; broader in scope than Xage across products and consoles
Learning curve	Low – fewer moving parts, one policy model	Moderate to high given the number of products, tiers, and infrastructure choices