xage SECURITY

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

CRITERIA	XAGE XPAM	BEYONDTRUST
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.	Automated Account Discovery: Discovers unmanaged local/domain accounts and service accounts across Windows/Active Directory.
Credential Management & Vaulting	Decentralized/Secretless-First: Eliminates standing credentials; supports dynamic rotation, vaulted secrets, and credential injection without exposing plaintext to users.	Centralized Vault (Password Safe): Rule-based auto-discovery and rotation stored in appliance/cloud vault database.
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
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.	Vault availability is central to the architecture; HA configurations reduce but don't eliminate this dependency
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.	Time-Bound Ephemeral Access (Entitle integration): On-demand approval workflows and access elevation; tied to Password Safe/PRA.
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.	Dedicated Appliance (PRA / Remote Support): Industry standard for vendor portals; requires maintaining internet-facing gateways.
SESSION MANAGEMENT & SECURITY FEATURES		
Command/process capture	Agentless SSH command capture and RDP process capture	Available; some capture scenarios rely on an installed agent
Session recording	Built-in, agentless	Built-in, agentless
Zero Trust Remote Access	Native, included in the same platform	Delivered via Privileged Remote Access / Remote Support, separate product lines within the Pathfinder platform
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 documented
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	Appliance / Gateway Clusters; Dedicated hardware/VM gateways; vulnerable network entry points
Deployment model	Software-based; Ubuntu/RedHat VM or virtual appliance	Available as software (Windows-based), virtual appliance, or physical appliance

xage SECURITY

CRITERIA	XAGE XPAM	BEYONDTRUST
DEPLOYMENT & INFRASTRUCTURE FOOTPRINT (CONTINUED)		
Core components	Minimum 2 (Manager + Nodes)	Full Total PASM suite (Password Safe + Privileged Remote Access + supporting services) typically involves 5 or more components
Agent requirement	Agentless	Agentless for core PASM; HTTP/HTTPS application access is typically proxied through a jump-server-style component
Air-gapped/offline support	Fully self-hostable, no cloud dependency, including ZTNA and remote access	On-prem/appliance deployment supported; SaaS-delivered elements and routine product updates typically depend on internet connectivity
Network/firewall changes	Outbound-only, unidirectional tunnels between nodes; minimal rule changes	Session proxying and jump-server components typically require broader network and firewall configuration
Centralized management	Single console for PAM, ZTNA, MFA, SSO, file transfer, and session collaboration	Separate consoles across Password Safe, Privileged Remote Access, and Endpoint Privilege Management
IDENTITY & ACCESS CONTROL		
AD/LDAP integration	Supported, including multi-level LDAP/LDAPS	Supported
Identity-based micro-segmentation	Supported via Xage Extended Protection (XEP)	Not a core PASM capability
Universal MFA Injection	Any System, Protocol, or Legacy Asset Injects Entra ID/Okta/YubiKey MFA in front of legacy Unix, switches, storage, and web tools natively.	Gateway Portal Dependent MFA required to enter PRA portal; internal direct connections lack MFA enforcement.
SCALABILITY & RESILIENCE		
Installation time	Containerized install; operational in hours	Multi-component install; Gartner notes customer feedback identifies initial setup and configuration as more complex and time-consuming than some competitors
HA model	Built-in fault tolerance via distributed consensus	HA supported via clustered/appliance configurations, 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 risk with public-facing PRA/Remote Support appliances that are proven targets for RCE zero-days.
LICENSING & TOTAL COST OF OWNERSHIP		
Infrastructure Overhead (TCO)	Eliminates RDP jump boxes, dedicated bastions, hardware appliances, and VPN licensing.	Fragmented with separate architectures and consoles for Password Safe, PRA, and EPM (disparate acquisitions).
Day-One Protection & Time-to-Value	Immediate (hours to days) agentless overlay wraps any asset with JIT access & MFA instantly, without prior vaulting.	Multi-Month Rollout Requires standing up appliance pairs, configuring gateways, and deploying desktop EPM agents.
License model	User-based, unlimited assets, single tier	Combination of user-based and per-component/module licensing across product lines
Cost	Lower infrastructure overhead because of 2-component architecture	Gartner's Oct 2025 PAM Magic Quadrant notes BeyondTrust's overall software pricing remains above the market average despite bundle discounts introduced with its Pathfinder Essentials/Plus/Flex tiers
USER EXPERIENCE		
Admin experience	Single console, unified workflows	Customer feedback identifies UI and navigation as an improvement area
Learning curve	Low – fewer moving parts, one policy model	Higher across multiple modules, each with distinct configuration logic