Marketing Resources

# E-Book Privileged Access Management

How AuthNull Delivers on Gartner's 2024 PAM Framework

AuthNull

# Introduction

Welcome to the Privileged Access Management E-Book by AuthNull.

This book exposes you to key concepts of Privileged Access and helps you map and implement PAM in your organization.

 Privileged Access Is the #1 Target in Cyberattacks — And Most Organizations Are Still Exposed.

**Context**

 In today's hybrid, cloud-first world, the attack surface is growing faster than ever. From ransomware groups to state-sponsored threat actors, the single most coveted prize remains the same: privileged access. Admin accounts, root access, service accounts, and machine credentials — if compromised, they grant near-total control of critical systems.

Welcome to the Privileged Access Management E-Book by AuthNull.

This book exposes you to key concepts of Privileged Access and helps you map and implement PAM in your organization.

 Privileged Access Is the #1 Target in Cyberattacks — And Most Organizations Are Still Exposed.

**Context**

 In today's hybrid, cloud-first world, the attack surface is growing faster than ever. From ransomware groups to state-sponsored threat actors, the single most coveted prize remains the same: privileged access. Admin accounts, root access, service accounts, and machine credentials — if compromised, they grant near-total control of critical systems.

AuthNull

# Introduction

## Introduction to Privileged Access Management (PAM)

Privileged Access Management (PAM) is a foundational cybersecurity discipline focused on controlling, monitoring, and securing accounts with elevated permissions that can access sensitive systems, data, and infrastructure. According to Gartner, PAM tools manage privileged access for both human users (e.g., administrators) and non-human entities (e.g., applications, scripts), categorizing them into four distinct tool types: Privileged Account and Session Management (PASM), Privilege Elevation and Delegation Management (PEDM), Secrets Management, and Cloud Infrastructure Entitlement Management (CIEM).

These categories address the growing complexity of hybrid environments, where privileged accounts are prime targets for cyberattacks, often involved in high-profile breaches.

Gartner emphasizes that effective PAM reduces risks by enforcing least-privilege principles, automating processes, and providing visibility into privileged activities. In the 2024 Critical Capabilities for PAM, Gartner highlights must-have features like account discovery and onboarding, remote privileged access management (RPAM), and secrets management as differentiators. With cyber insurance increasingly requiring PAM deployment, organizations must prioritize tools that support use cases such as DevOps, cloud entitlements, and endpoint protection.The evolution of PAM includes advanced authentication methods, just-in-time (JIT) access to minimize standing privileges, and integration with identity governance tools.

Traditional password-based systems are inadequate; modern PAM incorporates AI for anomaly detection and automation to operationalize tasks. This ebook examines how AuthNull embodies these Gartner-recommended features in an agentless, scalable platform.

AuthNull

# Why It Matters

74% of breaches involve misuse of privileged credentials (Verizon DBIR 2024)
PAM is a foundational pillar in any Zero Trust strategy
Regulatory frameworks like NIST 800-207, ISO 27001, and PCI DSS now require strong PAM controls

# Gartner’s Perspective (2024):

PAM is shifting from legacy vaulting toward dynamic, just-in-time, policy-driven access models integrated with identity fabric and security analytics.

# Gartner’s four pillars of PAM

**Track and Secure Every Privileged Account:** This pillar requires continuous discovery of privileged accounts across systems, as changes in IT environments can create unmonitored access points. Key points include ongoing scanning, governance to remove inappropriate access, and securing credentials to prevent exploitation. Gartner stresses that without full visibility, risks multiply, especially in cloud and hybrid setups.

**Govern and Control Access:** Effective life cycle management ensures accounts are provisioned, reviewed, and deprovisioned appropriately. Just-in-time access is recommended, granting privileges only when needed and revoking them afterward to eliminate standing access. This pillar aligns with zero-trust principles, using contextual factors like user behavior and device health for decisions.

**Record and Audit Privileged Activity:** Visibility into what privileged users do is crucial for compliance and threat detection. This involves session recording, logging changes, and tools to flag anomalies efficiently. Gartner notes that combining PAM with analytics tools enhances auditing, supporting regulations like GDPR and SOX.

AuthNull

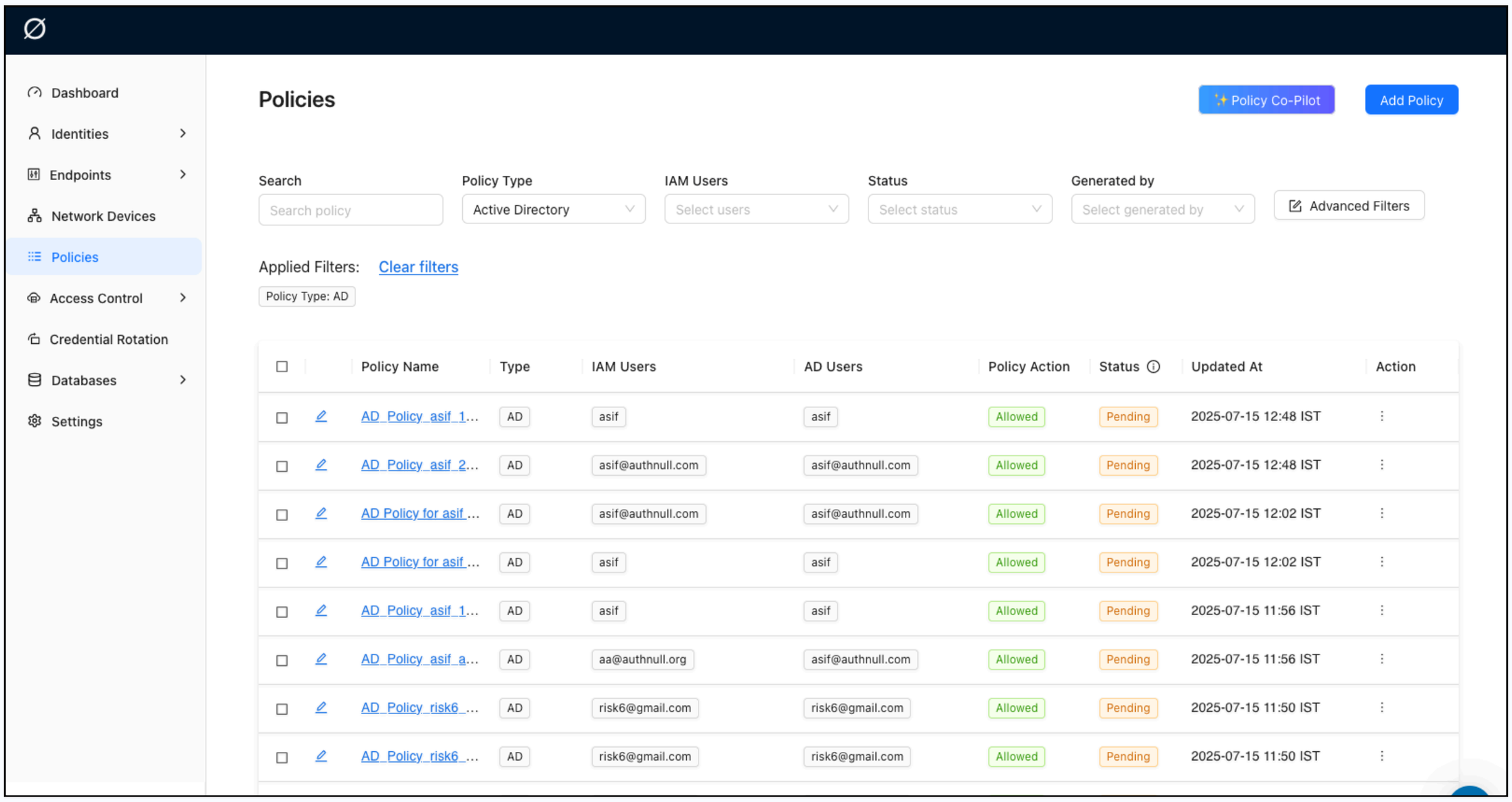
**Operationalize Privileged Tasks:** Automation of repeatable tasks, such as configuration changes or credential rotations, improves reliability and reduces human error. Integration with DevOps pipelines and RPA (Robotic Process Automation) is key, enabling seamless workflows in dynamic environments.

## AuthNull

AuthNull is an advanced  PAM platform designed to address Gartner's four pillars and critical capabilities in a unified, AI-powered solution. Supporting over 100,000 identities across Active Directory (AD), Windows, Linux, Radius devices, databases (e.g., PostgreSQL, MySQL), and cloud environments, AuthNull provides comprehensive coverage without requiring agents on endpoints, reducing deployment complexity and overhead.

Aligning with Gartner's PASM, PEDM, secrets management, and CIEM categories, AuthNull features include automated discovery of privileged accounts, JIT access, session recording, and AI-driven policy enforcement.

Key differentiators: Biometric MFA and passwordless authentication for frictionless access; autonomous AI agents that discover patterns and refine policies; and integration with LDAP, SSH, and DevOps tools. AuthNull reduces security incidents by up to 75% through proactive controls, meeting Gartner's emphasis on account onboarding and RPAM. Case studies show enterprises achieving compliance faster with its audit-ready logging.




# Privileged Access Management nice to have features that AuthNull Supports

These features enhance functionality and support advanced use cases, shaping a mature PAM program:

Privileged session management (monitoring, recording, real-time access control)

Comprehensive auditing (who/when/where privileged access occurred)

Agent-based privilege elevation (e.g., Windows, Linux, macOS)

Just-in-time privilege elevation to minimize exposure

Privileged account discovery across hybrid environments

PAM is a cornerstone for zero-trust and defense-in-depth, beyond compliance alone

AuthNull

# Discovery and onboarding of Privileged Accounts

Account discovery and onboarding are must-have capabilities in Gartner's PAM evaluation, enabling organizations to identify and secure all privileged accounts continuously.

AuthNull excels here scanning across endpoints, servers, and cloud services, automatically detecting local admins, domain admins, service accounts, and shadow admins.

How it works: AI agents perform real-time discovery, classifying accounts based on permissions and usage patterns. Onboarding integrates seamlessly with AD and LDAP, enforcing credential rotation and vaulting.

AuthNull

This addresses Gartner's pillar of tracking every privileged account, preventing "ghost" accounts that attackers exploit. Benefits include reduced manual effort—up to 80% automation—and compliance with standards like NIST, where discovery is key. In cloud scenarios, AuthNull's CIEM integration maps entitlements in AWS, Azure, and GCP, flagging over-privileged roles. A detailed dashboard provides insights, with alerts for anomalies like dormant accounts.

## Access Governance, MFA and Passwordless Authentication

Governing access is central to Gartner's second pillar, emphasizing life cycle processes and higher-trust authentication methods like MFA. AuthNull implements universal biometric MFA and passwordless options, supporting 1FA for Linux/Windows via identity-based verification, eliminating password vulnerabilities.

Features: Conditional access policies based on context (e.g., location, time, risk score); integration with external authenticators; and AI-refined rules for adaptive governance. This aligns with Gartner's recommendations for distinguishing PAM from general Access Management tools, focusing on privileged scenarios. In practice, AuthNull cuts access requests by 60%, using role-based workflows for approvals. For third-party access, it provides secure, audited channels, meeting Gartner's use case for external privileged users. Passwordless reduces phishing risks, with fallback to MFA for high-assurance needs.

**Privileged Access Management is a cornerstone**

PAM is a cornerstone for zero-trust and defense-in-depth, beyond compliance alone

A phased rollout is recommended—start with must-haves, then expand to include secrets management, CIEM, automation, analytics, integration with SIEM/ITSM, and resilience features (HA, break-glass

## Session Management, Recording and Auditing

Recording and auditing privileged activity form Gartner's third pillar, requiring tools for visibility and anomaly detection.
 AuthNull's PASM capabilities include centralized session management, full recording for databases and endpoints, and real-time monitoring with playback for audits.

Detailed functionality: Sessions are proxied through a secure gateway, logging commands and changes. AI analyzes recordings for threats, flagging deviations like unauthorized file access. This supports compliance audits, with searchable logs and integrations for SIEM tools.

Gartner notes session management as mature but differentiated by ease of anomaly identification. AuthNull enhances this with RPAM for remote vendors, ensuring no direct access and reducing risks by 90%. Automated reports operationalize auditing, aligning with DevOps needs

## Secrets Management and Credential Protection

Secrets management is a core Gartner tool category, growing in importance for DevOps and cloud environments.

 AuthNull's vault secures passwords, SSH keys, API tokens, and certificates, with programmatic access via APIs/SDKs.
Key features: Automated rotation, injection into applications without exposure, and support for nonhuman identities in pipelines. It integrates with CI/CD tools, addressing Gartner's emphasis on secrets for DevSecOps.

In hybrid setups, AuthNull protects service accounts across AD and cloud, preventing lateral movement attacks. Auditing tracks secrets usage, with AI detecting misuse. This capability ranks high in Gartner's use cases, where vendors like CyberArk lead, but AuthNull's agentless approach offers flexibility.

AuthNull

## Privilege Elevation, Just-in-Time Access, and Zero-Trust

PEDM is Gartner's category for controlled elevation on endpoints, including Windows, UNIX/Linux, and macOS.
 AuthNull supports dynamic elevation, removing local admin rights while allowing task-specific privileges via JIT.

JIT access, per Gartner's governance pillar, grants time-bound permissions based on requests, revoking them post-use.
 Zero-trust integration verifies every access, using context-aware policies.

Features: Endpoint agents (optional for deep PEDM) enforce least-privilege, blocking malware. This mitigates ransomware, as noted by Gartner. AuthNull's AI automates approvals, reducing admin overhead

Operationalizing tasks is Gartner's fourth pillar, advocating automation for reliability.

## AI-Driven Policy Engine and Automation

 AuthNull's AI-driven engine autonomously creates and updates policies, analyzing access patterns to suggest fine-grained controls.
Automation includes credential rotations, task scripting, and integrations with RPA/DevOps. This supports cloud entitlements via CIEM, managing IaaS permissions. Advanced AI detects threats proactively, like unusual privilege escalations, enhancing next-generation PAM as per Gartner.
Benefits: Faster incident response, compliance automation

AuthNull

# Benefits, Integrations, Case Studies, and Conclusion

Benefits of AuthNull include up to 90% incident reduction, immediate ROI through automation, and seamless compliance.
 Integrations: AD, LDAP, SIEM, cloud providers, DevOps tools.

Case Studies: A financial firm reduced breaches by 75% with JIT and secrets management; a healthcare provider achieved HIPAA compliance via auditing.

In conclusion, AuthNull transforms PAM by fully embodying Gartner's pillars and capabilities, offering a future-proof solution. Visit www.authnull.com to get started.