ManageEngine
PAM360

PAM maturity model

Craft a PAM journey that is your own

Introduction

Privileged identities have proliferated across every facet of companies' landscapes. They are now prevalent within fundamental components of the enterprise, both IT and otherwise, including engineering, human resources, payroll, operating systems, directory systems, hypervisors, cloud-based applications, CI/CD pipelines, and RPA routines. With more and more privileged identities being weaved into organizations' business workflows, there is now a need to manage authentication extensively and govern access to any and all critical business collaterals through these privileged identities.

Privileged access management (PAM) has been widely advised as a mandatory addition to your IT management portfolio, but it's no longer just that. PAM has surpassed its domain and purpose as a mere IT management strategy. It is now a business process necessity.

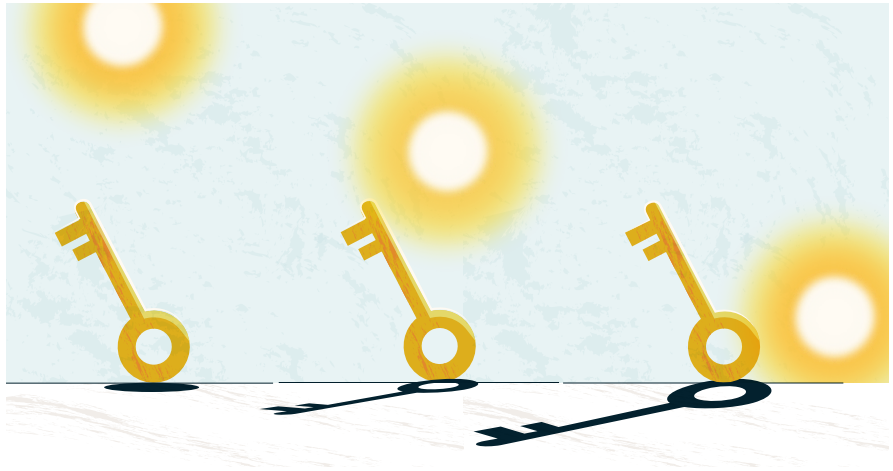
In order to govern privileged access, organizations are advised to incorporate PAM best practices into every part of their business process framework. However, this PAM deployment will differ for every organization depending on its maturity phase due to the fact that different organizations have unique infrastructures, risk profiles, financial priorities, security requirements, and specific use cases for privileged access.

Empowered by ManageEngine's tens of years of intricate research, inferences from thousands of PAM deployments, an omnipresent customer base, and our experience as a leading player in the global PAM market sphere, we have come up with a PAM maturity model that is all-inclusive but at the same time effective and uncompromising.

Our PAM maturity model will help you understand which maturity phase you are in and give you insights into how to navigate your PAM journey and increase your PAM maturity based on your risk profile, budget, types and number of privileged identities, and IT priorities, regardless of which industry vertical you belong to.

Identify your approach to PAM maturity

Your maturity and your attack surface are inversely proportional. The more PAM maturity you possess, the smaller your attack surface is.

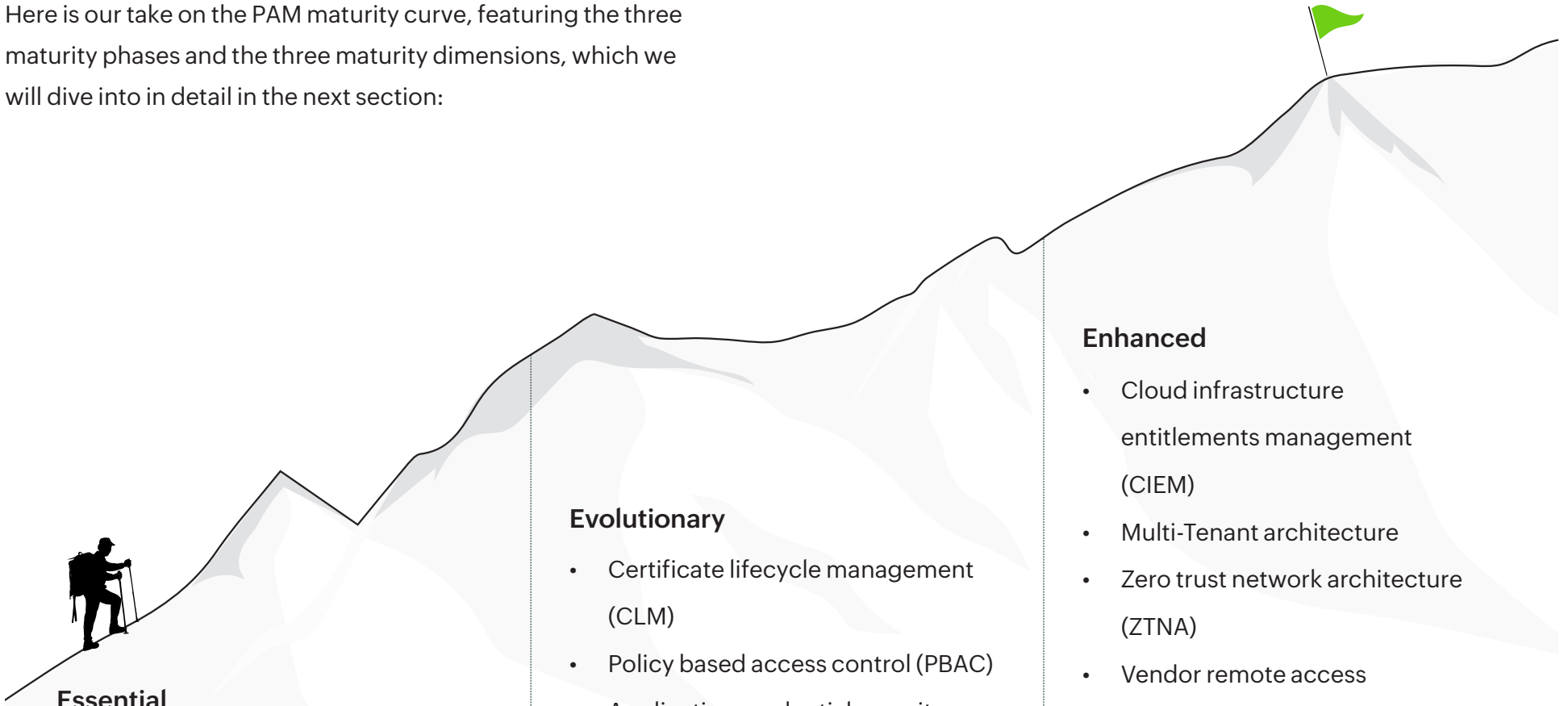


You will note that the wide range of use cases that PAM offers and the control it provides over your attack surface keep increasing as you traverse through each PAM maturity phase. Simultaneously, you will also notice an increase in the amount of automation involved (through integrations with other business and IT workflows) and the influence of AI-driven controls.

Various industry analysts have established a consensus on where a PAM journey typically starts and ends. They have also vastly discussed what PAM capabilities an organization should adopt on the path to becoming
PAM-mature.

Taking that into consideration, and based on our extensive research on market trends, we believe that all organizations, depending on their necessities, can be grouped into three phases: essential, evolutionary, and enhanced. Based on that interpretation, we have come up with a maturity graph that categorizes this vast set of PAM capabilities into three dimensions. We have also determined that an organization's maturity phase is judged based on how far the organization has implemented the capabilities under each maturity dimension.

Here is our take on the PAM maturity curve, featuring the three maturity phases and the three maturity dimensions, which we will dive into in detail in the next section:



Essential

- Privileged access governance
- Role based access control (RBAC)
- Audits and compliance

Evolutionary

- Certificate lifecycle management (CLM)
- Policy based access control (PBAC)
- Application credential security
- Privilege elevation
- Privileged threat analytics
- Integrations - ITSM and IGA

Enhanced

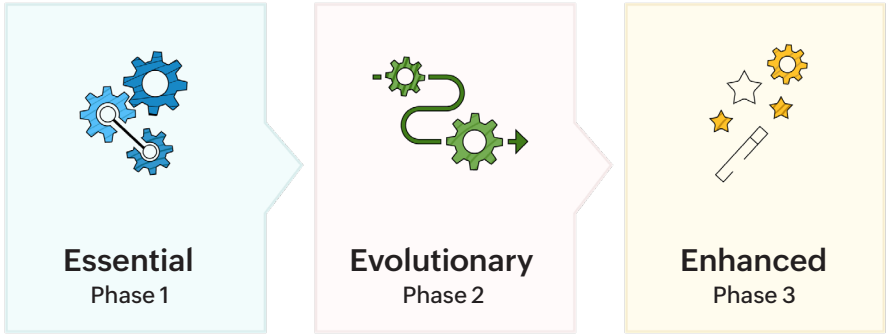
- Cloud infrastructure entitlements management (CIEM)
- Multi-Tenant architecture
- Zero trust network architecture (ZTNA)
- Vendor remote access
- Workload identity management
- Workflow orchestration

As you progress further from the origin of the maturity curve, you will notice that PAM will no longer be a siloed IT strategy that merely tends to secret sharing, but a mandatory addition to any business process.

PAM maturity dimensions

&

Maturity phases



We define each of these maturity phases this way in order to justify the complexity, effectiveness, and method of deployment of the controls contained in it. These controls and their method of deployment define the maturity phase itself and map out where it starts and ends, thus essentially defining its dimensions. Thus, these are what we like to call maturity dimensions. These maturity dimensions are based on the common consensus from popular industry analysts.

Maturity dimensions

Governance, risk, and compliance

Governance, risk, and compliance (GRC), in the context of PAM, refers to controls that enable organizations to take complete control over the processes of creating, discovering, sharing, and auditing privileged identities. GRC is not simply a PAM maturity dimension but also a security practice customarily followed by organizations and incorporated in any business process. The GRC dimension is primarily explored in the essential phase of your PAM journey.

Zero Trust

Zero Trust is a security framework that mandates the following three core principles in any and all business processes that involve the use of privileged identities: always verify, assume breach, and least privilege access. Access control measures that incorporate these three principles in their feature outlines, thus practicing the Zero Trust philosophy of privileged access and endpoint management, make up this dimension of our maturity model. Organizations tend to explore Zero Trust access controls vastly during their evolutionary phase, which boosts them closer than ever to the ultimate goal: Zero Standing Privileges.

Technical enablement

In our model, technical enablement is the solution that connects an enterprise's abstract IT potential with its real-time execution and implementation. When organizations take advantage of technical enablement, they are keeping pace with the latest technological advancements and leveraging them for transformative advancement.

In the context of PAM, controls that enable collaboration between your PAM solution and other third-party applications for the orchestration of privileged access routines are generally categorized as integrations. These integrations allow fluent communication between multiple business processes, interweaving PAM through every level across the enterprise. Further enhancing the fluidity of integrations, access controls, and GRC strategies by automating them is the icing on the cake.

This ensures that workflows run without manual overhead, weeding out human error and thus fulfilling the market standard for a PAM portfolio that demands Zero Standing Privileges. Technical enablement is majorly sought out by organizations in both the evolutionary and enhanced phases of their PAM journey.

Maturity phases

In the following sections, you will find detailed information on each phase, including specifics on what benefits you can look forward to, challenges that need addressing, and opportunities you need to explore in order to advance to the next phase.

What do we categorize as a benefit?

An organization that is on the road to digital transformation generally deals with amplified concerns surrounding risk and security. If the effect of a risk is reduced or eliminated altogether by adopting a control that is part of any of the mentioned maturity dimensions, we categorize this control as a benefit.

What do we mean by challenges?

If one or more of your existing controls does not cater to reducing or eliminating any of the security risks associated with your attack surface, you have a challenge that needs addressing. These challenges typically result in an increase in the manual administration overhead or attack surface.

What do we consider opportunities?

Addressing a challenge by adopting any measure that is part of any of the maturity dimensions in a particular maturity phase is an opportunity that needs to be explored. If such an exploration results in a reduction of the manual administration overhead or attack surface, there is a possibility of accelerating your PAM maturity and, in turn, advancing to a higher maturity phase.

Manual PAM

If your identity and access management IT portfolio does not incorporate any of the PAM dimensions mentioned above (GRC, Zero Trust, and technical enablement), that means you have yet to begin your PAM journey. At this point, there are not necessarily benefits that an organization can look forward to. In fact, organizations with manual PAM have multiple challenges to address and abundant scope for opportunities to explore.

Organizations that have yet to begin their PAM journey tend to practice secret management by hard-coding credentials and other privileged identities in text files and sharing them without proper request and release mechanisms, leaving room for critical identity threats and unproductive admin hours.

In the table below, you can observe what kinds of controls you are missing out on in each dimension if you are manually managing your privileged identities.

Maturity dimension	Controls
GRC	• No centralized management of privileged identities and users • No central inventory to manage privileged endpoints and secrets • No regularization or rotation of privileged identities • No measures in place to audit access sharing • No means of recording or reviewing privileged sessions • Failure to comply with federal IT standards such as HIPAA, SOX, and the PCI DSS
Zero Trust	• No means of providing ephemeral or periodic access to privileged domain or root accounts in Windows or Linux • No ability to share time-restricted access to privileged endpoints and secrets • No form of least privilege access (role- or policy-based access controls) in place • Heavy dependence on direct sharing with privileged domain or root accounts
Technical enablement	• No automatic discovery or onboarding of local and domain accounts • No integrations with any in-house IT tools, such as ITSM, ITOM, and IT analytics tools • No means of privileged access analytics using UEBA • No 2FA or MFA integration • No way to manage app-to-app and app-to-database credential requests • No means of managing critical secrets pertaining to CI/CD platforms, RPA routines, cloud containers, or microservices

If you fit into the above category and find yourself at the foothill of the PAM trek, that is only a good thing, because we have got you covered. If you do want to check out our PAM buyers' guide, which will help you begin your PAM journey by making the right decisions, you can do so here.

Phase 1
Essential

All organizations begin their PAM journey at this phase. In this phase, organizations are expected to opt for solutions to address their privileged identity vaulting needs. However, a small-scale organization with a small number of privileged endpoints and even fewer admins and users who need privileged access to such privileged endpoints tends to stick to this maturity phase until its risk profile demands otherwise.

If you have a mechanism or tools in place to help reduce the hard-coding of your privileged identities through the automatic discovery and rotation of secrets, central vaulting, and audited sharing of access to privileged identities, you are currently in the essential phase of your PAM journey.

Benefits

An organization that is on the road to digital transformation generally deals with amplified concerns surrounding risk and security. If the effect of a risk is reduced or eliminated altogether by adopting a control that is part of any of the mentioned maturity dimensions, we categorize this control as a benefit.

When you are in the essential phase of your PAM journey, there are several benefits that you can look forward to gaining, especially from the GRC dimension.

- Exercise governance over privileged users and accounts by securing their credentials in a centrally accessible PAM console.
- Enable MFA for privileged users accessing the PAM dashboard.
- Mandate access limitations in terms of the user roles of privileged users by assigning user roles that cater to specific access needs and nothing more.
- Enforce a request and release process that requires all access requests to be approved by specified IT administrators.
- Inventory passwords and reduce hard-coding by encrypting them using a central vault.
- Implement complex password policies for all passwords across the enterprise.
- Automatically discover privileged users, Windows local and domain accounts, Windows service accounts, Linux root accounts, network devices, virtual machines, and much more from multiple directories, such as AD, LDAP, and AWS.
- Set up automatic password reset routines according to organizational IT standards.
- Maintain end-to-end audit trails to keep track of all privileged activity in the network.
- Record all privileged sessions for access review, threat detection, and response measures.
- Conveniently generate reports that determine adherence to compliance standards, such as HIPAA, the PCI DSS, and SOX.

Challenges

In its essential phase, the primary challenge that an organization faces is the regularization of sharing digital secrets. In this phase, an organization typically has controls to manage secret sharing. However, these secrets need to be revoked manually by an IT administrator upon task completion. These secrets or passwords then need to be rotated by an administrator.

Furthermore, this access sharing is not ephemeral and does not limit the opportunities for privilege abuse during these privileged sessions. Once an access request is authenticated, the user has unlimited access to the entire machine and is unrestricted by time or access limits.

Opportunities

As you progress further, in order to overcome the challenges associated with your maturity phase, you must adopt strategies that will further scrutinize if secret sharing is necessary for each case. To further limit access sharing, adopt Zero Trust controls such as policy-based access controls, just in time (JIT) access and privilege elevation, and command and application controls for Windows and Linux endpoints.

Maturity dimension	Controls
GRC	• A central vault to manage users' privileged identities • A central inventory to manage privileged endpoints and secrets • Regularization or rotation of privileged identities • Automated auditing and recording of privileged sessions • Compliance with federal IT standards such as HIPAA, SOX, and the PCI DSS
Zero Trust	• Role-based access controls to assign access based on the employee's profile • A request and release process for access requests based on administrator approval
Technical enablement	• Automatic, scheduled discovery of privileged accounts from directories such as AD and LDAP • Automated, scheduled password resets of privileged accounts, including service accounts • Scheduled custom report generation for the privileged account inventory • Automatic revocation of privileged access based on a pre-stipulated time period

Conclusion

Organizations at this stage of their PAM maturity often establish controls as and when they see fit, reacting to inconsistencies in their IT networks whenever they turn up. Their approach to IT security is more reactive than proactive. They typically define access sharing on an all-or-nothing basis and have limited controls for threat detection, mitigation, and response. Their deployments often include an automatic account discovery feature that discovers accounts directly from the orgnization's directories as well as a role-based access control feature that serves as the highlight of this otherwise unpolished yet blooming maturity phase.

Phase 2
Evolutionary

The primary goal associated with phase 2 of PAM maturity is to reduce the number of privileged passwords shared and in turn increase the amounts of checks and measures in place for them. This is made possible by exploring the Zero Trust dimension beyond the binary approach to contextual access sharing and by dealing with access requests on a case-by-case basis. Furthermore, in this phase, organizations have fully functional integrations in place between their PAM solution, other IT management tools (such as ITSM tools), and secondary security solutions (such as extended detection and response (XDR) and SIEM tools).

If your organization has mastered access sharing through advanced, granular controls, such as JIT privilege elevation; trust-score-driven, policy-based access controls; and application and command controls, then your maturity is rapidly evolving.

Benefits

On top of the multiple benefits they enjoyed in the first phase, organizations in their evolutionary phase can add more feathers to their PAM maturity cap, with a focus on the Zero Trust dimension.

- Gauge user and device postures using real-time risk assessments to isolate potential threat actors. Employ a trust scoring system based on the risk assessments and devise appropriate access policies based on the scores.
- Configure access policies that allow or deny access requests automatically based on trust scores associated with privileged users and endpoints.
- Share temporary access to privileged accounts such as Windows domain accounts and Linux root accounts.
- Further limit the opportunities for privilege abuse during privileged sessions by mandating command controls and application controls.
- Extend PAM to not just passwords but also machine identities, such as certificates and keys, through certificate life cycle management.
- Govern app-to-app credential retrieval through tailor-made APIs.
- Regulate access to critical enterprise applications through secure access gateway servers.
- Integrate your PAM solution with ITSM tools to validate access requests based on the ticket ID generated in the ITSM tool.
- Integrate with UEBA tools to supervise user and resource behavior throughout your PAM deployment and mitigate any possible security risks.
- Integrate with identity provider (IdP) and identity governance and administration (IGA) tools to map privileges to users based on their attributes.
- Integrate with adjacent security solutions, such as XDR, SIEM, and SOAR solutions, to facilitate privileged endpoint and server access based on real-time threat analytics.

Challenges

In the evolutionary phase, the elephant in the room that every organization struggles to address is the enterprise-wide adoption of the Zero Trust principle of eliminating standing privileges. This elimination process is catalyzed by incorporating granular access controls to formulate all possible permutations for scrutinizing access requests and ensuring Zero Standing Privileges every step of the way.

This challenge goes beyond the realm of IT management, extending to any workflow in the enterprise network that demands privileged access. In the evolutionary phase, organizations struggle to expand the application of Zero Trust access controls across all facets of IT and business operations. This results from a lack of integrators and connectors, which allow the expansion of privileged access security for enterprise-wide PAM needs.

Opportunities

To conquer the challenges associated with the evolutionary phase, you must broaden your PAM deployment beyond IT. Automation and integration are the oil and grease that your otherwise fully functional PAM engine needs.

Although seemingly minor, invisible additions, technical enablement efforts that concentrate on integration and automation will polish your PAM deployment to run fluently and implement the principle of Zero Standing Privileges across all types of business processes. This can be approached through multiple angles, such as integrations with container platforms and DevOps tools as well as automation for robotic and business processes.

Maturity dimension	Controls
GRC	• Real-time risk assessments (popularly in the form of trust scores) for all privileged accounts, dependent on various privileged actions performed • Certificate life cycle management • App-to-app credential management
Zero Trust	• Policy-based access controls to validate access sharing based on user and endpoint behavior • Application and command controls for privileged endpoints • JIT privilege elevation of privileged accounts, such as Windows local and domain accounts and Linux root accounts • Access provisioning through secure access gateway servers
Technical enablement	• Integrations with ticketing systems to automate access provisioning • Integrations with IDP and IGA tools to achieve holistic privileged access security by applying access policies at a granular level and mapping privileges based on the user's role, department, directory groups, and requirements • Integrations with UEBA tools to determine baseline user behavior and detect potential threats from internal actors • Integrations with adjacent security solutions, such as XDR, SIEM, and SOAR solutions, to manage endpoint privileges and enable real-time event correlation to make better security decisions

Conclusion

Organizations in the evolutionary phase have a strong PAM routine in place to ward off privilege abuse through Zero Trust access controls. Although the evolutionary phase is a good place to be, organizations in this phase tend to miss out on the benefits provided by exploring technical enablement through integration and automation.

Phase 3
Enhanced

When an organization's PAM routine extends beyond the confines of the IT management infrastructure to encompass all privileged identities across the digital business landscape, it is poised to achieve escape velocity. Robust access controls devoid of hard-coded credentials blanket all levels of operations, employing multifaceted, multilayered measures to detect and prevent intrusions at various points. Industry recommendations also advocate for PAM features that regulate privileged access for third-party collaborators, such as auditors and vendors.

Simply put, when an organization's PAM has evolved to automate access controls comprehensively, embracing provisioning, rotation, deprovisioning, and reporting with an unwavering commitment to achieving Zero Standing Privileges at the enterprise scale, that organization is in the enhanced PAM maturity phase. Furthermore, organizations in the enhanced stage often seek to augment their security posture with a cloud infrastructure entitlement management (CIEM) solution to govern cloud access risks, especially in hybrid and multi-cloud setups.

Benefits

While mastering access controls can certainly help an organization gain considerable momentum in its PAM journey, the benefits it enjoys in the enhanced phase are what allows it to attain the ultimate goal of Zero Standing Privileges.

- Practice identity governance for legacy systems, multi-tenant infrastructures, SaaS, and internal applications.
- Set up step-up authentication mechanisms for a layered approach to privileged access security.
- Expand PAM to the network, application, and database levels by adopting Zero Trust network access (ZTNA) principles.
- Integrate with cloud container and DevOps platforms to automatically fetch and rotate encrypted secrets from cloud clusters and container platforms, such as Kubernetes, according to custom organizational policies.
- Automate and integrate privileged access routines across other business apps.
- Centrally manage cloud access risks by implementing a CIEM solution.

Challenges

In the enhanced phase, your deployment is no longer responsible for just simple access management; it is an umbrella that covers every form of privileged access, including and beyond IT. An organization that finds itself in this maturity phase generally struggles with scaling its privileged access security routines to geographically distributed sites. We suggest opting for a PAM vendor that supports effortless upscaling opportunities without levying migration costs.

As your enterprise's operations begin to span multiple geographies, the most important thing to do is to maximize disaster recovery mechanisms by fully automating failover services to operate in adverse situations so that they do not require manual intervention, thereby ensuring seamless business continuity.

While pursuing an uncompromising approach to Zero Standing Privileges is necessary, we also believe that this approach must be financially prudent. All PAM deployments need to be value-optimized to avoid hidden costs and remove unnecessary, over-the-top capabilities that are either seldom needed or harmful to your IT budget in the long run for no real results.

Opportunities

While on the cusp of your PAM journey's fruition, the improvement that your organization can incorporate into its IT profile is error-free maintenance, especially now that all your PAM routines are mostly expected to work on their own. Error-free maintenance involves constant updates to discovery schedules, reset schedules, and access control settings as well as constant supervision of integrated links between your PAM tool and other business applications.

An opportunity on which to capitalize that most PAM-mature organizations tend to overlook is your ROI. It is important to optimize controls in order to achieve a quick time to value on your ROI from your PAM solution. It also comes in handy to be up to date with the latest market trends and PAM features in order to make the best decision when upgrading your PAM solution.

Organizations can take advantage of extending PAM beyond passwords and secrets to an extensive range of machine identities, such as IoT devices, operational technology (OT) and supervisory control and data acquisition (SCADA) systems, and other workloads that are not conventionally managed within the scope of PAM.

An organization is fully PAM-mature if its existing controls satisfy its existing risk profile and boast Zero Standing Privileges across all forms of privileged access throughout the organization.

Maturity dimension	Controls
GRC	• Governance for legacy systems, multi-tenant infrastructures, SaaS, and internal applications • Access governance and monitoring for cloud entitlements
Zero Trust	• Step-up authentication for layered Step-up authentication for layered privileged access policies • ZTNA to manage network-, application-, and database-level privileged access • One-click access through the PAM solution for third-party vendors and other collaborators who require privileged access
Technical enablement	• Integrations with DevOps tools and CI/CD pipelines for managing secrets shared across engineering routines • Integrations with container platforms like Kubernetes to automate cloud-cluster-based secret management • Integrations with RPA tools to manage secrets that authenticate bot routines • Business workflow automation to weave privileged access security throughout all enterprise applications and orchestration routines

Conclusion

Organizations in the enhanced phase have all the bases equally covered. They have a fluent account discovery practice that works on its own without manual intervention to onboard privileged accounts on the go, thus fulfilling their GRC needs. These organizations also have granular access controls in place to counter unauthorized access and privilege abuse as a result of exploring and adopting the Zero Trust philosophy of IT management throughout their security routines. These controls are also entirely automated and capable of contextually integrating with other enterprise IT or business applications.

How quickly should you accelerate your PAM maturity?

No two organizations follow the same color palette of changes when it comes to PAM maturity acceleration. For organizations that are new to the digital transformation bandwagon, protecting access to their limited number of privileged identities will have a huge impact on their risk profile, and the other dimensions (Zero Trust and technical enablement) might follow later.

However, as organizations start to leave a larger digital footprint, their risk profile also evolves to incorporate more complex priorities. With expansion also arises the need for scalability and a bigger IT budget. But in certain cases, even though a company might scale digitally, their workforce might remain stagnant, leading to fewer administrators managing a broader, more diverse range of critical endpoints. These organizations will naturally tend to prioritize automation over other aspects of PAM.

In contrast, a company that has limited critical endpoints but is now expanding its client base will tend to collaborate further with third-party vendors, contractors, and partners. This type of organization tends to prioritize IT spending on complex Zero Trust access control measures.

Organizations that are pursuing the PAM journey through a route that mandates compliance will tend to prioritize authentication controls, privileged session recording, and other capabilities that assist with meeting compliance standards.

At the end of the day, maturity acceleration boils down to each organization's risk profile, IT budget, and priorities.

How can ManageEngine help?

ManageEngine's enterprise PAM suite helps enterprises enforce strict governance on access pathways to mission-critical endpoints and assets. Loaded with all the smart PAM essentials, our suite checks all the boxes for delivering a strong security posture while helping you realize a faster ROI. ManageEngine's PAM products take a holistic approach to privileged access security by offering contextual integrations with IT management solutions, developer tools, and business applications, resulting in nifty insights, granular access controls, and quicker remedies.

Our business philosophy is deeply rooted in research and development (R&D), so much so that our parent company, Zoho, 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.

With such experience in the field of IT comes our preliminary outline on which our PAM products are built: PAM is not a one-size-fits-all solution. ManageEngine's cutting-edge PAM products are designed to be kick-started where and when you need them, optimized to ride alongside your trajectory as you progress through the PAM maturity curve. We have proven expertise in building extensive IT management solutions that can natively and contextually integrate. On average, a customer who uses a PAM solution of ours uses at least five other ManageEngine products, thereby effectively eliminating vendor fatigue.

Our ultimate goal is not to make an offer you cannot refuse but to make products that you will actually use. Our mission is defined by your progress. We are here to supply you with the right tools, resources, strategies, and expert advice that you need in order to navigate through a PAM journey that is your own.

Why trust ManageEngine with your PAM journey?

ManageEngine's enterprise PAM suite helps enterprises enforce strict governance on access pathways to mission-critical endpoints and assets. Loaded with all the smart PAM essentials, our suite checks all the boxes for delivering a strong security posture while helping you realize a faster ROI. ManageEngine's PAM products take a holistic approach to privileged access security by offering contextual integrations with IT management solutions, developer tools, and business applications, resulting in nifty insights, granular access controls, and quicker remedies.

Here are some reasons why over a million IT administrators trust ManageEngine with their PAM:

The rightsized 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, 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

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, easy-to-use deployment options, you can achieve the fastest value realization on your security investments.

Easy to deploy to achieve a rapid time to value

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

Value-optimized pricing to realize a faster ROI

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

Part of ManageEngine's comprehensive IT management ecosystem

On average, customers using a ManageEngine product also use at least four other ManageEngine products, including ITSM, UEBA, and IT analytics solutions. Our tightly knit IT ecosystem helps our customers eliminate vendor fatigue and create immense synergy to extend PAM across the enterprise, thus helping them progress through their maturity phases quickly yet coherently.

ManageEngine

PAM360