Marketing Resources

E-Book Privileged Access Monitoring

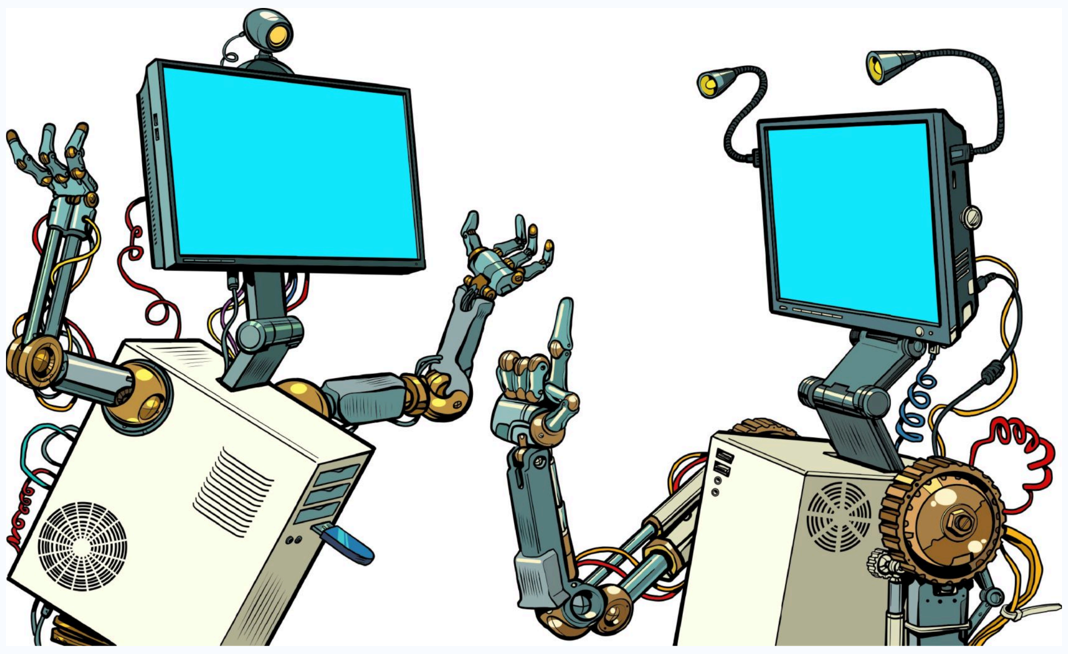
AuthNull

Introduction

Privileged access monitoring is a key part of privileged access management.

Privileged access monitoring refers to the processes and tools used to oversee, audit, and control access to high-privilege accounts and systems within an organization. These privileged accounts, often held by administrators, service accounts, or automated processes, grant elevated permissions that can access sensitive data, modify configurations, or control critical infrastructure. Monitoring such access is a core component of Privileged Access Management (PAM), which encompasses discovery, protection, and auditing of these privileges to prevent misuse, breaches, or insider threats.

In today's cybersecurity landscape, where cyber threats like ransomware and privilege escalation attacks are rampant, effective monitoring is crucial. It ensures compliance with regulations such as GDPR, HIPAA, and PCI DSS, while enabling a zero-trust model where no access is inherently trusted. According to Gartner, PAM is an essential cyber defense mechanism that goes beyond mere compliance to support defense-in-depth strategies. Organizations often face risks from human errors, unauthorized elevations, and privilege proliferation, particularly in cloud environments like IaaS.



Gartner emphasizes prioritizing PAM because minimal controls may suffice for audits but leave vulnerabilities to sophisticated attacks, such as service account exploitation or lateral movement by adversaries. Their Magic Quadrant for PAM evaluates vendors based on a uniform set of criteria, categorizing tools into four types: Privileged Account and Session Management (PASM), Privilege Elevation and Delegation Management (PEDM), secrets management, and cloud entitlement management. Leaders in the 2024 quadrant include BeyondTrust and CyberArk, recognized for comprehensive solutions that address these areas.This ebook explores Gartner's guidelines, best practices, top products, and real-world reviews to help you implement robust privileged access monitoring.

Gartner provides detailed guidance for security and risk management leaders to design and implement PAM capabilities that enable zero-trust access and mitigate privilege exploitation. Key recommendations include creating a PAM control coverage matrix aligned with your organization's cybersecurity framework to adopt a risk-based approach.

This involves mapping out privileged accounts across all assets, including human-to-machine and machine-to-machine interactions.

Core capabilities outlined by Gartner include governance, discovery of privileged accounts, protection through vaulting and rotation, monitoring and auditing of sessions, and just-in-time (JIT) privilege elevation to minimize standing privileges. For monitoring specifically, Gartner stresses auditing privileged operations for visibility and integrating with SIEM tools for real-time alerts on anomalous behavior. In zero-trust environments, PAM should drive a "zero standing privilege" model, where access is granted temporarily and revoked automatically.

To avoid common pitfalls, Gartner advises against deploying only minimal controls that focus on compliance checkboxes, as these fail against advanced threats like privilege escalation. Instead, extend PAM to cloud platforms, DevOps pipelines, and RPA scenarios, incorporating secrets management to handle API keys and credentials securely.

Best practices include regular access reviews, implementing multi-factor authentication (MFA) for privileged sessions, and using behavioral analytics to detect unusual patterns, such as impossible logins from disparate locations.Gartner also recommends architecting PAM solutions for resiliency with high-availability designs and disaster recovery processes, ensuring break-glass access for emergencies without compromising security. Integration with ITSM tools enhances workflow automation for access requests and approvals.

Key Capabilities and Best Practices for Monitoring

Effective privileged access monitoring requires a blend of tools and processes to ensure real-time oversight and rapid response. Key capabilities from Gartner's framework include PASM for session recording and playback, PEDM for elevating privileges on-demand, and secrets management for automating credential handling in CI/CD pipelines. Cloud Infrastructure Entitlement Management (CIEM) is vital for monitoring entitlements in multi-cloud setups, preventing over-privileging.Best practices emphasize the principle of least privilege: Grant access only when needed and for the shortest duration. Conduct quarterly audits of access points, segment privileges like vault rooms, and automate reviews to detect dormant accounts. Implement MFA everywhere, especially for vendors, and use Privileged Access Management tools for behavioral biometrics to flag unusual activities.

Organizations should focus on high-risk areas first, such as admin access and recent changes, with continuous monitoring to maintain integrity. For implementation, discover all privileged accounts, secure them with vaulting, audit usage, and automate rotations. In dynamic environments, integrate monitoring with vulnerability assessments and task automation to reduce manual errors.

Common recommendations include using AI-native, agentless monitoring for real-time insights, moving away from legacy systems that cause friction. Regular privileged account reviews and JIT access minimize risks, as highlighted in cybersecurity discussions.

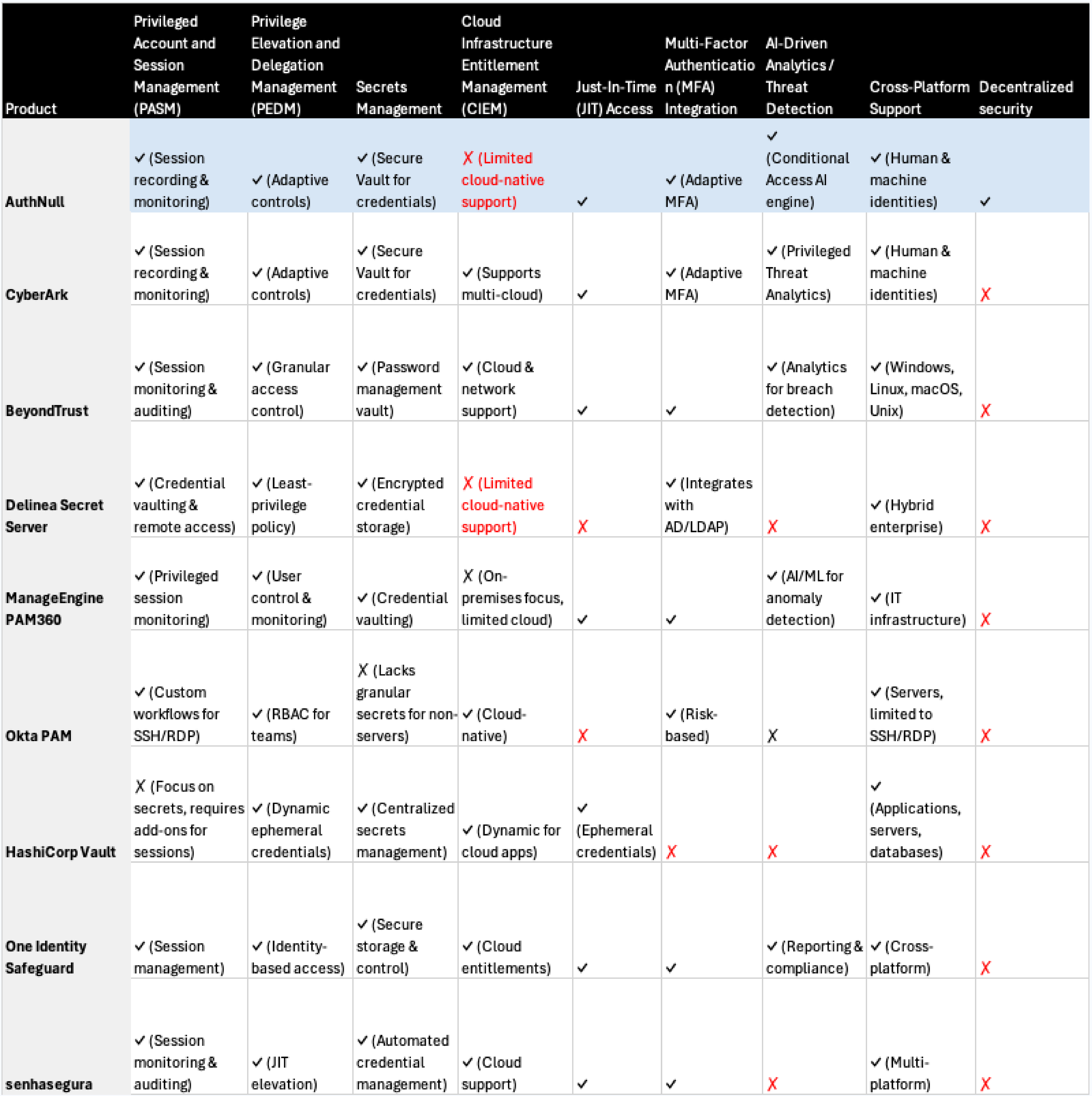
Products in the Market and How AuthNull compares?

Several products dominate the PAM landscape, offering robust monitoring features.

- Remote access to infrastructure without revealing passwords. **Passwords are decentralized** and are delivered without the need of a secret server
- **Conditional access** delivers time-bound just in time access in addition to dynamic access policies, risk based credentials and so forth.
- **Policy driven access control** enables administrators to create fine grained policies for access.
- **Session recording, access to local credentials, breakglass accounts** are all standard features built into AuthNull.
- **Integrated MFA delivers push notifications** on mobile for most common MFA to access infrastructure.

How do we compare?

AuthNull is well positioned to the bet of breed solutions out there with a big differentiator - decentralized security that is almost unhackable.



Product	Privileged Account and Session Management (PASM)	Privilege Elevation and Delegation Management (PEDM)	Secrets Management	Cloud Infrastructure Entitlement Management (CIEM)	Just-In-Time (JIT) Access	Multi-Factor Authentication (MFA) Integration	AI-Driven Analytics / Threat Detection	Cross-Platform Support	Decentralized security
AuthNull	✓ (Session recording & monitoring)	✓ (Adaptive controls)	✓ (Secure Vault for credentials)	✗ (Limited cloud-native support)	✓	✓ (Adaptive MFA)	✓ (Conditional Access AI engine)	✓ (Human & machine identities)	✓
CyberArk	✓ (Session recording & monitoring)	✓ (Adaptive controls)	✓ (Secure Vault for credentials)	✓ (Supports multi-cloud)	✓	✓ (Adaptive MFA)	✓ (Privileged Threat Analytics)	✓ (Human & machine identities)	✗
BeyondTrust	✓ (Session monitoring & auditing)	✓ (Granular access control)	✓ (Password management vault)	✓ (Cloud & network support)	✓	✓	✓ (Analytics for breach detection)	✓ (Windows, Linux, macOS, Unix)	✗
Delinea Secret Server	✓ (Credential vaulting & remote access)	✓ (Least-privilege policy)	✓ (Encrypted credential storage)	✗ (Limited cloud-native support)	✗	✓ (Integrates with AD/LDAP)	✗	✓ (Hybrid enterprise)	✗
ManageEngine PAM360	✓ (Privileged session monitoring)	✓ (User control & monitoring)	✓ (Credential vaulting)	✗ (On-premises focus, limited cloud)	✓	✓	✓ (AI/ML for anomaly detection)	✓ (IT infrastructure)	✗
Okta PAM	✓ (Custom workflows for SSH/RDP)	✓ (RBAC for teams)	✗ (Lacks granular secrets for non-servers)	✓ (Cloud-native)	✗	✓ (Risk-based)	✗	✓ (Servers, limited to SSH/RDP)	✗
HashiCorp Vault	✗ (Focus on secrets, requires add-ons for sessions)	✓ (Dynamic ephemeral credentials)	✓ (Centralized secrets management)	✓ (Dynamic for cloud apps)	✓ (Ephemeral credentials)	✗	✗	✓ (Applications, servers, databases)	✗
One Identity Safeguard	✓ (Session management)	✓ (Identity-based access)	✓ (Secure storage & control)	✓ (Cloud entitlements)	✓	✓	✓ (Reporting & compliance)	✓ (Cross-platform)	✗
senhasegura	✓ (Session monitoring & auditing)	✓ (JIT elevation)	✓ (Automated credential management)	✓ (Cloud support)	✓	✓	✗	✓ (Multi-platform)	✗

Get in touch

Get in touch with us if you require a POC at
https://authnull.co/contactus

sales@authnull.com