xage SECURITY

Xage Security XPAM vs. Idira (formerly CyberArk)

CRITERIA	XAGE XPAM	IDIRA
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.	Heavy Discovery & Ingestion: Multi-month discovery scans, account dependency mapping, and complex onboarding backlogs.
Credential Management & Vaulting	Decentralized / Secretless-First: Eliminates standing credentials; supports dynamic rotation, vaulted secrets, and credential injection without exposing plaintext to users.	Monolithic Vault (EPV/Privilege Cloud): Central database stores and rotates static credentials. High blast radius if compromised.
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 encryption with standard PKI; not built on post-quantum cryptography
Resilience	No single point of failure; one node compromised does not expose credentials or policy. 100% Resilient Local Enforcement Nodes sync cryptographically; full authentication and policy enforcement continue during WAN/cloud outages.	Vault security/availability is central to the system. Fragile Failover Requires complex clustered vaults, database replication, and active WAN links. Outages cause lockouts.
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.	Dynamic JIT via Alero / Secure Web Sessions: Session brokering with short-lived access, but often relies on underlying vaulted local accounts.
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.	Remote Access (formerly Alero): Biometric/mobile-authenticated remote access brokered through Idira Cloud and PSM.
SESSION MANAGEMENT & SECURITY FEATURES		
Command/process capture	Agentless SSH command capture and RDP process capture	Delivered through the PSM jump-server component
Session recording	Built-in, agentless	Built-in, agentless
Zero Trust Remote Access	Native, included in the same platform	Available via a separate SaaS module (e.g., Secure Cloud Access)
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

xage SECURITY

CRITERIA	XAGE XPAM	IDIRA
DEPLOYMENT & INFRASTRUCTURE FOOTPRINT		
Architectural Model	Distributed Zero Trust Mesh • Tamper-proof, multi-node consensus • Zero single point of failure	Monolithic Central Vault • Database-centric (EPV / Privilege Cloud) • Single point of compromise
Deployment model	Software-based; Ubuntu/RedHat VM or virtual appliance	Software-based; PAM Self-Hosted requires Windows servers, Privilege Cloud offered as SaaS
Core components	Minimum 2 (Manager + Nodes) for full capability	Full suite typically 7+ components (Vault, PVWA, CPM, PSM, and module-specific add-ons)
Agent requirement	Agentless	Agentless for core PASM; session proxying relies on the dedicated PSM jump-server component
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.	Fully self-hostable, no cloud dependency, including ZTNA and remote access
Network/firewall changes	Outbound-only, unidirectional tunnels between nodes; minimal rule changes	Session proxying through PSM typically requires broader network and firewall configuration
Centralized management	Single console for PAM, ZTNA, MFA, SSO, file transfer, and session collaboration	Separate consoles/components across vaulting, session management, and secrets modules
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	Universal MFA Injection: Integrates with Entra ID, Okta, Ping; injects MFA into legacy IT/OT systems, protocols, and devices that lack native MFA support.	Identity Security Platform: Native MFA/SSO (Idaptive) or integration with enterprise IdPs; step-up authentication at vault/PSM.
SCALABILITY & RESILIENCE		
Installation time	Containerized install; operational in hours	Multi-component install; Gartner's Oct 2025 PAM Magic Quadrant notes customer-reported complexity in initial setup and upgrades
HA model	Built-in fault tolerance via distributed consensus	HA supported via clustered vault and redundant components, adding architectural complexity
Patching/upgrades	Rolling updates across distributed nodes	Sequential upgrade path across Vault and dependent components
Blast Radius Containment	Asset-Layer Isolation Compromise of one node or credential cannot compromise the rest of the estate.	Severe Vault Risk Breaching the central vault or PSM tier compromises all vaulted enterprise secrets.
LICENSING & TOTAL COST OF OWNERSHIP		
Infrastructure Overhead (TCO)	Zero Appliance Sprawl Eliminates RDP jump boxes, dedicated bastions, hardware appliances, and VPN licensing.	Extremely Heavy Footprint Requires fleets of Windows servers for PSM, DR vault instances, CPM engines, and endless compute.
Day-One Protection & Time-to-Value	Immediate (Hours to Days) Agentless overlay wraps any asset with JIT access & MFA instantly, without prior vaulting.	Multi-Year Projects Requires account discovery, dependency mapping, custom CPM plugins, and heavy professional services.
License model	User-based, unlimited assets, single tier	Combination of user-based and per-module/component licensing
Cost	Lower infrastructure overhead due to a 2-component architecture	Gartner's Oct 2025 PAM Magic Quadrant identifies Idira's pricing as consistently on the high end of the PAM market, and notes it does not offer a discount for multi-year deals over a one-year term
USER EXPERIENCE		
Admin experience	Single console, unified workflows	Separate interfaces across vaulting, session management, and secrets modules
Learning curve	Low – fewer moving parts, one policy model	Higher – multiple modules, each with distinct configuration logic

xage SECURITY