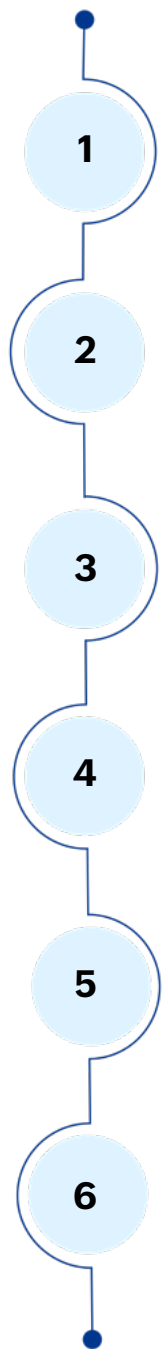




The cost of a PAM implementation



Contents



1	Introduction	– 3
2	Software licensing costs	– 4
3	Infrastructure costs	– 7
4	Professional service costs	– 9
5	Supporting technology costs	– 12
6	Onboarding and training costs	– 14

What is the cost of a PAM implementation?

At a glance, this might seem like a straightforward question.

However, while budgeting for the purchase of any kind of IT software, there are several factors to consider apart from the obvious software licensing costs, and that applies to PAM implementations as well.

This document will dissect all the hidden costs and additional services that you need to look out for and that could break your IT budget if you're not careful. We will also discuss how to navigate these complex pricing conditions through advanced planning and by setting smart priorities while implementing a PAM solution in your organization.

Simultaneously, this document will also argue that choosing PAM360, ManageEngine's full-stack PAM platform bundled with all the necessary PAM essentials and beyond, eradicates unnecessary, bloated billing troubles.

What should you look out for?

If your organization is yet to implement a PAM solution and is looking to purchase one, we recommend you take a look at our [PAM Buyer's Guide](#). It's the one-stop, ultimate guide for everything you need to know while choosing a PAM solution for your organization.

Alternatively, if your organization has taken the primary steps towards implementing a PAM solution and is looking to upscale into a more advanced deployment, you must leverage our [PAM maturity model](#) to prioritize the must-have and good-to-have objectives of your PAM plan based on your IT priorities, budget, scale, and more.

But we digress; let's stick to the economics, for now. First thing's first.

Software licensing costs

Let's start with the obvious.

Choosing a PAM license that fits your needs and leaves room for your IT budget to breathe must be your number one priority. To accomplish that, you need a vendor that delivers the essential features that satisfy your use cases without hamstringing you along with intractable contracts and expensive purchase loops—which happens to be a favorite customer retention strategy for most vendors.

But let's not get ahead of ourselves.

Figure out if your PAM priorities call for purchasing a new solution to handle the typically vast amount of privileged access use cases or if you can quickly adopt a PAM action plan with existing software.

More often than not, organizations use full-scale PAM solutions as mere password vaults. So, it's better to identify what is already deployed in your environment and figure out if you can use those existing solutions to handle your privileged access security use cases before jumping the gun on a new purchase.

When it comes to PAM, vaulting privileged identities in your environment with the help of a password management tool might seem like enough to keep things intact, in theory. Practically, it leaves you wishing for a more granular approach to addressing standing privileges.

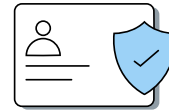
Several industry experts and analysts recommend certain primary controls apart from credential vaulting to be covered while structuring a PAM portfolio.



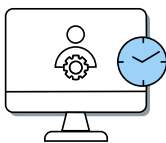
**Governance and
administration**



**Discovery and
onboarding**



**Credential
management**



**Session
management**



**Elevation and delegation
management**



**Logging, reporting,
and auditing**

What else?

When looking for software, it's crucial to purchase solutions that integrate seamlessly with your current environment without causing IT operational hazards or discontinuities while also extending the use cases of your existing infrastructure. Seek a PAM solution that both blends with other facets of your IT environment and leverages existing routines, making your privileged access strategy more efficient.

Despite these core components being essentially interdependent, vendors typically split these modules into multiple siloed solutions requiring separate purchases, thereby maximizing their profit during implementation.

Integrated security with ManageEngine PAM360's all-inclusive pricing

ManageEngine PAM360 challenges this a-la-carte approach by mobilizing all the necessary PAM essentials into one integrated identity security platform designed to blend with your existing IT ecosystem.

Unlike other vendors that push add-ons, PAM360 offers a unified, all-in-one PAM solution—no silos, no upsells. With transparent pricing and a straightforward licensing model, you pay only for admin users and keys while discovering unlimited privileged accounts and endpoints.

The base pack with 10 administrators and 25 keys starts at \$7,995/year. Moreover, regardless of the size of your purchase, we provide free, annual maintenance and support for all customers. You can find our pricing model [here](#).

Infrastructure costs

The software adapts to your infrastructure, not the other way around.

The traditional claim that software is only as efficient as the infrastructure in which it is hosted is a myth—an oversimplified statement made to justify the complex design and architecture of solutions that vendors build.

Infrastructure bloating

Most PAM solutions that boast an arsenal of bloatware—half of it serving no real purpose when it comes to the essential core of access management—demand a huge infrastructure footprint from their clients, i.e., organizations such as yours.

This will increase the total cost of your PAM implementation in two ways.

One, these solutions are already overpriced owing to the unnecessary add-ons that are mandated as part of the software license, making you spend more than what's required for your needs. Two, you will also end up spending more on futile infrastructure upgrades as well as on actual licensing costs (even considering the overpricing) trying to maintain such an environment.

These costs can skyrocket, especially for on-premises offerings. Vendors often demand additional physical or virtual servers for each and every component of core PAM functionalities, such as a password vault, password rotation, remote access and session monitoring, SSH key and TLS certificate management, privilege elevation, session recording, and behavioral analytics.

ManageEngine PAM360's infrastructure requirements are zero to none

PAM360 is built to challenge the traditional “more is more” philosophy that justifies creating solutions packed with unnecessary features that offer little value to core access management functions.

Since PAM360 consolidates all essential PAM functionalities into one platform, you don't need multiple servers or complex infrastructure setups—it's a straightforward deployment that delivers comprehensive PAM without the infrastructure bloat. By eliminating this bloat, you can further reduce both the immediate and long-term costs that come with maintaining your otherwise large infrastructure footprint.

PAM360 comes bundled with libraries for immediate deployment, but we understand organizations have diverse infrastructure needs. That's why PAM360 seamlessly integrates with various database platforms, allowing you to leverage existing investments without compromising performance.

Professional service costs

Time is money.

Professional services, regardless of their persuasion, are necessary for a speedy and hassle-free PAM implementation, especially to set up integrations and perform updates and customizations. As your implementation scales up, you'll need to account for these add-on professional services as well.

PAM vendors typically pump up the professional service dependency during the implementation phase and beyond, taking up another chunk of your expenses. Every passing day, your PAM deployment isn't complete; you're paying for professional services, thus increasing your total implementation cost.

Blackboxing

Another way professional services could be forced into your billing proposal is when vendors offer proprietary blackbox solutions and corresponding hardware as part of your software purchase.

Contradictory, isn't it?

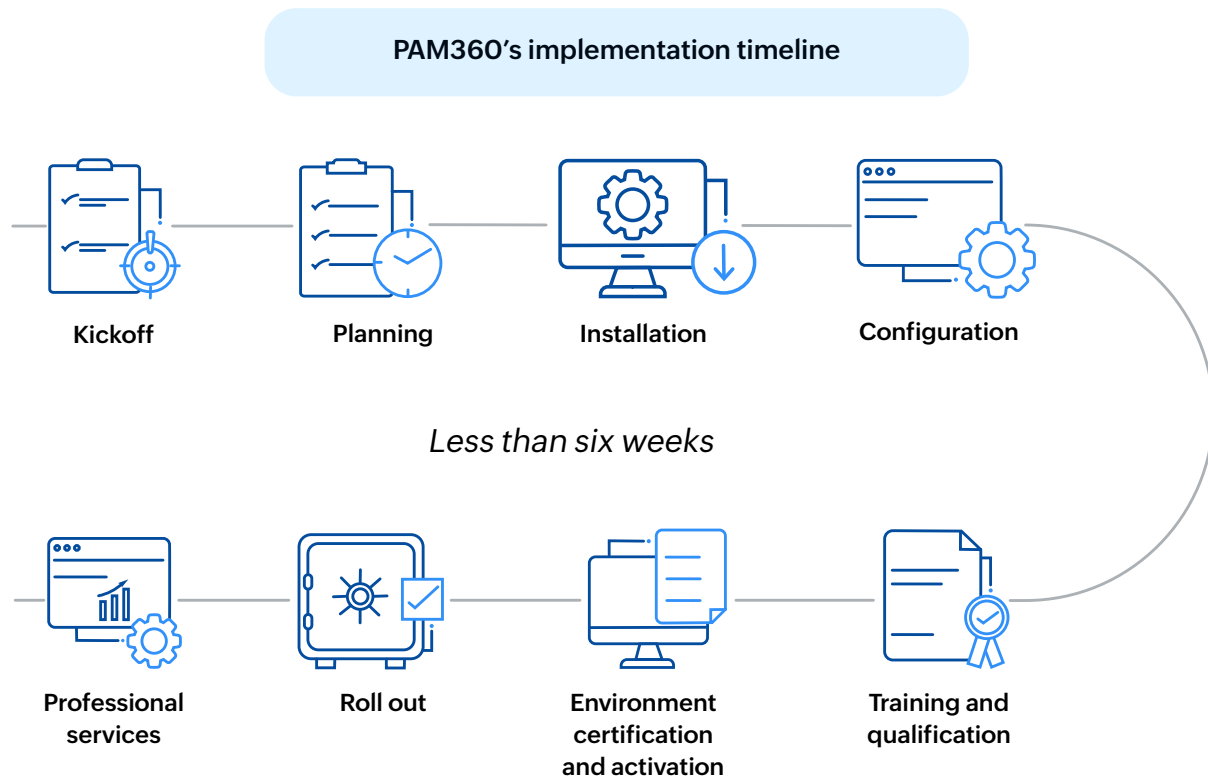
Your IT teams will have zero control over this hardware, making it a compliance nightmare. This is because every time the blackbox solution needs to be updated or modified to suit your policy requirements, you will be persuaded to pursue professional services from the vendor. It is much simpler, faster, and cheaper when you are in control of when and how you want to patch your systems.

Customization

Relying on professional services for every small modification can be expensive. If you need to integrate with legacy tools or automate password resets for custom endpoints, the solution should support infrastructure-specific scripting that you can manage yourself. Avoid vendors that lock you into proprietary tools or ongoing service fees—true extensibility means you control customizations without constant

external support. Over time, your dependency on professional services should naturally decrease after the initial implementation phase.

Professional service dependency with PAM360, or lack thereof



Our team can fully deploy PAM360 with all integrations and customizations in place in high availability mode across multiple servers in less than six weeks, which is normally one-fourth of the time it would take to get another solution on the market simply up and running. PAM360's intuitive UI and easy-to-use design facilitate an exponentially smaller learning curve compared to other vendors' complicated solution dynamics, which call for rigorous training, making the job easier for our implementation professionals and your administrators.

Here's how we make it that simple.

Our solution functions as a self-managed on-premises tool. That means you're in full control of the hardware that you choose to run the service on, so you have complete control over making modifications to your hardware to meet policy standards, with zero dependency on the professional services we have to offer.

Unlike solutions that lock you into proprietary hardware or mandate vendor-specific infrastructure, PAM360 relies on easily available, off-the-shelf configurations. Your IT team can directly manage, upgrade, or modify the infrastructure based on your organization's needs and compliance requirements without waiting for expensive vendor consultations or professional service engagements.

This vendor-agnostic approach not only reduces your total cost of ownership but also accelerates deployment and maintenance cycles. Your team can quickly implement changes, perform upgrades, or scale the infrastructure using standard hardware and your existing operational procedures. Whether you need to add more storage, enhance processing power, or implement new backup systems, you can do so using your preferred hardware vendors and internal IT processes, eliminating the costly overhead of vendor-mandated professional services for routine infrastructure management.

Supporting technology costs

Software that depends on other software to satisfy your use case is not a solution. It's a complication.

Solutions that depend on additional software licenses are often based on outdated PAM architectures and can bump up your expenditure.

For example, in certain cases, the vendor's offering might use legacy tech, such as jump hosts for session recording, which will force you to purchase separate Microsoft Remote Desktop Services licenses for every privileged remote user you onboard into the solution.

Some vendors might require you to purchase additional databases, load balancers, or in some cases even an entire operating system (OS) since their solutions are only optimized enough to function in a particular OS environment.

Some solutions do not offer reporting systems as part of the out-of-the-box PAM bundle. Though a PAM solution's significant role is addressing your organization's GRC mandates, some vendors offer less than 10 audit reports and charge you for creating additional reports. Some vendors might push costly professional services to customize reports; or worse, they might require external reporting or data visualization software.

You should be able to generate reports that detail privileged user activity in your environment when you want it, the way you want it. Therefore, look for vendors that offer free, built-in reports for major global compliance standards that will keep you perpetually ready for internal and external audits. You should be allowed to generate an unlimited number of reports without charges, with options for customization as needed.

Even primal elements of a PAM stack, such as certificate life cycle management, vendor access management, and secrets management, are often bifurcated and sold as separate entities by a single vendor. This fragmentation not only increases total cost of ownership but also introduces significant operational complexity, as

security teams must manage multiple interfaces, coordinate various renewal cycles, and ensure seamless integration of disparate systems.

PAM is a constantly evolving discipline, shaped by the ever-expanding landscape of privileged identities. To stay ahead, your solution must not only align with current IAM trends but also anticipate and adapt to the broader spectrum of PAM use cases. A thorough evaluation of the vendor's roadmap is essential to ensure a commitment to innovation, with the latest advancements seamlessly integrated as free upgrades.

PAM360: An integrated enterprise PAM platform

PAM360 can be deployed in any popular OS and does not require additional licenses to implement the basic PAM functionalities.

When you deploy any ManageEngine product in your environment, you deploy a part of a much larger, entire IT ecosystem. That means regardless of what your use case might be, there is always a solution within arm's reach for you to simply plug and play. So if you're looking to expand your PAM arsenal beyond the scope of conventional PAM, you can leverage the **ManageEngine ecosystem** advantage to integrate PAM360 with our in-house IT management suite and third-party solutions to cover extended use cases.

For example, while we offer integration opportunities with popular ITSM tools such as Jira, ServiceNow, and other ticketing systems to validate privileged access requests with service ticket IDs, by integrating PAM360 with our in-house solution ServiceDesk Plus (which is available both on demand and on-premises), you eradicate all the support and professional service complications that may arise, which could result in unnecessary expenses and be a waste of precious admin time.

PAM360 encapsulates all the cyber essentials you need in a PAM solution, seamlessly integrating across identity governance, threat analytics, user behavior analysis, cloud security, and workflow orchestration. By consolidating critical security functions into a unified platform, it reduces complexity, eliminates cross-vendor dependencies, and streamlines identity security management across your organization.

Onboarding and training costs

Choose software that reduces the workload and doesn't increase your workforce.

If you've stuck with us until now, it's safe to assume that you understand the complexities that might arise during a PAM implementation, and that it can sometimes prove to be a laborious task. So it only makes sense to allocate room for human resource expenses in your budget.

Assess your workforce and determine if you need to hire a dedicated team to manage your PAM solution or if you already have a part of the workforce that you can leverage. While you're at it, make sure you make considerations for salary, benefits, and training costs and time. As an enterprise ourselves, we at ManageEngine have noticed a perennial need for skilled cybersecurity experts, and it can prove to be a challenging task to find them. Therefore, it's important to ensure that you have a PAM solution in place that is easy to train people on and offers an optimal user experience that requires a very small learning curve.

Rarely do vendors take a modular approach towards building their PAM solutions. Since often all the necessary functions of a basic PAM portfolio are separated by vendors into individual software, it's almost as if your administrators need to be trained on five to six different solutions (sometimes even from multiple vendors) instead of just one. We strongly recommend that you opt for a solution that offers a free trial with options for extension upon request. This will help you get a vivid idea of the effort you will need to put in to manage the solution from end to end. The free trial should be able to answer two important questions:



Are you able to set up the basic configurations of the solution from scratch without the need for vendor support?



Is the product easy enough for your existing workforce to pick it up without rigorous training?

PAM360 is layperson friendly

PAM360 is recognized by industry analysts and our customers alike for its easy-to-implement and quick-to-use design. With PAM360, you can hit the ground running in less than six weeks, including installation, configuration, training, certification, and everything else you need to have a fully functional deployment across multiple sites.

While this might differ based on the scale of the environment you intend to secure, our customers have never required dedicated resources to manage the solution. The majority of other PAM vendors normally require three to four dedicated, full-time resources to maintain their solutions owing to their complexity, thereby extending their PAM implementation process.

Furthermore, all our product-related literature can be found on our website free of cost, right from the installation guide to a solution brief detailing every step of the installation and deployment process. We also have extensive product help documentation hosted online that deep dives, step by step, into the nitty gritty of each and every configuration process, ranging from MFA setup to integrations and everything in between

You can straightaway download and install the fully functional [trial version](#) of PAM360 for 30 days. We also offer a free, personalized consultation with our security experts, who will assess your environment, identify process and security gaps, and offer recommendations to strengthen your security posture. We'll evaluate your organization's PAM maturity and provide customized recommendations to implement and scale PAM360 based on your security needs.

Think our claims seem too good to be true? Well, we thought so too—until we realized how vendors have bloated the market with their overpriced solutions and impossible infrastructure expectations, leading to a bubble that organizations such as yours are forced to fit into.

Don't trust us?

The ManageEngine PAM360 promise

To compare apples to apples, fetch a proposal from any other leading PAM vendor in the market for an on-premises deployment model. We promise that you'll barely spend a fraction of that cost if you choose to implement ManageEngine PAM360 instead.

Have doubts? [Get a quote](#) tailor-made for your enterprise's needs.

Feel free to [schedule a personalized demo](#) of the product before you do so. Or if you would like to play around and test the solution, [download PAM360 for free](#) and take it for a test drive.



ManageEngine
PAM360