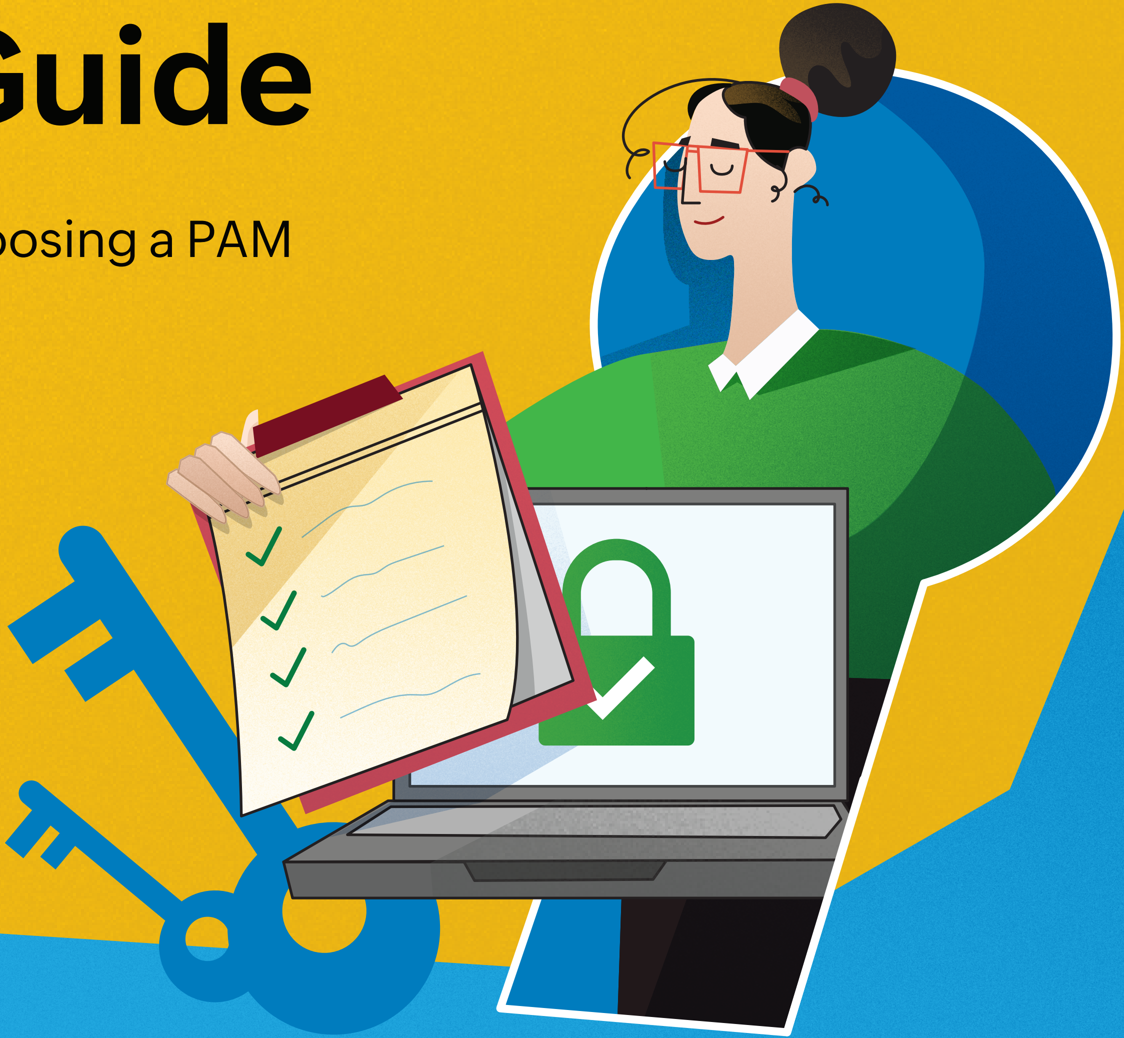
ManageEngine
PAM360

PAM Buyer's Guide

Everything you need to know while choosing a PAM solution for your enterprise.



Introduction

In today's cyber landscape, privileges comprise an integral part of an enterprise's business-critical components, such as operating systems, directory systems, hypervisors, cloud applications, CI/CD pipelines tools, and robotic automation processes. Cybercriminals are interested in these privileges because they can enable them to gain easy access to an organization's most critical targets.

The attack surface is rapidly expanding.

Abuse of privileged access and compromised identities has become the key vectors of modern cyberattacks. With the rapid and rampant adoption of hybrid work models, the traditional security perimeters have started to fade.

On-premises

Shared admin accounts

Service accounts

Desktops, servers and workstations

Network devices

Applications and databases

Hypervisors and virtual devices

Machine identities

Cloud infrastructure

Cloud management platforms

SaaS applications

Cloud-based entitlements

Workloads

Internet of Things

Industrial control systems,

OT and SCADA

Mobile workstations

BYOD, printers, sensors and other endpoints

DevSecOps

DevSecOps tools

CI/CD pipelines

Micro-services and container platforms

Types and categories of modern privileged identities

To safeguard against evolving external and internal threats, and meet increasing compliance demands, it is crucial to control, monitor, and audit privileges and privileged access for employees, vendors, systems, applications, and IoT devices within your IT environment.

How to use this guide

For I&O leaders, IT admins and security practioners in charge of identity security, selecting the appropriate privileged access management (PAM) tool to befit their enterprise requirements can be a challenging endeavor due to the widening threat landscape. Securing, monitoring, governing and auditing privileged access across the enterprise is essential for safeguarding mission-critical assets from both internal and external threat vectors, and proving compliance with industry laws, regulatory bodies and cyber insurance firms.

However, where do you begin? And once you've started, will your tool scale with the evolving maturity levels of the PAM market?

Most vendors offer PAM suites that come with bloated offerings, expensive add-ons, and contracts with long lock-in periods. These products might be a far cry from your organization's actual requirements. More efficient is a fully-functional PAM suite that is easy to install, configure, and launch, can be customized to your organization's unique business requirements, helps ensure regulatory compliance, and provides value to your IT investments almost immediately.

This PAM Buyer's Guide will help you get started with your PAM journey by providing you with all the basic and requisite details to help you choose a PAM solution that is right-sized for every business scenario, and which demonstrates how you can bolster your security posture, and how the right PAM tool helps you achieve optimal business outcomes. You also receive a complimentary vendor assessment checklists to help you compare PAM vendors during your evaluation process.

This guide is the result of ManageEngine's vast experience with hundreds of thousands of PAM deployments completed over the years, consisting of a myriad of security scenarios and challenges. We believe that every successful PAM journey should be well-informed and unbiased.

Critical capabilities to look for in a PAM solution

01 Privileged account management

The first and most crucial first step in achieving greater control over privileges is to gain visibility over privileged identities that are distributed across the organization, such as user accounts and passwords. According to Verizon's 2023 Data Breach Investigations Report (DBIR), over **49%** of all data breaches occurred because of weak or stolen credentials.

Embedded or hard coded passwords used across multiple systems, applications, and IoT devices further increase the likelihood of privilege misuse and unauthorized access. Manual management of privileged passwords—including periodic discovery, rotation, policy enforcement—is both unreliable and cumbersome. Without proper management tools in place, it is difficult to ensure complete control and security for critical credentials.

Critical privileged password management capabilities to look for in a PAM solution

PAM solutions are designed to enhance the lifecycle management of privileged accounts and credentials, including both human and non-human accounts. These solutions should be purpose-built for enterprise password management, and be able to automate the management of the lifecycle of privileged identities, such as passwords, keys, digital certificates, and so on.

This process includes automatic discovery, onboarding, vaulting, periodic rotation and live tracking of identities.

Here are some of the mandatory privileged account management capabilities to consider if you are looking to deploy a PAM solution in your organization:

Privileged account management checklist

☑ Performs end-to-end discovery, scanning, and onboarding of all the critical accounts and credentials associated with endpoints across the corporate network.

☑ Automatically stores and manages credentials across multiple platforms (Windows,

☑ Linux, Cloud, Unix, hypervisors, network devices) in a digital vault that is encrypted at multiple levels using algorithms, like AES-256, to ensure a secure repository of highly classified assets and credentials.

☑ Includes APIs to automatically fetch, manage, and rotate application password to eliminate hard-coding of credentials in files and scripts.

☑ Offers built-in controls to manage the lifecycle of other privileged identities, such as SSH keys, SSL/TLS certificates, service accounts, IIS App Pool accounts, and so on.

☑ Enforces true least privilege access by offering just-in-time (JIT) access and password request-release controls.

☑ Enforces strict password policies that cover password complexity, frequency of password resets, strong SSH key pairs generation, time-limited access to privileged accounts, automatic reset upon one-time use, and other robust controls.

☑ Integrates with developer tools, container platforms, RPA solutions for secure fetching and management of critical application credentials.

- ☑ Provides comprehensive audit trails of all privileged operations, such as user logins, password shares, password access attempts, reset actions, and so on.
- ☑ Provides fine-grained access controls based on user roles and access policies.
- ☑ Offers flexible SAML and RADIUS compliant MFA options.
- ☑ Provides break-glass options for emergency check-outs and controls.
- ☑ Includes options to manage and rotate credentials pertaining to custom devices, resources in DMZs and firewalled environments, as well as internal and legacy applications.

When considering a PAM solution for your enterprise, scalability is a factor that should not be overlooked. Depending on the size of your credential repository, you might need a PAM solution that can scale to manage tens or hundreds of thousands of privileged user credentials, keys, and certificates.

Solution: ManageEngine PAM360 offers a comprehensive account management module that offers end-to-end management of privileged credentials pertaining to multiple types of endpoints and IT resources. PAM360 offers assorted account management capabilities, such as account discovery, vaulting of credentials, access control workflows, remote password management, SSL/TLS certificate life cycle management, secure remote access, and so on—all built into a single platform.

02 Least privilege access and granular access controls

The least privilege access aims to shrink the attack surface by granting users permission to access only the mission-critical systems necessary for their current role, minimizing the risk of misuse or abuse. This strategy only elevates privileges as needed, reducing the threat surface and the potential for lateral movement, and minimizing risks such as phishing, social engineering, and ransomware.

Admin access is tightly controlled and audited to safeguard critical assets. However, relying on native or in-house tool sets to manage user privileges can be cumbersome and time-consuming. Despite the risks, some applications require elevated privileges to run. To minimize these risks without impeding IT productivity or bombarding the help desk with permission requests, most PAM solutions are equipped with least privilege controls that can automate the entire access provisioning workflows.

A PAM solution that incorporates Zero Trust and the principle of least privilege allows IT admins to restrict user privileges based on their roles, reducing the attack surface, and limiting potential damage caused by compromised accounts. These solutions should ideally eliminate access.

Here are some of the top least privilege access controls to look for in a PAM solution:

Least privilege and granular access controls checklist

☑ Conducts periodic audit to discover and identify accounts with excess privileges that have no associated owners.

☑ Defaults minimal, adequate privileges to users based on their roles. Grants elevated privileges on a temporary basis based on their requirements.

☑ Enforces access control policies at the application, service, and device levels.

☑ Removes administrative access rights to all servers within the network, and make every user a standard user by default.

☑ Provides fine-grained control over applications through controls, such as application allow-listing, sandboxing, and self-service privilege elevation.

☑ Enables admins to enforce SSH command filtering by allow-listing and grouping of select commands.

☑ Assigns JIT access and elevation controls for domain, root and local accounts through temporary administrative privileges.

☑ Assigns JIT access and elevation controls for domain, root and local accounts through temporary administrative privileges.

☑ Automatically rotates the passwords of critical devices after every use.

☑ Includes adaptive access control mechanisms, such as trust-score and policy-based access controls.

☑ Enforces restrictions on privileged command execution, application installations, and OS changes.

☑ Records live privileged sessions. Provides detailed audit trails of user activities to aid in compliance audits and forensic analyses.

Solution: PAM360's built-in Zero Trust access capabilities enable IT teams to implement JIT and least privilege access, application and command controls, and policy-based access provisioning across multiple types of resources and operating systems, thereby ensuring that the right users have administrative access to sensitive resources.

03 Governance, management, and security for cloud entitlements

As enterprise networks and cloud environments grow more complex, traditional access management solutions struggle to provide the granularity required to secure dynamic cloud infrastructure and associated privileges. PAM traditionally focuses on managing privileged access in on-premise environments, ensuring that sensitive accounts (admin users, superusers) are protected.

In multi-cloud or hybrid cloud infrastructures, managing privileged access becomes complex. Cloud infrastructure entitlements management (CIEM) enables centralized identity governance across multiple cloud platforms (AWS, Azure, Google Cloud), ensuring a unified approach to managing entitlements and privileges. PAM, when combined with CIEM, benefits from this multi-cloud visibility, helping organizations enforce consistent access controls across all cloud services. CIEM strengthens and complements the capabilities of PAM by providing specialized tools and controls for cloud infrastructure, ensuring that privileged and non-privileged identities in cloud environments are properly governed.

CIEM plays a crucial role in enforcing least privilege across cloud environments by continuously analyzing entitlements and removing unnecessary or excessive permissions. This helps prevent privilege sprawl and minimizes the attack surface. Further, cloud environments are dynamic, with resources, services, and access requirements changing frequently. While PAM can establish controls over traditional privileged accounts, CIEM automates the monitoring and management of entitlements across constantly evolving cloud environments. This automation ensures that the correct privileges are maintained in real-time, reducing the manual burden on security teams.

Cloud infrastructure entitlements management checklist

☑ Discovers and manages all entitlements pertaining to multi cloud infrastructure and security admin consoles.

☑ Correlates cloud entities from cloud service providers and understands the roles and corresponding privileges they carry.

☑ Periodically scans and monitors cloud environments to identify excessive permissions, unused/stale accounts, inadequate segregation of duties, policy violations, and other risky misconfigurations that can expose critical accounts and resources.

☑ Analyzes cloud IAM accounts and resources with excessive privileges, which are susceptible to exploitation.

☑ Visualizes access maps to understand access flows within users and determines excess privileges.

☑ Enforces least privilege access by assigning enough privileges to all the accounts.

☑ Automates policy resolution based on recommendations offered through real-time risk assessment.

☑ Audits cloud environments to detect accounts with excessive privileges.

☑ Offers mitigation insights and secures vulnerable accounts against privilege escalation attempts.

☑ Identifies and terminates potential risky behavior using real-time usage monitoring.

Solution: PAM360 delivers CIEM capabilities out-of-the-box, as a part of its native resources that help organizations streamline cloud entitlement governance from Day One. With PAM360, enterprises can confidently manage entitlements, accounts, and resources pertaining to multi-cloud platforms from a single console, ensuring their cloud environments are secure, efficient, and compliant.

04 Secure remote access for employees and third-party users

To perform their job duties effectively, employees, contractors, and third-party vendors require privileged access to remote systems. However, organizations often struggle to monitor vendor activities when accessing their network. Traditional remote access solutions such as VPNs grant excessive access, and often lack contextual security settings, comprehensive audit trails, and support for diverse operating systems and scenarios, leading to potential security risks.

Secure remote access is an integral part of PAM solution, as it enables administrative users to gain VPN-less and password-less access to critical IT endpoints, such as servers, applications, databases, hypervisors, and so on. PAM solutions should be well-equipped with session management engines for monitoring sessions and user activities in real time, by identifying, and terminating anomalous sessions, and enabling playback options for forensic and organizational audits.

Privileged session management checklist

- ☑ Eliminates access provisioning on “all-or-nothing” basis. Implements true least privilege by authorizing JITaccess for remote sessions.
- ☑ Provides instant, passwordless access to remote systems and applications using standard protocols such as RDP, VNC, HTTPS, and SSH.
- ☑ Includes granular session management controls such as session shadowing, recording and bidirectional file transfer.
- ☑ Enables remote access to third-party users and vendors through a thick client.
- ☑ Generates comprehensive audit trails of every user activity during the privileged sessions, as well as helps meet compliance requirements.
- ☑ Provisions secure access to remote data centers with jump server options.
- ☑ Includes options for offering app-only access, instead of providing access to the entire machine.

Solution: PAM360 has an integrated session management module that allows secure access to remote endpoints with a single click, without revealing passwords. The console logs and records all sessions started through PAM360, and administrators can track user activity and terminate sessions if they detect any suspicious behavior. PAM360 also offers instant, secure access to remote data centers through landing servers. In addition, PAM360 allows users to initiate RDP and SSH connections to target machines through a native desktop client.

05 Real time trust analysis to ensure Zero Trust privilege

Suspicious activities, such as failed login attempts, traffic from block-listed IPs, and so on, can remain undetected when they occur in isolation. When granting access to sensitive systems, admins are often challenged with the onerous task of sanctioning privileges based on the merits of user requests.

With appropriate access controls in place, users are granted the necessary privileges for their job roles. However, PAM tools should provide appropriate mechanisms to evaluate access requests based on multiple parameters, thereby helping admins identify and contain anomalous user activities in real time. These tools should assess potential risk parameters before granting access, and make access provisioning more contextual and stringent. For instance, how do admins provide their users with privileged access to critical applications that reside within isolated systems and networks? The answer is to verify user and device trust based on several critical security parameters.

That said, how do you get started with access provisioning based on real-time risk scoring and threat analytics? Here are some bare minimum essentials a PAM tool should sport to ensure Zero Trust privilege.

Adaptive Zero Trust access controls checklist

☑ Formulates baseline trust scores for users and devices based on critical parameters, such as login attempts, IP address, MFA status, and so on.

☑ Creates dynamic access policies based on contextual factors such as trust scores, existing access controls, and so on.

☑ Processes access requests automatically and grants access to users based on the best policy applicable.

☑ Isolates users and devices that are not compliant with the access policies, thereby eliminating any potential security risk.

☑ Initiates runtime actions for terminating anomalous activities based on the dynamic trust scores.

☑ Provides detailed audit trails of all privileged activities right from the time trust scores are generated, up until the user session has ended.

Solution: PAM360's approach to Zero Trust is the first of its kind in the industry. It entails leveraging a dynamic, automated trust score mechanism to assess real-time threats posed by users and devices. You can set customizable baseline trust scores for a variety of risk factors based on user and device parameters you deem vital for your organization's security. Subsequently, you can set up access control policies based on these trust scores and other crucial factors, and trigger automated follow-up actions.

06 Certificate lifecycle management

Enterprises rely on SSL/TLS certificates for secure communications and data transmission, and in the absence of an adequate certificate management system, businesses might experience unforeseen disruptions and expose themselves to potential exploits. IT admins must monitor and manage numerous certificates daily, including detecting vulnerabilities, tracking usage, and expiration dates.

In fact, certificate-related outages increased by 26% in the recent past, resulting in a total of 2.4 million hours of business downtime.

The certificate management process is often siloed, hindering visibility over certificate creation, deployments and expiration. PAM tools should be equipped with a native module to manage the entire lifecycle of SSH/TLS certificates. This includes controls to discover, create, deploy, renew, and manage encryption keys and certificates alongside privileged accounts.

Here are some of the critical certificate lifecycle management capabilities to look for in a PAM solution:

Certificate lifecycle management checklist

☑ Discovers and enumerates SSL/TLS certificates across multiple environments and endpoints.

☑ Automatically deploys certificates to applications and target devices.

☑ Provides timely certificate expiry alerts for quicker remediation.

☑ Offers integrations with third-party CA for effective management of certificate life cycles.

Solution: PAM360 provides a native module for managing SSH key and SSL/TLS certificates, which are an integral part of your PAM ecosystem. This module enables IT admins to automatically discover, manage, deploy, and track the entire life cycle of SSL/TLS keys mapped to mission-critical endpoints across the IT ecosystem. This eliminates the need for a standalone solution from other vendors to manage their SSL/TLS certificates and SSH keys.

07 Unified privileged user behavior analytics, auditing, and compliance reporting

PAM tools should offer a comprehensive privileged user behavior analytics (PUBA) module, which leverages AI and machine learning to analyze and derive user behavior patterns, and correlate privileged access data with other events across the enterprise to mitigate security threats in real time. This helps admins understand anomalous user activities, perform detailed root cause analysis, and remediate security events to minimize the risk of a data breach by extracting actionable inferences from the event data.

In addition, PAM tools should have built-in options to generate real-time logs and audits that can be sent to SIEM tools for further analyses. These audits should cover the entire “who”, “what”, and “when” of every privileged access activity, which IT teams can use to understand suspicious behavior, and make informed decisions in the future.

Privileged user behavior analytics checklist

☑ Includes native UEBA capabilities to analyze and build user behavior patterns for effective anomaly detection.

☑ Offers interactive dashboards to track and monitor privileged user access activities in real time.

☑ Generates comprehensive audit trails to delve into privileged access patterns, and swiftly terminate user actions that deviate from usual behavior.

☑ Shares data as syslog messages and SNMP traps with SIEM tools and network management solutions for further correlation.

☑ Provides instant reports for compliance mandates, such as HIPAA, PCI DSS, SOX, the GDPR, and so on.

☑ Provides historical data for deriving insights from multiple perspectives.

Solution: PAM360 offers native PUBA to detect and terminate suspicious user and activity on privileged systems effectively. The solution's PUBA capabilities are powered by deep learning and machine learning to monitor and establish comprehensive user behavior patterns. This enables IT teams to make informed security decisions based on past data. PAM360 offers real-time alerts for logged events such as privileged session activities, password changes, and policy updates. These alerts can then be sent to log management systems for further analysis and correlation.

08 PAM for workload identities

DevSecOps teams often require credentials for authenticating their workflows and microservices. These credentials are generally hard coded in files and scripts in plaintext formats, and are frequently used by multiple stakeholders working on CI/CD pipelines, RPA processes, and engineering workflows. If these credentials are altered without any prior planning or intimation, it could lead to a cascading failure of multiple critical processes simultaneously. Furthermore, if these credentials are exposed, even by chance, anybody with malicious intent could exploit them to breach an organization's critical information systems.

While it is clear that PAM needs to be integrated into DevSecOps processes, how do IT teams achieve it without compromising on speed and agility?

Solution: PAM360 provides out-of-the-box integrations with container platforms, DevSecOps CI/CD solutions, and RPA tools to ensure secure management of application credentials. This integration allows processes and applications to automatically retrieve credentials from PAM360's vault, and perform sensitive actions such as access provisioning, periodic password changes, granular control, and auditing, without disrupting internal workflows.

Additional factors to consider when deploying a PAM solution for your enterprise

In addition to all the critical capabilities described above, organizations should also consider these crucial factors while looking for a PAM solution.

Is value-realization faster with the tool?

Most PAM solutions come with bloated functionalities and implementation complexities, while some of them require skilled consultants or technicians to tailor their solution to your environment. Thus, you would need to direct your efforts and budget on capabilities, which could be a far cry from your actual requirements. PAM tools should be able to hit the ground running, without getting stuck in an implementation cycle or cycles that last for months.

Is your organization taxed by contractual lock-ins and exit barriers?

Some PAM vendors boast about their high retention rates, but that is often due to their long and complex contracts that restrict options for their customers. For many organizations during challenging economic times, IT budgets are shrinking and it is important to choose a PAM solution that does not come with long lock-in periods and intractable contracts.

Does the tool come with a complex pricing schedule?

Your PAM tool should not require you to navigate a complex maze of offerings. The à la carte pricing approach for critical capabilities coupled with expensive and lengthy implementations can makes a large dent in your budget and delay your value-realization.

Is the tool compliance and cyber insurance-ready?

With compliance and cyber insurance mandates becoming a non-negotiable need for many enterprises, PAM tools should include all the requisite capabilities to help you effortlessly comply with industry standards and insurance requirements.

What sets ManageEngine PAM360 apart?

PAM360 is ManageEngine's enterprise PAM suite, which helps enterprises enforce strict governance on access pathways to mission-critical endpoints and assets. Loaded with all the smart PAM essentials, PAM360 checks all the boxes for delivering a strong security posture while realizing a faster return on your investments. PAM360 takes a holistic approach to privileged access security, offering contextual integration with IT management solutions, developer tools, and business applications, which results in nifty insights, granular access controls, and quicker remedies.

Here are some reasons why over 5,000 enterprises like you trust ManageEngine with their PAM.

- **The right-sized PAM solution for the value-oriented enterprise**

  ManageEngine offers a comprehensive PAM portfolio that caters to all PAM use cases and enterprise IT maturity levels. PAM360, our flagship PAM solution, sports all the essential PAM capabilities for enterprises of all sizes. With flexible and easy-to-use deployment options, you can achieve the fastest value-realization on your security investments.

● Zero Trust by design, down to the last detail

PAM360 offers a multitude of granular Zero Trust security controls to regulate your access routines. These come as request-release workflows, role- and policy-based access provisioning, and dynamic user and endpoint trust scoring, among others. With these comprehensive capabilities, we've got your access activity covered and secured!

● Easy to deploy, achieve a rapid time to value

PAM360 is easier to install, configure, and manage, compared to other programs that push the boundaries of operational and maintenance complexities. With PAM360, you can hit the ground running. Most of our customers can fully implement PAM360 in four weeks or less. Further, we provide flexible deployment models to best suit your needs.

● Value-optimized pricing, realize a faster ROI

PAM360 provides a transparent pricing structure, without any hidden costs, bloated add-ons, or intractable contracts. The product is licensed only based on the number of admin users, without any cap on the number of end users or endpoints. PAM360 offers all the essential controls and capabilities you want in a PAM solution, without denting your IT budget.

- **Be part of ManageEngine's comprehensive IT management ecosystem**

  On an average, customers using PAM360 also use at least four other ManageEngine solutions, including ITSM, UEBA, IT analytics solutions. Our tightly-knit IT ecosystem helps our customers eliminate vendor fatigue, and create immense synergy to extend PAM across the enterprise.

- **Partner with a company whose business philosophy is deeply rooted in R&D**

  Zoho Corp., our parent company, invests 50% of its revenue in R&D efforts to build and future-proof resilient IT security solutions for the enterprises of today and tomorrow. We believe in building solutions, not acquiring them.

ManageEngine
PAM360

Complimentary PAM vendor comparison checklist

The following checklist is carefully curated to help you assess and compare PAM vendors based on the standard critical PAM capabilities they offer. Download our PAM buyer's guide, which provides you with all the basic and requisite details to help you choose a PAM solution that is right-sized for every PAM need.

Top privileged account management features

Feature	PAM360	Vendor A	Vendor B
Performs end-to-end discovery, scanning, and onboarding of all the critical accounts and credentials associated with endpoints across the corporate network.	✓		

Performs end-to-end discovery, scanning, and onboarding of all the critical accounts and credentials associated with endpoints across the corporate network.	✓		
Automatically stores and manages credentials across multiple platforms (Windows, Linux, Cloud, Unix, hypervisors, network devices) in a digital vault that is encrypted at multiple levels using algorithms, like AES-256, ensuring a secure repository of highly classified assets and credentials.	✓		
Includes APIs to automatically fetch, manage, and rotate application passwords to eliminate hard-coding of credentials in files and scripts.	✓		

Offers built-in controls to manage the lifecycle of other privileged identities, such as SSH keys, SSL/TLS certificates, service accounts, IIS App Pool accounts, and so on.	✓		
Enforces true least privilege access by offering JIT access and password request-release controls.	✓		
Applies stringent password policies that cover password complexity, frequency of password resets, strong SSH key pairs generation, time-limited access to privileged accounts, automatic reset upon one-time use, and other robust controls.	✓		
Integrates with DevSecOps tools, container platforms, RPA solutions for secure fetching and management of critical application credentials.	✓		

Provides comprehensive audit trails of all privileged operations such as user logins, password shares, password access attempts, reset actions, and so on.	✓		
Provides fine-grained access controls based on user roles and access policies.	✓		
Offers flexible SAML and RADIUS compliant MFA options.	✓		
Includes options to manage and rotate credentials pertaining to custom devices, resources in DMZs and firewalled environments, as well as internal and legacy applications.	✓		
Provides break-glass options for emergency check-outs and controls.	✓		

Least privilege and granular access controls

Features	PAM360	Vendor A	Vendor B
Conducts periodic audit to discover and identify accounts with excess privileges that have no associated owners.	✓		
Defaults minimal, adequate privileges to users based on their roles. Grants elevated privileges on a temporary basis based on their requirements.	✓		
Enforces privilege elevation policies at the application, service, and device levels.	✓		
Removes administrative access rights to all servers within the network, and makes every user a standard user by default.	✓		

Provides fine-grained control over applications through controls, such as application allow-listing, sandboxing, and self-service privilege elevation.	✓		
Enables admins to enforce SSH command filtering by allow-listing and grouping of select commands.	✓		
Assigns JIT access and elevation controls for domain, root, and local accounts through temporary administrative privileges.	✓		
Automatically rotates the passwords of critical devices after every use.	✓		
Includes adaptive access control mechanisms, such as trust-score, and policy-based access controls.	✓		

Enforces restrictions on privileged command execution, application installations, and OS changes.	✓		
Records live privileged user sessions. Provides detailed audit trails of user activities to aid in compliance audits and forensic analyses.	✓		

Cloud infrastructure entitlements management controls

Features	PAM360	Vendor A	Vendor B
Discovers and manages all entitlements pertaining to multi cloud infrastructure and security admin consoles.	✓		
Correlates cloud entities from cloud service providers and understands the roles and corresponding privileges they carry.	✓		
Periodically scans and monitors cloud environments to identify excessive permissions, unused/stale accounts, inadequate segregation of duties, policy violations, and other risky misconfigurations that can expose critical accounts and resources.	✓		

Analyzes cloud IAM accounts and resources with excessive privileges, which are susceptible to exploitation.	✓		
Visualizes access maps to understand access flows within users and determines excess privileges.	✓		
Enforces least privilege access by assigning enough privileges to all the accounts.	✓		
Automates policy resolution based on recommendations offered through real-time risk assessment.	✓		
Audits cloud environments to detect accounts with excessive privileges.	✓		

Offers mitigation insights and secures vulnerable accounts against privilege escalation attempts.	✓		
Identifies and terminates potential risky behavior using real-time usage monitoring.	✓		

Privileged session management

Feature	PAM360	Vendor A	Vendor B
Eliminates access provisioning on an “all-or-nothing” basis. Implements true least privilege by authorizing JIT access for remote sessions.	✓		
Provides instant, passwordless access to remote systems and applications using standard protocols such as RDP, VNC, HTTPS, and SSH.	✓		
Includes granular session management controls such as session shadowing, recording, and bidirectional file transfer.	✓		
Enables remote access to third-party users and vendors through a thick client.	✓		

Generates comprehensive audit trails of every user activity during the privileged sessions, as well as helps meet compliance requirements.	✓		
Provisions secure access to remote data centers with jump server options.	✓		
Includes options for offering app-only access, instead of providing access to the entire machine.	✓		

Adaptive Zero Trust access controls

Features	PAM360	Vendor A	Vendor B
Formulates baseline trust scores for users and devices based on critical parameters, such as login attempts, IP address, MFA status, and so on.	✓		
Creates dynamic access policies based on contextual factors such as trust scores, existing access controls, and so on.	✓		
Processes access requests automatically and grants access to users based on the best policy applicable.	✓		
Isolates users and devices that are not compliant with the access policies, thereby eliminating any potential security risk.	✓		

Initiates runtime actions for terminating anomalous activities based on the dynamic trust scores.	✓		
Provides detailed audit trails of all privileged activities right from the time trust scores are generated, up until the user session has ended.	✓		

Certificate lifecycle management

Features	PAM360	Vendor A	Vendor B
Discovers and inventories SSL/TLS certificates across multiple environments and endpoints.	✓		
Automatically deploys certificates to applications and target devices.	✓		
Provides timely certificate expiry alerts for quicker remediation.	✓		
Offers integrations with third-party CA for effective management of certificate life cycles.	✓		

Privileged user behavior analytics

Features	PAM360	Vendor A	Vendor B
Includes native UEBA capabilities to analyze and build user behavior patterns for effective anomaly detection.	✓		
Offers interactive dashboards to track and monitor privileged user access activities in real-time.	✓		
Provides comprehensive audit trails to delve deep into privileged access patterns, and swiftly terminate user actions that deviate from normal behavior.	✓		

Shares data as syslog messages and SNMP traps with SIEM tools and network management solutions for further correlation.	✓		
Generates instant reports for compliance mandates, such as HIPAA, PCI DSS, SOX, the GDPR, and so on.	✓		
Provides historical data for deriving insights from multiple perspectives.	✓		

About ManageEngine

ManageEngine is the enterprise IT management division of Zoho Corporation. Established and emerging enterprises—including 9 of every 10 Fortune 100 organizations—rely on ManageEngine's real-time IT management tools to ensure optimal performance of their IT infrastructure, including networks, servers, applications, desktops and more. ManageEngine has offices worldwide, including the United States, the United Arab Emirates, the Netherlands, India, Colombia, Mexico, Brazil, Singapore, Japan, China and Australia, as well as 200+ global partners to help organizations tightly align their business and IT. For more information, please visit manageengine.com; follow the company blog and on LinkedIn, Facebook and Twitter.