

A Privileged Access Management Guide

for Mid-Market and Lower Enterprise Organizations

Table of contents:

1.	Introduction _____	04
2.	About the Company _____	07
3.	What Is Privileged Access? _____	10
4.	What Is Privileged Access Management? _____	13
5.	Privileged Access Management Challenges _____	15
	• The missing granular insight and the challenge of a manual process _____	16
	• The risk posed by privilege excess _____	17
	• Shadow privilege risk _____	17
	• Default credentials and those stored in unencrypted files _____	18
	• Privileged sessions are not managed from a central location _____	18
	• The PAM tool interface is complicated _____	18
	• Companies fail to meet audit requirements _____	19
6.	Why Is Privileged Access Management Important? _____	20
	• It prevents cyberattacks _____	22
	• It properly manages, protects and provides a good overview over privileged accounts _____	23
	• It supports productivity _____	24
	• It supports compliance providing a clear-audit trail _____	24
	• It prevents lateral movement across the network _____	25

7.	How Privileged Access Management Works	26
8.	Privileged Accounts Types	28
	• Privileged User Accounts	29
	• Privileged Service Accounts	32
9.	Privileged Attack Vectors	34
10.	Privileged Access Management Related Concepts	38
	• IAM vs. PAM	39
	• PASM and PEDM	40
	• The Zero-Trust Model	41
11.	Traditional PAM vs. Modern PAM	43
12.	Privileged Access Managements Myths	45
13.	Privileged Access Management Best Practices	47
	• Make an inventory of all your privileged user accounts within the company	48
	• Perform a risk assessment	48
	• Separation of duties and segmentation of systems is important	48
	• Remove local admin rights	50
	• Privileged account monitoring and session logging	50
	• The importance of Zero-Standing Privilege	50
	• Foster a cybersecurity awareness culture	51
	• Multi-factor authentication should be implemented for all admin accounts	52
	• Automate your PAM strategy with a Privileged Access Management Tool	53
	• Do not rely solely on the PAM product	53

14.**Top Qualities of a Good PAM Solution _____ 54****15.****About Heimdal Privileged Access Management _____ 56**

- General data _____ **57**
- How does our PEDM tool work? _____ **58**
- What does the PAM module display? _____ **60**
- What Does Privileges & App Control - Privileged Access Management View Display? _____ **60**
- Case Study _____ **61**

16.**Conclusion _____ 65**

Introduction

Introduction

Privileged Access Management (PAM) solutions have started to gain ground since the 2000s, being like the guardian angel for admin credentials and a necessity on the cybersecurity market. In the initial phase, these were developed only for on-premises requirements. However, things have evolved and everyone's moving to the cloud, so these solutions should adapt their features to be able to protect a cloud infrastructure that is both more complex and more challenging.

Gartner says that the PAM market will meet an increasing interest in the following years:

“The market will continue to witness increased interest for the coming two to three years and the worldwide market, measuring buyer spending, is expected to reach \$2.7 billion by 2025. (...) The growth is mainly driven by the increasing awareness among security staff regarding criticality of PAM solutions. Several high-profile breaches have been linked to compromised privileged account credentials. Coupled with this, the accelerated migration to cloud, blurring enterprise security perimeters and the overall increase in the number of cyberattacks all contribute to the growth of PAM adoption.”

[Source: Gartner, 2021](#)

This e-book is a guide designed to better understand basic Privileged Access Management Concepts that will further underline the necessity of a privileged access management solution in today's corporate context.

We will:

- Explain privileged access and privileged access management definitions, through different types of privileged accounts.
- Emphasize aspects regarding PAM's importance and related concepts like PEDM and PASM.
- Define PAM challenges.
- Outline what makes a good PAM product and how can Heimdal™ help you.



About the Company

About the Company

Heimdal was founded in 2014 in Copenhagen, Denmark. When speaking of the European market, Heimdal proves itself a leading provider that offers efficient cloud-based cybersecurity solutions, as we all know that the present and the future lie in the cloud.

The enterprise promotes the concept of unified and user-friendly cybersecurity owning a diversified suite of products aligned with the current market requirements, from products supporting DNS filtering like [Threat Prevention](#) and endpoint protection like [Next-Gen Antivirus & MDM](#), to products that focus on automated privileged access management and application control to properly protect privileged accounts or to patch and asset management and email security products.

The most current demanding needs on the cybersecurity market are reflected in 3 directions: domain name system protection, a proper patch and asset management strategy, and an accurate privileged and access management approach and Heimdal has modern and automated solutions that will properly cover all these needs being focused on protecting critical business assets and keeping away emergent threats.

Over 45 countries benefit from the Heimdal's solutions, the enterprise being also ISAE 3000 certified, a fact that adds to its trustworthiness. Not to mention that over 10.000 businesses with their 2 million endpoints are well safeguarded by Heimdal's products.

The company is recognized in the cybersecurity industry, being awarded multiple times for the excellence it brings to the table.

The most recent prizes acknowledge that [Heimdal Threat Prevention](#) is the best DNS traffic filtering on the market to prevent future threats, being named:



**Cloud-Delivered Security
Solution of the Year**



**AI and Machine Learning-Based
Security Solution of the Year**

Last but not least, Heimdal believes in a strategic partnership and the continuous efforts put in a steadfast ecosystem, this mindset being aligned with its partners' goals.

Become a Heimdal Partner



Get in touch with us and learn more about the Heimdal unified suite.

 +44 330 808 9413

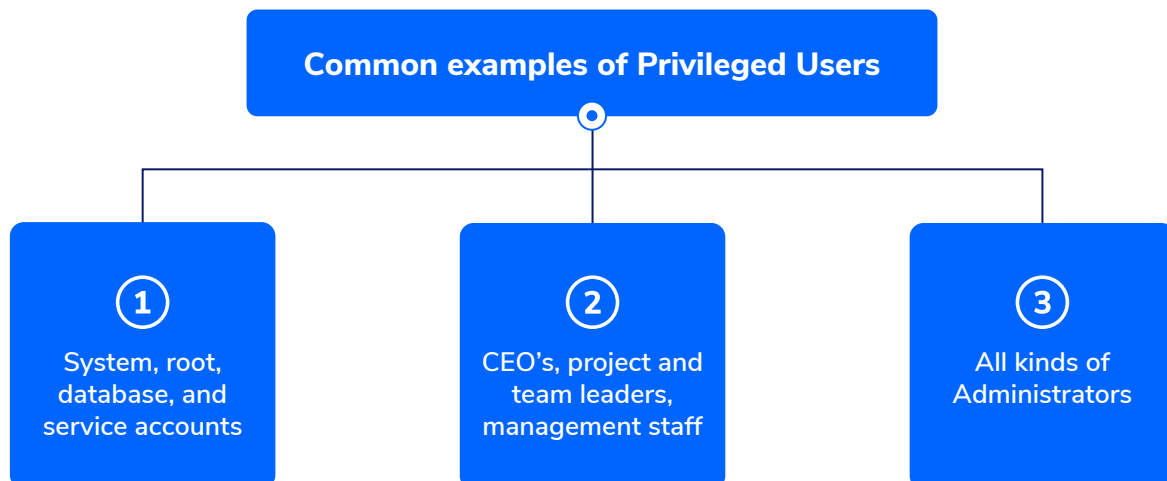
 sales.inquiries@heimdalsecurity.com

What Is Privileged Access?

What Is Privileged Access?

Privileged access refers to that type of elevated permission within an organization, either on-premises or in the cloud, that goes beyond standard user rights. Privileged accounts have access to critical business infrastructure and are essential for protecting the organization's critical assets and the sensitive data that come with them along with maintaining their confidentiality.

Privileged access is usually granted to an individual who is given the power to get access to restricted data or information in a company or to an application or system that needs to communicate with another system.



Privileged access facilitates the carrying out of many activities in a network or computing system that a normal user cannot do. Here we can give some examples: network or system configuration, cloud instances configuration, performing a system shut down, admin changes to apps, IT infrastructure and systems updates, and so on.

Privileged users could be people from inside an organization like system administrators, administrators of databases, web developers, architects, application owners, or even IT managers. However, privileged access can be also granted to outsourcing partners or external vendors that might have permission to access critical corporate data.

Misuse of privileged access results in security breaches, service outages, and a negative financial impact on the business.

What Is Privileged Access Management?

What Is Privileged Access Management?

We hope that we have shed some light upon this confusing concept of “privileged access”. Let's move then to the definition that counts. [What is Privileged Access Management?](#)

Privileged Access Management is an information security mechanism of practices, technologies, and strategies brought together to help enterprises define, monitor, manage and protect privileged accounts owned by users or different applications, systems and processes, and the data they have access to.

PAM works on two aspects: preventing the misuse of privileges and credentials theft. PAM offers a better overview on who or what has what rights within an organization, how those rights are used and how can these be efficiently managed and controlled for the proper functioning of a business, and the limitation of cyberattacks.

PAM protects an organization from insider threats as well as from external threats, limiting the attack surface and maintaining the sensitive data's integrity and confidentiality.

PAM is strictly correlated with [the principle of least privilege \(POLP\)](#), this being a PAM's integrative part. The principle of least privilege is a concept that promotes that users, applications, accounts, systems, devices, or computing processes are granted the minimum access level they need to certain resources (apps or systems) in order to complete a specific activity. So, nothing more. If a payroll employee needs access to the payroll database, he/she won't have access to the coding database where Web Devs store and work on their code models, let's say. As simple as that. Limiting user and app rights and elevating them when not necessary anymore will also limit the infiltration and propagation of malware. As the saying goes, less is more. Fewer rights, more protection for an organization!

Privileged Access Management Challenges

Privileged Access Management Challenges

In order to implement a proper privileged access management strategy, here are the PAM challenges you need to be aware of:



The missing granular insight and the challenge of a manual process

In today's corporate environments, thousands of policy and configuration settings and also tens of thousands of human identities as well as service identities facilitate access to various systems and services. When speaking of an on-premise context, privileged users can have permissions related to cloud storage, the configuration of the server, or the management of the firewall. When speaking of a cloud environment we can extend the elevated permissions to network configuration, buckets, or VMs.

Since everyone's moving to the cloud, this means thousands of virtual machines having elevated permissions and more superusers with rights like configuring, altering, and managing systems. What becomes difficult here is to manage so many privileged accounts in the cloud and this is also because identity access in the cloud is inherited, so if a user, application, or service has access to some identities, they will inherit the identities' permissions.

Such complex systems or networks are hard to manage without granular insight and impossible to handle manually which becomes a challenge for today's PAM. That is why an automated Privileged Access Management tool that covers both aspects becomes essential in terms of scalability.

Here we can also mention the challenge that comes with manually updating and rotating privileged account credentials. Credential management should not be approached in a manual manner, but an automated tool should be used instead, so human error would not cause any damage.



The risk posed by privilege excess

Users accumulate too many rights within the network and this happens particularly when they have new roles within the company and/ or when they leave their job. Privileged access should be always revised and curated because it can only lead to the expansion of the attack surface when not properly taken care of.

This process of users and identities' gradual accumulation of privileges and rights that are not necessary and are beyond their task requirements is called privilege creep. It usually emerges as users always need access to certain data, the network, or applications, this way there's a lack of proper account review and authorization for this type of access. As we have mentioned earlier, privilege creep is a consequence of users having new job roles and not having their past permissions revoked, thus facilitating both insider threats as employees might misuse privileges or external threats when a hacker takes over an account and performs malicious actions.



Shadow privilege risk

IT providers or system administrators tend often to help end-users with their technical issues by granting them local admin rights or even elevated permissions at the domain level. This is, of course, a bad practice, because it makes you lose control over what happens and this practice is popular and known as an organization shadow privilege access.



Default credentials and those stored in unencrypted files

Application to Database (A2D) or Application to Application (A2A) access is usually provided through privileged credentials. Where the problem lies when speaking of privileged credentials is in the fact that network drivers, hardware systems, applications, or [IoT devices](#) normally come with predefined credentials called default credentials. These, of course, are not complex and a hacker can guess them easily. These are usually stored in plain text within files that are not encrypted for ease of use. However, in terms of security, this is a bad practice that only makes the hacker's path easier.



Privileged sessions are not managed from a central location

Centralization is the key. Many enterprises fail to properly manage privileged sessions from a central location, so basically from a single platform. This might in the end bring out security breaches.



The PAM tool interface is complicated

A basic PAM tool is not enough to simplify the life of IT administrators, it should be characterized by a user-friendly interface that will let them effortlessly grant access, revoke access or create users, embodying the essential balance between its safety and its interface that keeps everything simple and makes for a smooth approval/denial flow.



Companies fail to meet audit requirements

Since companies do not have proper strategies and proper tools to manage and control privileged accounts, they fail to meet audit requirements. Privileged sessions should be logged not only for audit purposes but also for further internal reviews that will help the organization see where the problem lied.

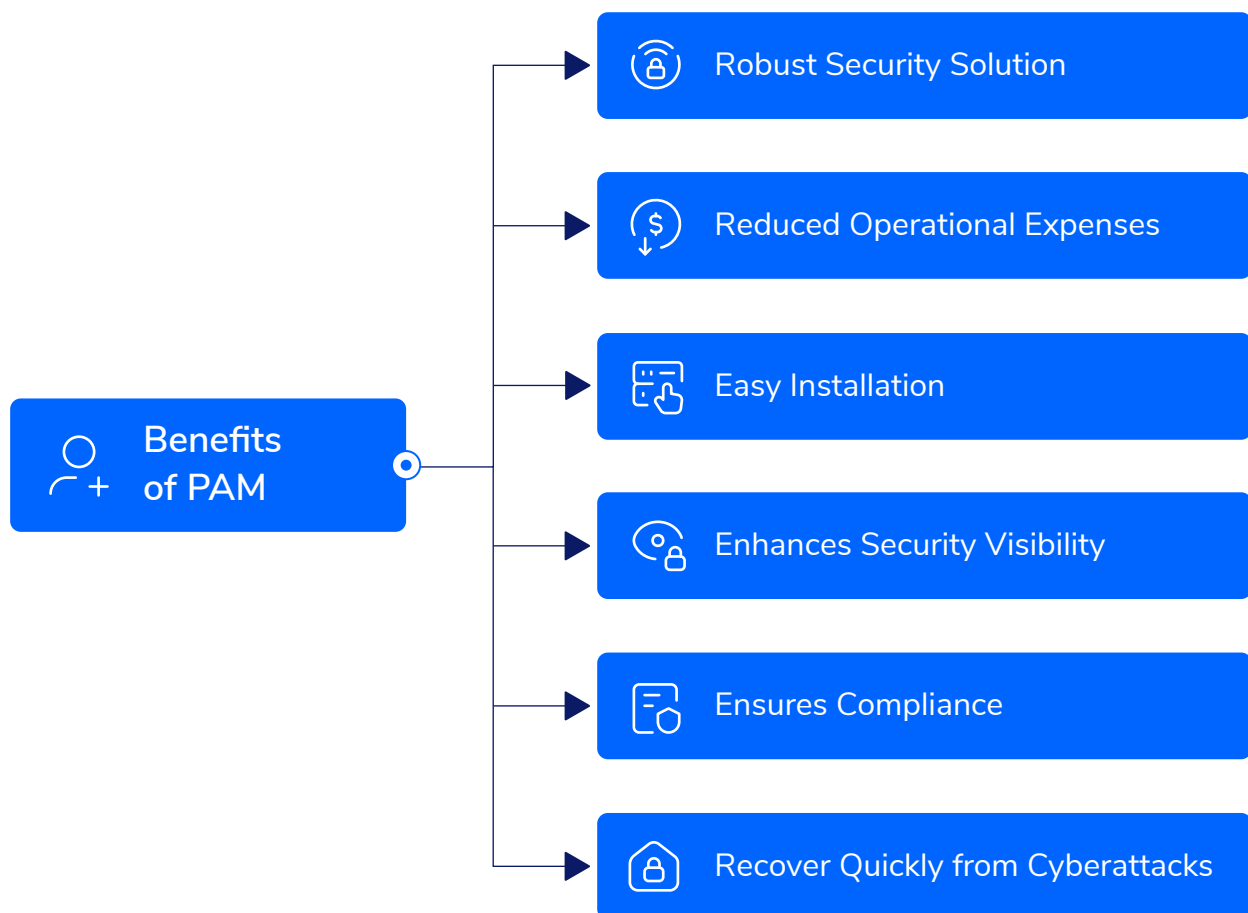
This challenge can be easily solved with an automated PAM tool that has the ability to track privileged access, generate and save audit logs and provide accurate and comprehensive reports.

This way, reputational damage, and fines are avoided through a clear audit trail.

As we've shown you what are the PAM challenges today's companies have to cope with, stressing on the cause and effect, now the following topic comes naturally, emphasizing the necessity of a solution: why is privileged access management important?

Why Is Privileged Access Management Important?

Why Is Privileged Access Management Important?



The core aspect of why privileged access management is important is that it protects privileged accounts, thus safeguarding the organization's sensitive data these accounts have access to.

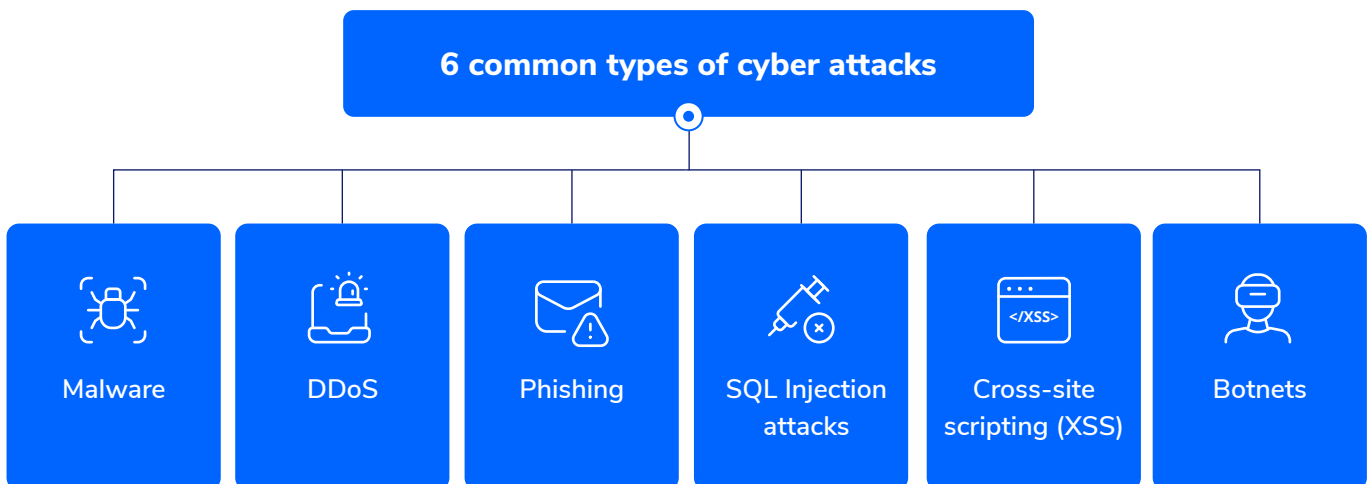
In the following lines, we will itemize some reasons for which Privileged Access Management counts.

1. It prevents cyberattacks

The most obvious reason why PAM is important is of course, that it works on cyberattacks prevention, limiting and mitigating two most encountered cybersecurity threats: both insider and external threats.

[Insider threats](#) because a user can abuse the already owned privileges and external threats because hackers are blocked to gain access to an account with privileged permissions.

Further extending this, PAM protects against incidents that may involve security breaches or sensitive [data leakage](#). Hackers crave privileged accounts to bring down an organization's infrastructure.



Cybercriminals have switched their focus from targeting standard user accounts to targeting privileged accounts. Why? Because those accounts within a company with special permissions have access to sensitive data, so basically to the core organization's infrastructure.

These are the key to bringing down a network infrastructure, infiltrating [ransomware](#), or other types of malware. Privileged account compromise means that vital data is compromised, so it falls in the wrong hands.

2. It properly manages, protects and provides a good overview over privileged accounts

With so many privileged users and accounts out there, it's hard to have the proper visibility over them, many special accounts can be overlooked in the long run or former employees have been left with their previous accesses in a company. To manage this, a good PAM strategy along with an automated PAM tool is required.

Besides, during their journey in a company, employees can be promoted and have new roles and these will always add up to other previous privileges like a snowball, leading to privilege excess. Also, many IT admins share the same accounts for comfort purposes, so personal accountability for shared accounts through a PAM strategy will help better manage the privileged access in the long run.

Today's organizations have more and more processes, systems, and applications that communicate with each other to work in synergy.

With this shift to the combination between on-premises, cloud, and hybrid environments, of course, that the number of apps and services is bigger even than the employees' number, that meaning more privileged accounts. That's why a PAM strategy is vital, otherwise, how can all those privileges be monitored, controlled, and thus protected? Privilege access stands at the core of proper business management.

Not to mention that in the cloud, entire servers can be stored and users with privileged rights have the power to make various changes, that's why PAM is needed to keep track of privileged accounts and protect them properly.

3. It supports productivity

Privileged Access Management promotes and supports increased productivity of system administrators and systems. Firstly, PAM tools reduce the risk posed by human error when keeping track and controlling all the privileged accounts in a company.

If in the past tasks such as password creation or password vaulting were completed manually, implying of course human error and a lot of time from the admins' side, nowadays this process is automated in a PAM tool for better accuracy. This is a win-win situation. Employees do not waste valuable time with a password and access managing, IT administrators do not waste time correcting issues in the system.

Productivity is also supported by the fact that privileged access is managed from a central location and users have a digital identity of their own, so no need for multiple credentials management.

Productivity can also be challenging in the context of moving to hybrid work. PAM ensures that even if users log in from various locations and devices, there won't be access issues. This all means that supporting productivity, the risk of a business outage is mitigated and the overall operational performance is improved.

The approval/denial flow a PAM tool offers will also support reducing the IT workload, making the process of granting and revoking privileges automated, so easier.

4. It supports compliance providing a clear-audit trail

If you have a PAM strategy along with an automated PAM tool with the help of which you can live monitor and record details about your privileged accounts and privileged sessions, this will allow you to meet compliance requirements providing a crystal-clear audit trail and report.

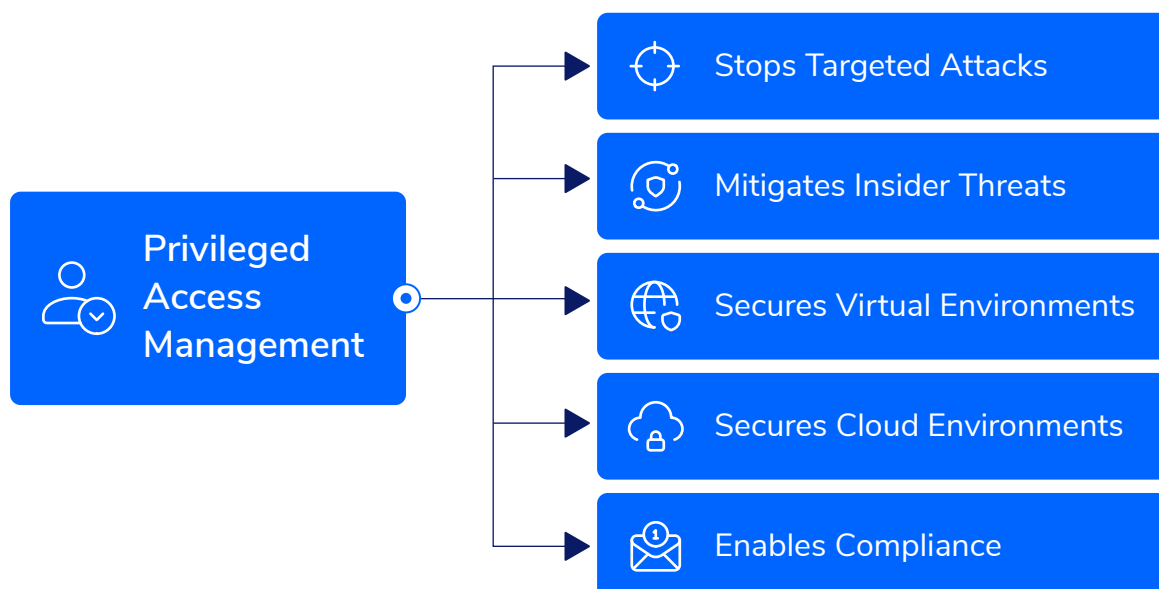
Reports are not only useful to show the auditors you're on the right path, it also helps you review what went wrong in your company in case of an incident and who is responsible.

Facilitating the path to an audit-friendly environment means that it will be easier to present audit reports regarding your critical data and what happened to them when required.

To give some examples here, a PAM tool will help organizations prove compliance with authorities like NIST, SANS, GDPR, HIPAA, Sarbanes-Oxley (SOX) section 404, FERN/NERC, or even with the PCI-DSS (Payment Card Industry Data Security Standard) policy.

5. It prevents lateral movement across the network

If hackers manage to get access to a privileged account, this means that they will also be able to further access other systems and facilitate malware propagation. Here comes also the principle of least privilege into play. If an administrator is given a limited amount of rights access, this will stop [lateral movement](#) across a network since the only damage that can be done will be to a limited number of resources.



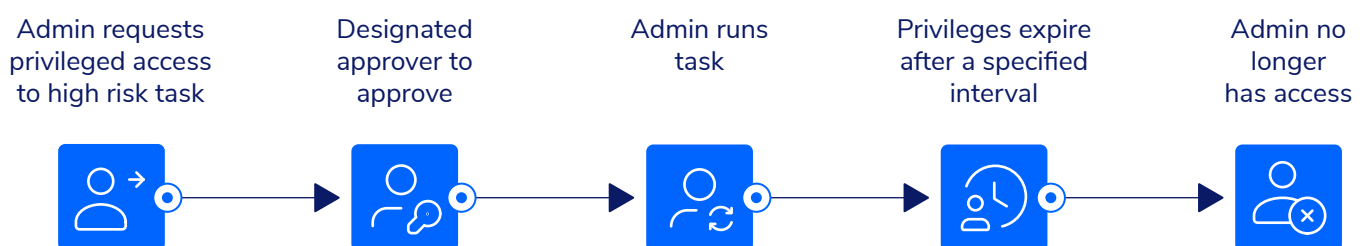
How Does Privileged Access Management Work?

How Does Privileged Access Management Work?

You might want to know how such a strategy works. Well, it all begins with a privilege risk assessment, so basically make an inventory of all the privileged accounts within your company to know what you are dealing with.

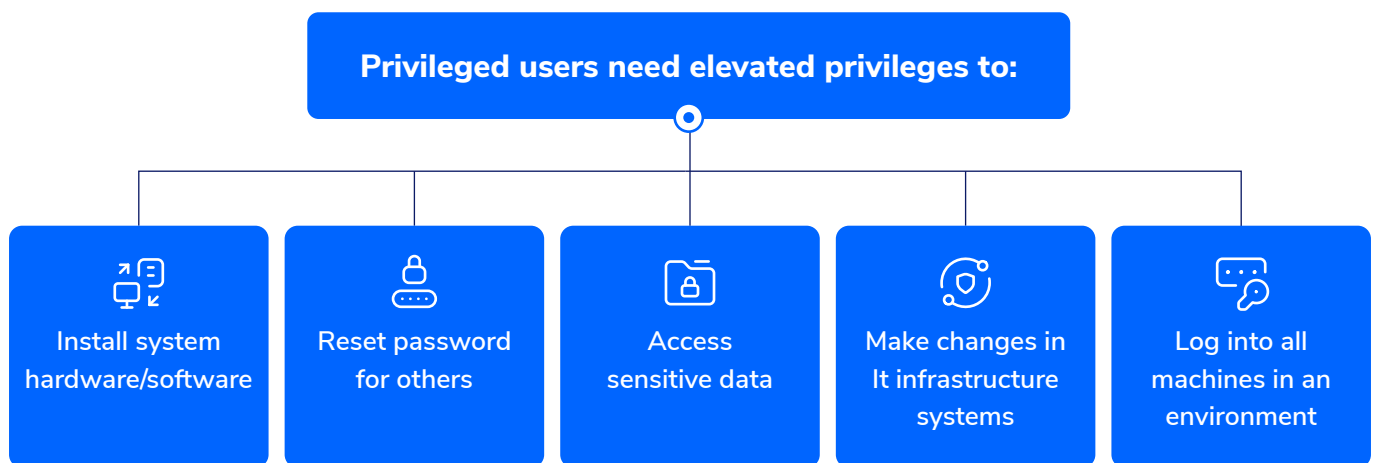
What follows next is to know which ones are the most prone to be exploited and establish what rules you want to apply for these kinds of accounts, meaning what they can do and they cannot and how they can do it.

This means that you need to put in place a PAM policy. Now comes that part when you know what privileged accounts are in your company and you set up some rules through a policy, it's time to monitor and audit them in order to keep them well safeguarded. This means using an automated PAM solution that will help properly monitor, control, and audit privileged access accounts through a centralized interface.



Privileged Accounts Types

Privileged Accounts Types



Privileged accounts are generally referred to as the Keys to the IT Kingdom because through them one can have access to critical data of an organization and make different changes. There are two broad categories which privileged accounts can be split into: those accounts with elevated rights used by human being entities and those accounts with special rights used by non-human being entities like apps or services. Shortly, we're going to talk about privileged user accounts and privileged service accounts.

Privileged User Accounts

The first category, privileged user accounts can be divided into several categories. These are:

- **The superuser accounts**

The [superuser accounts](#) are privileged accounts used normally by IT admins for different sets of activities. Some examples here could be users' removal or addition, they can use this kind of privilege to perform app or system configurations or they can execute different commands

within the system as they consider, they can perform software and files installation or creation, settings and files modifications or have access to parts of the operating system that are restricted to anyone else. It's worth mentioning here that, when speaking of a Windows environment, these superuser accounts are also met under the name of "administrator" and in a Linux/Unix environment they are called "root".

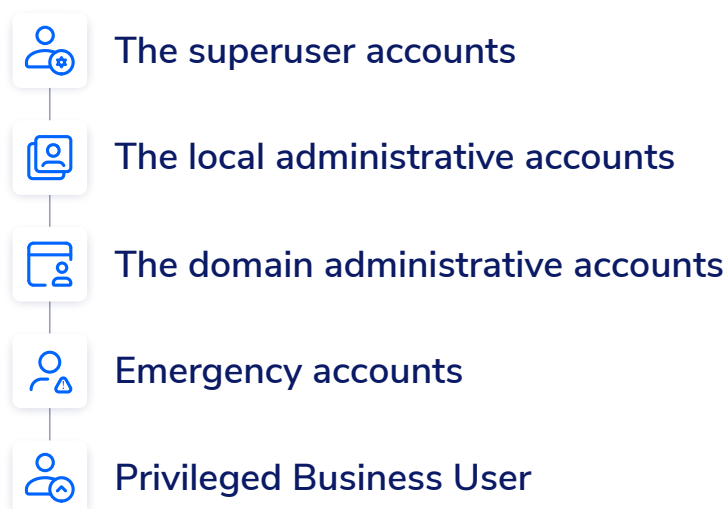
- **The local administrative accounts**

The IT Team normally uses this type of accounts for maintenance purposes on workstations, servers, network devices, servers' mainframes, etc. These pose a risk because sometimes the password is reused, shared passwords endangering an organization's security and letting free path for malware.

Local administrative accounts include any account that belongs to the local admin group on any computer and is useful for different changes to local devices or local machines like software installation or employing various changes to a device operating system. This is limited in terms of the nature of elevated access, as this type of special access is provided only to the local host.

This is dangerous if the privileged user falls into the trap of a phishing attack, meaning that a malicious actor would have the possibility to perform system settings changes and malware deployment, facilitating the creation of a network foothold.

Privileged User Accounts



- **The domain administrative accounts**

As the name suggests, the domain administrative accounts are those types of privileged accounts through which users can have special access to all servers and to all workstations that belong to a network domain. Thus, all domain controllers are under these privileged users' control as they can change admin account membership and these are also known as accounts with god-mode privileges.

These however can build a path for lateral movement across a network. If threat actors manage to compromise domain admin accounts this will enable the creation of user accounts that have escalated privileges posing as valid users, so no doubt hackers can move laterally across the network and nothing seems suspicious, because they pass unnoticed.

- **Emergency accounts**

When there's an emergency, the emergency accounts come into play. They can be also found under other names like break glass accounts or firecall accounts. These can be used for system safety purposes giving admin access to users, of course with the IT management's approval. So basically, accounts intended for unprivileged users that become admins in the case of an emergency. The process is usually manual and this triggers security risks.

- **Privileged business users**

Privileged business users are those accounts that show that not only IT sysadmins could have special rights. For instance, if someone, who is not related to the IT domain, needs access to sensitive information or databases from departments like marketing, HR, finance, and so on, they can benefit from this access through privileged business user accounts and can modify the data stored there.

A good example of a privileged business user could be an accounting employee who needs this kind of access when it's time to pay a vendor. As we have explained now how many types of privileged user accounts can fall under this category, we'll move on to privileged services accounts, the second category, so basically permissions used by applications and services which are non-human entities.

Privileged Service Accounts



- **Application accounts**

Application accounts are related to the application software and they are particularly useful for the administration and configuration of an app software access. What can applications do with these kinds of rights? They have access to different databases, they can also grant access to other apps, or they can perform batch jobs and scripts running. The passwords related to these accounts are as a rule kept in unencrypted plain text files (the credentials we've mentioned earlier in the chapter presenting PAM challenges), a factor that makes these accounts vulnerable to [APTs \(Advanced Persistent Threats\)](#).

- **Service accounts**

Service accounts can be used either by applications or by certain services to communicate with the operating system. Through these accounts, operating systems can be accessed and modified.

- **Active directory or domain service accounts**

Through this type of accounts interactions with the operating system can also be performed. An Active Directory service account enables management of computers and users, and performing actions like data organization or password modification.

- **Secrets**

However funny the name, secrets are very common among web developers and operation teams. They often use this term to refer to SSH keys or API keys. These types of accounts are useful to establish the connection to servers that engage in code running.

Secrets also stand for the authentication method when web services try to establish a connection with other systems. So, they are basically privileged credentials.

Now, we want to mention a type of account that can be a privileged user account but also a privileged service account.

- **SSH keys**

Through SSH Keys or expanding the acronym, Secure Socket Shell accounts, root access to critical systems can be provided. You should understand here what is a root and what are exactly SSH keys. Simply put, SSH keys can be understood as access control protocols and roots are basically those types of accounts with default access to files or commands and are related to operating systems like Linux or other Unix-based ones. Encryption keys could be a good example of SSH keys.

In this sense, this type of account can be used by administrators to perform single sign-on implementation and also by automated processes. The last use SSH keys for activities like routers, switches, or firewalls access.

Privileged Attack Vectors

Privileged Attack Vectors

In “Privileged Attack Vectors”, Morey J. Haber mentions six stages of insider attacks - which are similar to external threats.

Infiltration – insider and external threats

Various attack vectors like internal access can facilitate the path of infiltration, that meaning that external threats are not the only ones one should focus on. External threat actors focus on obtaining access to privileged accounts and credentials of course.

The initial foothold is most of the time achieved through a low level-exploit. A low-level exploit can mean a standard user account or even a phishing attack and then through lateral movement, they reach an account with privileges. On the other hand, insiders already know what they are dealing with, having a good knowledge of the perimeter, for instance, they know where to find the important data and assets.

Command and Control

Intruders and cybercriminals can create communication with a C&C server in order to gain access to toolkits or payloads that will let them prepare for the next phases of attack.

Privileged escalation attempts

In privilege escalation attempts, hackers examine your network, identify the most important assets and privileged accounts and search methods to gather several passwords, and take advantage of the already abused user rights.

Lateral movement between assets, accounts, resources, and identities

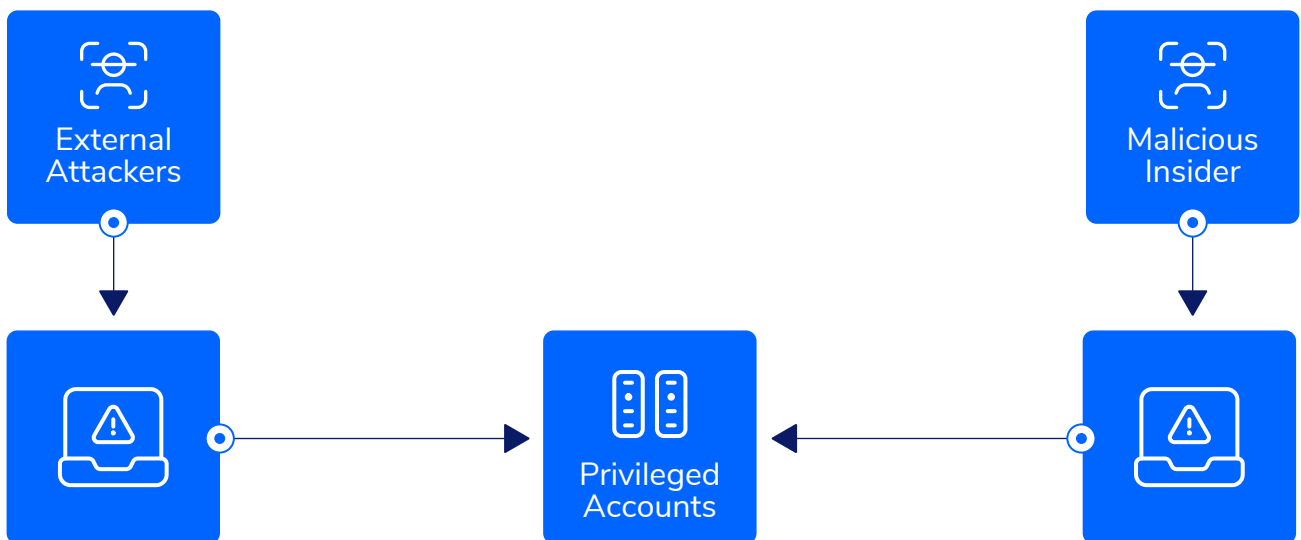
After they infiltrate, their malicious actions do not stop there. Through lateral movement, hackers basically move across the network in their attempt, and sometimes they successfully complete the mission of infecting other assets and accounts.

Searching for extra opportunities

Anonymity, as you may already think, is the keyword when speaking of the hackers' purpose. If threat actors remain undetected, they can broaden their attack surface from vulnerabilities to compromised identities and they can do this through several means like various attack vectors identification, malware installation, or the discovery of new targets.

Data exfiltration or destruction

Eventually the threat agent performs activities (such as data collection, data storage, or data exfiltration) causing the system to be infected with malware which is, most often, ransomware. These types of attacks could be caused by internal or external threats. Not to mention that an insider threat facilitates usually faster malware propagation and security controls bypassing.



Privileged Access Management Related Concepts

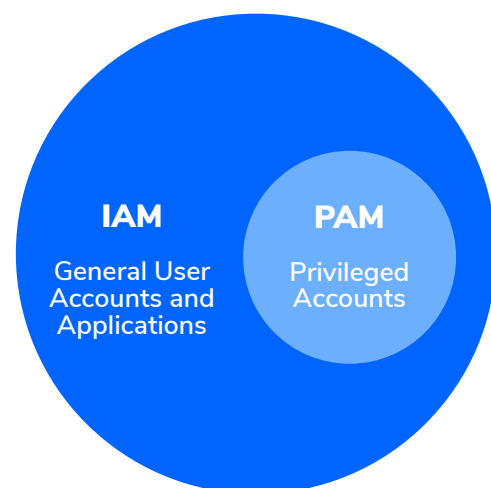
Privileged Access Management Related Concepts

We have previously mentioned Privileged Access Management concepts like the principle of least privilege or privilege escalation. Now, we want to underline other concepts related to PAM that you need to know.

1. IAM vs. PAM

PAM and IAM are both acronyms for the two concepts: Privileged Access Management and [Identity Access Management](#). PAM is a subcategory of Identity Access Management, the broad domain that does not focus solely on the management of accounts with elevated permissions, but on the management of all user accounts, making sure these have the necessary permissions when they need it. To understand the difference, we can consider PAM as being characterized by a much granular aspect.

Another difference between IAM and PAM is that the first intends to operate over larger attack surfaces, while the second is focused on smaller areas, on that part of a system with high privileges. PAM is intentionally designed to cover a restricted area, while IAM is a broader category.



As we said, IAM focuses on all user accounts, not only on privileged ones, from internal employees' accounts to external customers, partners, and vendors. IAM should be integrated with PAM because one of the Identity Access Management benefits could be the fact that this helps organizations terminate a privileged account when an employee leaves the company for instance. To further illustrate the difference between IAM and PAM and to emphasize the restrictive characteristic of PAM, we will give an example.

In identity access management, the OAuth (Open Authorization) standard is used. Through this, access to a third-party mobile app is authorized by a corporate application: a mobile user can use this OAuth standard to see a stock trading account balance that belongs to another entity. Privileged Access Management, on the other side, would not use standards related to third-party authorization.

2. PASM and PEDM

The Gartner's Magic Quadrant defines two different PAM mechanisms: PASM and PEDM. These two types of combination of letters represent the acronyms for Privileged Account and Session Management and respectively, [Privilege Elevation and Delegation Management](#). We will elaborate on each of them in the following lines.

PASM aka Privileged Account and Session Management, sometimes also referred to as password vaulting, is a security mechanism that has the role of privileged credentials creation and distribution in a secure way. In order to access a server, users have to request this type of access from the vault. What happens next is that a temporary account with privileged permissions is created for them. It's worth mentioning that this account will be valid for one single session and that the privileged session will be both monitored and recorded.

In PASM, privileged account credentials like passwords or SSH Keys or AWS IAM credentials, API Keys, and also IP addresses, which are basically generic secrets, can be stored and monitored.

For instance, actively managing privileged account credentials might mean changing them at certain intervals or depending on the context. This vault ensures that people have access to specific resources and also encompasses capabilities like brokered login or password checkout.

PEDM stands for Privilege Elevation and Delegation Management, which is a type of Privileged Access Management (PAM) that focuses on delivering more granular access controls than Privileged Account and Session Management (PASM) technologies normally do. Our PAM tool does exactly that, focusing on the so called "PEDM" component.

PEDM helps to mitigate the dangers created by overprivileged users by giving more explicit restrictions. PEDM lets businesses to strengthen their cyber security posture by assigning admin permissions to certain tasks, programs, or scripts on a case-by-case basis.

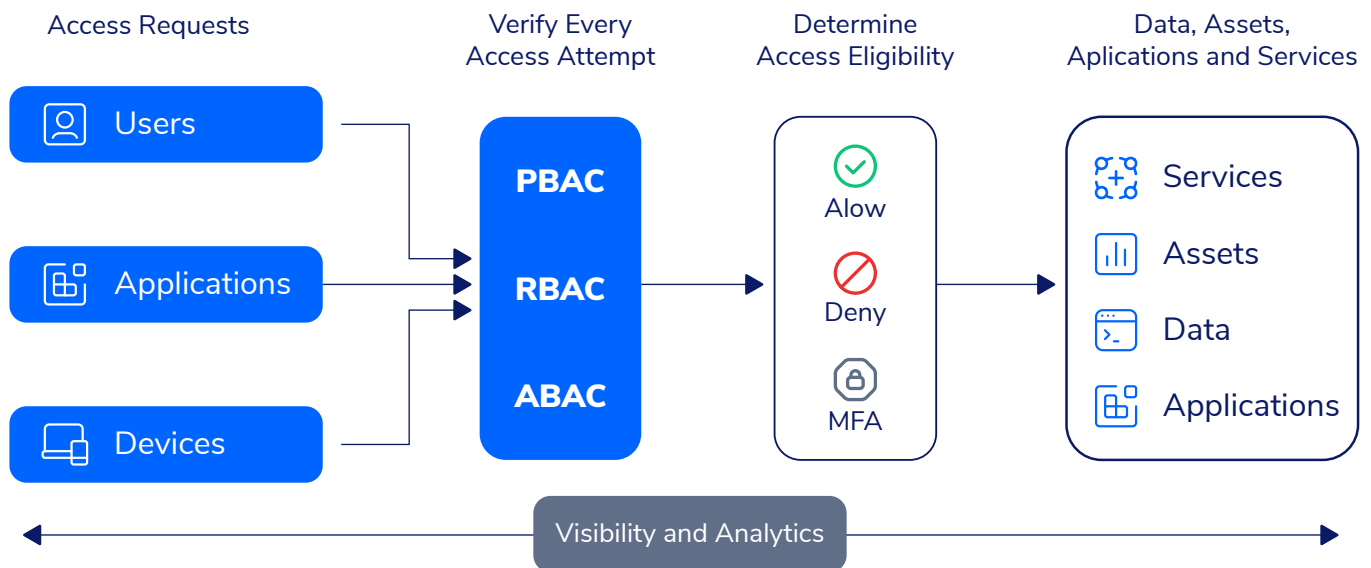
3. The Zero-Trust Model

The Zero-Trust Model becomes an essential security model that all cybersecurity strategies should encompass. The concept behind is quite simple: nothing should be trusted by default, nor people, nor devices that establish a connection to the corporate network, even after the verification was performed. This is specifically useful to prevent insider threats and their propagation across the network to further disrupt a business.

Now you might want to know what's the relation of this concept with privileged access management. Well, the zero-trust model follows a simple, but an efficient protocol that says to always verify and never trust, even users already within the corporate network. For a long time, an illusional concept of trustworthiness has been fostered when speaking of users that already have access within a network, so if they are already in, that would mean that they should be trusted. Well, it's not like that. Using the Zero-Trust model integrated with PAM means that the requirements will define from the beginning that every access request is invalid and whenever there is such a request that requires elevated access it will be first checked before granted.

This is particularly useful to mitigate lateral movement across the network. Let's say a hacker would exploit an account with privileged permissions and gain access to it going undetected. The hacker could use these credentials and remain on the network for months without anyone noticing. With zero trust implemented and correlating this with the already established policies, every access and every device will be verified at each access request.

You should not buy one PAM tool and then a different Zero-Trust tool for this kind of protection. Why? Because of the fact that this concept has started to gain ground, many PAM tools implement the zero-trust model as a feature of their already existing interface. We, at Heimdal, also have recently added to our PAM module the Zero-Trust capability.



Traditional PAM vs. Modern PAM

Traditional PAM vs. Modern PAM

Traditional PAM was based on two things: a complex pattern of password vault and PSM systems (privileged session manager) being not very efficient as it hindered everyone's work. However, the modern PAM is based on the principle of least privilege, where users have the minimum level of access to do their job, thus limiting both insider and external threats.

The process in a traditional solution follows these steps: users want to complete a specific task, but for this, they need special permission. They will ask for this access, providing also a reason for their need. The PAM solution will automatically approve the request based on a policy or it can be sent to a manager for instance for manual approval in other specific cases. Once the approval is on, the decision will be logged by the PAM and then the user who requested permission will have temporary access to that specific task. Normally, this granting of permission is done through the PAM, so users do not have knowledge of the privileged account password.

Old PAMs use password vaults for credentials storing. Now, the new trend in PAM solutions is represented by privilege on-demand featuring the zero-standing privilege. What does this mean? That the time of privileged access is limited for administrator and the time amount is also restricted. That means that admins have only the access and the time they need to finalize a task and that's it. Following the completion of the task, there are two possibilities: the privileges are revoked or the account is deleted.

The two main challenges with traditional PAM are that it is complex, so the configuration, the ongoing maintenance, or the rollout take many hours to implement, and its focus relies only on controlling the privileged access. On the other hand, a modern PAM should also be able to implement the zero-standing privilege in order to fight against the expansion of the attack surface like lateral movement, the privilege on-demand concept working both on supporting the company's cybersecurity and also its efficiency.

Privileged Access Management Myths

Privileged Access Management Myths

Privileged access management is an important topic that should not be underestimated. Many myths that surround this topic flourish every day. We will look at the most common ones and try to debunk them.

Myth 1: A privileged user can't be tricked into giving up their credentials.

It is possible for a user to be tricked into divulging their credentials or other sensitive information by an attacker. They can also be tricked into giving up their log-in information through phishing attacks or [social engineering methods](#).

Myth 2: Privileged users would have to use [two-factor authentication](#) every time they log in.

There are too many instances where this would just slow things down, so two-step verification only needs to be used when it is necessary for security reasons, such as logging into a high-risk account.

Myth 3: PAM is the answer to all cybersecurity issues.

Well, if only it was that easy, you wouldn't see so many cyberattacks emerging every day. A PAM strategy paired with an automated PAM solution is just a part of what a multilayered cybersecurity suite must include. Companies also need a [Patch & Asset Management Tool](#) for instance to keep their software updated regularly, blocking thus hackers from exploiting vulnerabilities in the programs, a DNS traffic filtering that will stop threats at the domain level, and an E-Mail security suite that will keep away [supply chain attacks](#), [CEO fraud](#), [Business Email Compromise \(BEC\)](#) or everything SPAM, or even a [Ransomware Encryption Protection Tool](#) that will make sure that ransomware gangs will not encrypt or, even worse, exfiltrate your critical corporate data.

Privileged Access Management Best Practices

Privileged Access Management Best Practices

To efficiently implement a privileged access management strategy, you should follow a set of basic PAM best practices.

1. Make an inventory of all your privileged user accounts within the company

The most important PAM best practice is to start with a privileged accounts inventory. See what privileged accounts you have within your company, what's their number, what is still active, and what is not. Maybe some employees left the company but their privileged rights had not been revoked, maybe some were given higher positions but still have redundant privileges.

So, clean it up!

2. Perform a risk assessment

Another best practice is to focus on prioritization. Now that you've established and known how many privileged accounts are in your company, you need to know what should be prioritized, so basically what's the most at risk and needs immediate enhanced protection.

3. Separation of duties and segmentation of systems is important

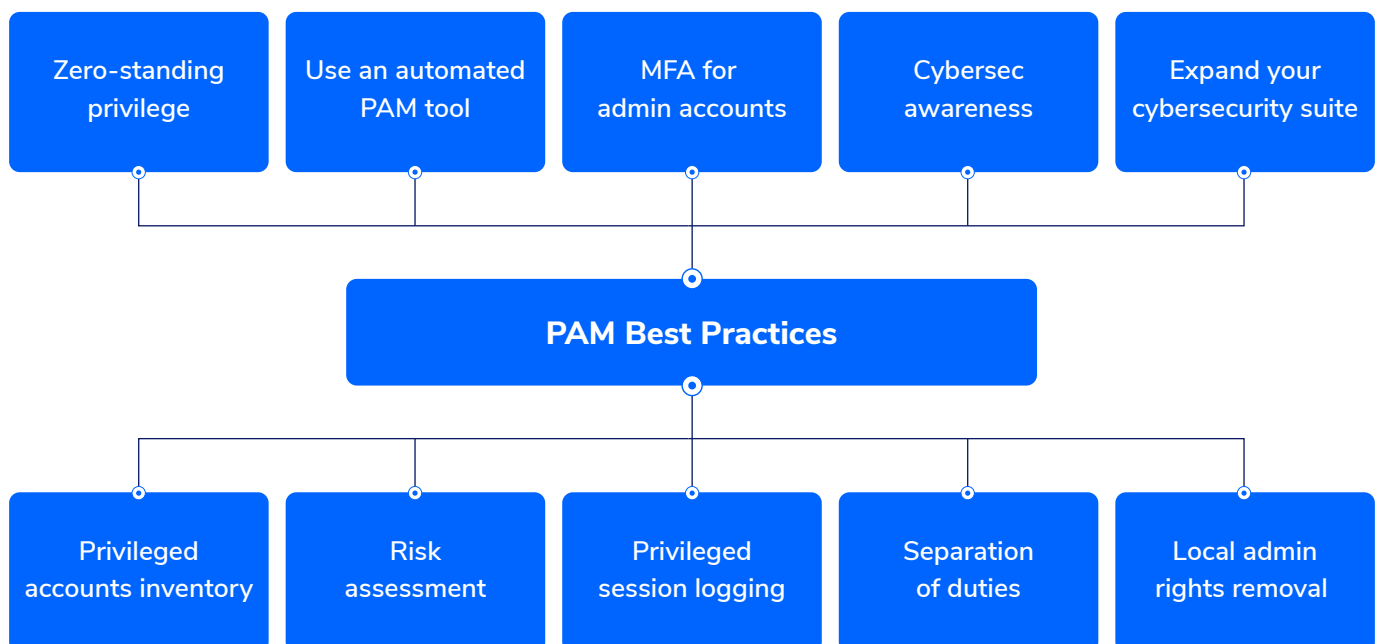
When you create a privileged account management policy, there are two practices that will surely fit right in: separation of duties and system segmentation. Separation of duties and privileges means that depending on the current roles users own, a digital identity will be implemented for each of them, thus separating their privileges based on job roles.

For instance, an account with admin privileges will be separated from an account with privileges regarding the system's functionality. The privilege to audit sessions is yet another example of an account that should be separated from the rest.

Once this separation of duties was put in place, each account could be given the specific tasks they will need to complete. Another thing to mention here is that personal accounts should be separated from admin accounts.

You use a personal account to check some e-mails or to browse the internet, you don't need a privileged account for that and it would be a bad practice if you'd use one in this sense. That's why it is recommended that admins have two accounts: one that is personal for routine tasks, and one with privileged permissions.

Thus, segmentation should be implemented both for users and processes taking into account the role, trust, and permission. This is a good practice in terms of scalability as it provides a way to create a flexible policy on privileges and make security controls based on segments, as it's a bit hard for an enterprise to keep all the assets and systems in just one pool.



4. Remove local admin rights

[Removing local admin rights](#) is a bare minimum to keep the cybersecurity strategy well put in place. This means that you can make admin rights a default setting for your organization. Basically, through admin rights removal you will block any malware strain right from the beginning and this also helps with preventing both insider and external threats and prevents hackers to exploit vulnerabilities in the system.

In our PAM solution, we have the option of removing local admin rights. You should simply log to the Heimdal dashboard, then select Endpoint Settings, then choose and click the policy you want to update, and then you should simply select the PAM tab and check the Revoke local admin rights box.

This box, once checked, will make sure that all admin rights are automatically deescalated on all machines.

5. Privileged account monitoring and session logging

You should continuously monitor privileged accounts and record every session but for compliance and also for review purposes. However, this is impossible to be done manually with reports written in spreadsheets because you lose track of the information on the way, that is why an automated PAM tool will both make the approval/denial flow smooth and the privileged accounts monitoring accurate and easy.

6. The importance of the Zero-Standing Privilege

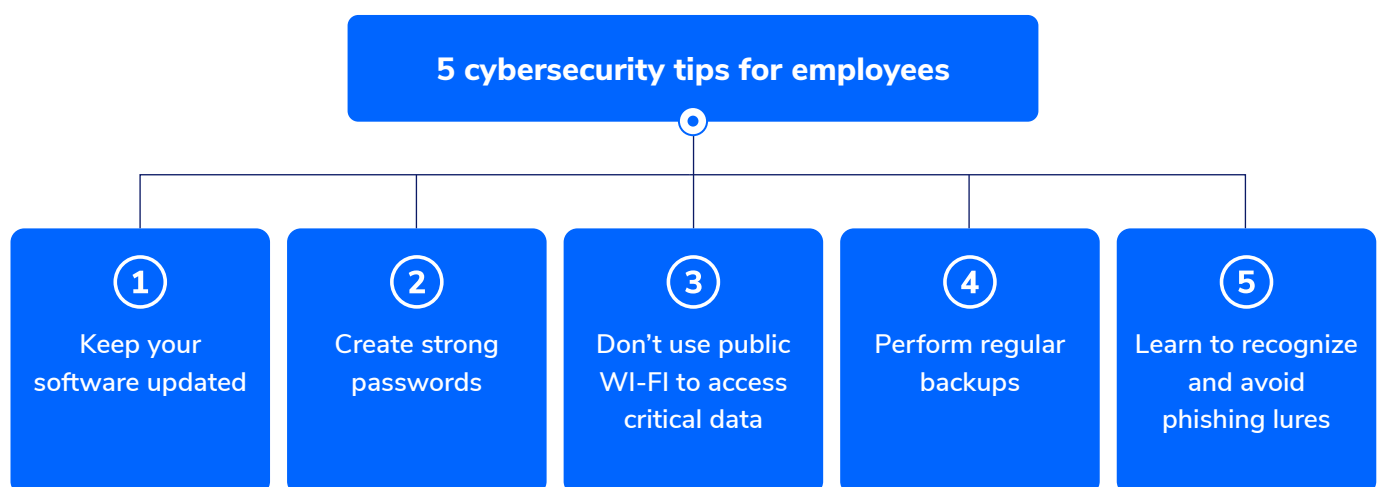
The Zero-Standing privilege concept is a practice that more and more organizations start to implement, as eliminating standing privileges within a corporate context becomes an essential measure to fight against the risk of data breaches, meet compliance, avoid credentials being stolen, and also prevent the abuse of privileged permissions.

Standing privilege means that accounts have permanent privileged access and zero-standing promotes quite the opposite, implementing the just-in-time (JIT) capability to provide elevated access only when needed and for a limited period of time. This concept promotes the idea of the principle of least privilege we have talked about at the beginning of this paper. It is proven that an account with zero standing privileges will pose a lower risk to the organizations' critical assets than an account with standing privileges.

7. Foster a cybersecurity awareness culture

When talking about employees' education, cybersecurity awareness comes first and all employees need to be aware and understand that they also play a significant part in protecting the critical assets of an organization. This way, they can learn how to recognize and avoid a phishing email, so fewer chances to click on a malicious link and provide private details to a third party or download a dubious attachment that will launch a ransomware payload.

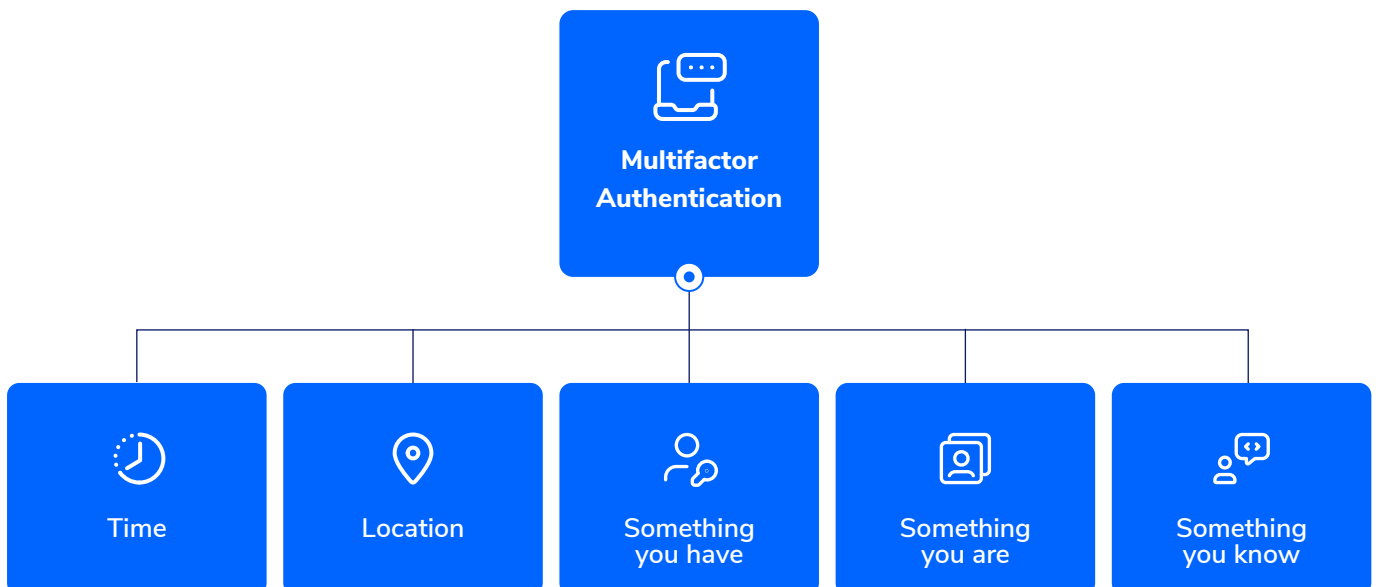
One method to make sure your employees stay safe and sound is to have regular role-based pieces of training for them both for technical and non-technical staff. Of course, more in-depth knowledge like data or elevated permissions management is the IT department's problem, however, even the rest of the employees should not consider themselves outsiders. Everyone is a piece of the puzzle that can be assembled to prevent security breach risks.



8. Multi-factor authentication should be implemented for all admin accounts

Multi-factor authentication (MFA) should be implemented for all admin accounts: be them domain admin accounts, Active Directory admin accounts, and so on. But keep in mind to choose and adopt an MFA that will not make your IT admins frustrated as this slows them down.

That's why, when setting up an MFA you must ensure this can be easily adapted to your IT infrastructure, so it can be deployed without being necessary to go to every workstation and without requiring complex customized code, the easy deployment also means that it does not require additional software or hardware and it can be managed effortlessly as admins would not be prevented to have a quick reaction to end-users issues. Besides, it should support your organization's scalability.



However, it's a misconception that MFA should be implemented only for privileged users, as any user who has access to critical data, like a payroll database account let's say should benefit from this kind of protection. Take for instance the emergency privileged accounts we've talked about in a previous chapter.

9. Automate your PAM strategy with a Privileged Access Management Tool

A PAM tool will make sysadmins life easier because it provides a user-friendly interface, allows the management of all privileged accounts from one location, smoothes the denial/approval flow, supports the JIT (just in time) concept by offering a limited session duration, logs privileged session and facilitates accurate reports and data compliance achievement.

10. Do not rely solely on the PAM product

A PAM solution won't be enough. As we have underlined in the chapter "PAM Myths", there is an illusion that if you have PAM in place, everything is protected. Well, it's not really like that. PAM protects only a part of an organization's infrastructure.

As we mentioned before, solutions like a SPAM filter, a DNS filter, a good Antivirus for endpoint protection, or a Patch Management tool will make the picture look complete.

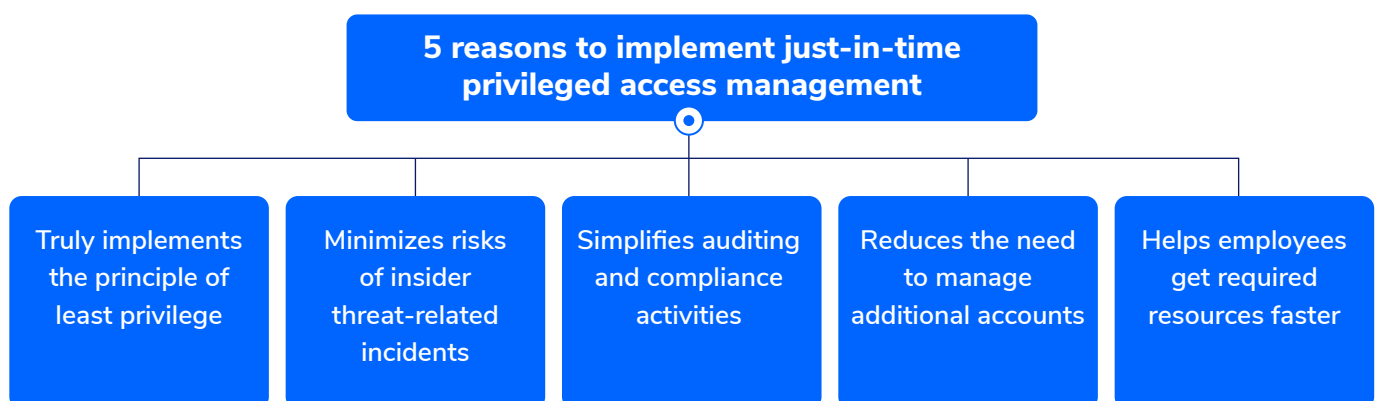
However, what we want to underline here is how our PAM works with our NGAV, as when the last detects a threat, PAM automatically deescalates privileged rights during a session. This happens only if used with our antivirus, not with any other antivirus, and this is one of the main characteristics of why our solution stands out.

Top Qualities of a Good PAM Solution

Top Qualities of a Good PAM Solution

A vast number of business-level initiatives can be addressed using a PAM solution, that's why companies are starting to adopt it more and more. Here are the top characteristics of a good PAM solution:

- Embodies password management capabilities like password auto-generation and also password auto-rotation;
- Permits creating an approval workflow meaning escalating and de-escalating users' rights;
- Supports proper management of the privilege account lifecycle, this meaning privileged accounts monitoring and control and sessions logging that will help both with compliance and also with reviewing what happened in case of a security incident;
- Applies the just in time principle (JIT), allowing only a limited amount of time for the users' session: for instance, our PAM supports, for now, a maximum session duration of 2 hours with potential extension in the future, so rights have a limited elevation time;
- Automates PAM activities like creation and deletion of users or user account configuration.
- Enables multi-factor authentication for admins.



About Heimdal[®] Privileged Access Management

Or Heimdal[®] Privilege Elevation
and Delegation Management

About Heimdal[®] Privileged Access Management or Heimdal[®] Privilege Elevation and Delegation Management

General data

With Heimdal Privileged Access Management, files executions or user rights can be effortlessly elevated, and escalations can be revoked. What's more, as we have underlined that Zero-Trust has started to gain ground and since Heimdal always tries to keep up with everything new on the cybersecurity market, we have integrated into our PAM tool a Zero-Trust function too, that starts to act when a running process has no known or trusted signature, thus this module will check that app and see if it's a safe application or a compromised one. Based on the diagnosis, the process will be either allowed to run or killed.

Heimdal Privileged Access Management is also referred to as Heimdal Privilege Elevation and Delegation Management as our product supports PEDM-type non-privileged user account curation features for AD (Active Directory), Azure AD, or hybrid setups.

Curation of lower-privileges accounts befalls on individuals from the IT administration team, empowered by non-exclusive administrative rights (i.e., person or persons fulfilling an administrative role in an RBAC setup can only exercise specific functions within the allotted group policies, thus eliminating over-privileged accounts) as specified in the corresponding product sheet.

[Learn more about PEDM](#)

The user's elevated session in the PAM tool can be managed with full control through the very easy-to-use interface, as you can create an approval/denial flow and manage it from your Heimdal Dashboard. This is not everything, the process of privileged access management can be taken care of from your mobile too, supporting this way the flexibility you need in today's modern activity.

With PAM, privileged sessions can be tracked, system files elevation can be blocked, administrator rights of the users can be live-canceled and what's more, you can establish escalation periods. So, you can use the Administrator Session or the Run with PAM option to select a period of time in which users are granted access to install on their endpoint the desired software.

The options previously specified are available only for a single file elevation, you can revoke the user's rights at any time. What's more is that our tool supports a full audit trail as, at the end of the sessions, actions are logged. Simply put, an end-user requests admin privilege. How? After a request is sent to the Heimdal Dashboard administrator, the request can be either approved or denied. If approved, the user has a limited time for an elevated session, the session's details being eventually logged into the Heimdal Dashboard.

How does our PEDM tool work?

The service called Heimdal Admin Privilege is the one that controls the PAM tool and this module also falls under the Heimdal Agent. What does the Heimdal Agent do? It handles the user permissions management both on a domain-joined computer as well as on a non-domain-joined computer.

You should also know that our PEDM runs under the local SYSTEM user and there are two ways in which it can be used: the first is called Run with PAM, a method that focuses on single-file elevation, and the second is called Administrator Session which focuses on rights of administrators.

Highlights of the Run with PAM Method:

- with this method, a user can right click an executable file and he/she can launch the file with admin permissions;
- executable file means something ending in .exe, .msi, .bat, .cmd;
- users can add reasons for their requests if the Require Reason option is on, if it's not active, then no need to provide any reason;
- then click on Elevate and here are two possibilities in relation to the way the Group Policy was configured: either the server will receive a request to require permission from the Heimdal Dashboard Administrator or the elevation of rights will happen automatically;
- the first situation happens if in your Group Policy the Option "Approval via Dashboard" is checked, the second scenario happens if instead, the "Auto-Mode" is checked in your GP (group policy).

Now let's talk about the second way in which PEDM can be used.

Highlights of the Administrator Session Method

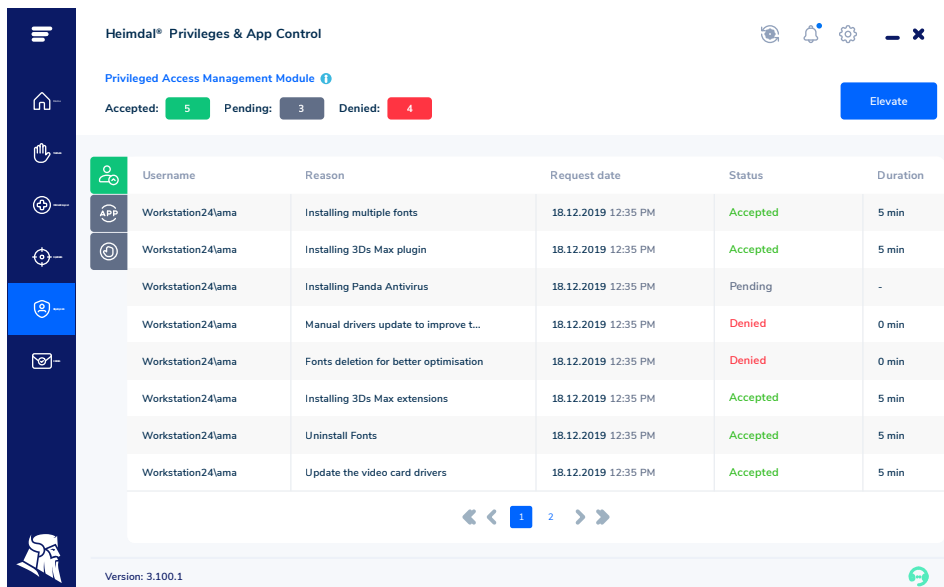
- with this method, the user will have a specific number of minutes to use the admin rights in order to run apps or processes;
- users can use the Elevate button from the Heimdal Agent to request elevation or they can use the method with System Tray: find the Heimdal icon and choose Request admin rights;
- the same pattern with Require Reason repeats as in the first case and the elevation can be granted either automatically or via the Heimdal dashboard as in the first situation above;
- basically, this method makes users part of the local Administrator's group, as a temporary admin level has been given to them, so if users right click on an executable file and choose Run with administrator, since they are designated as temporary admins, they can use their own credentials to run this process;
- it's also worth mentioning here that during an elevated session .cmd files or BAT files are not possible to be executed.

What does the PAM module display?

Our PAM module in your Heimdal Agent gives you data about the following aspects:

- Accepted elevations
- Pending elevations
- Denied elevations
- Username
- Reason
- Request date
- Status
- Duration

See picture below:



The screenshot shows the Heimdal® Privileges & App Control interface. At the top, it displays 'Privileged Access Management Module' with summary statistics: Accepted: 5, Pending: 3, Denied: 4. Below this is a table of requests with columns for Username, Reason, Request date, Status, and Duration. The table contains 8 rows of data. A navigation bar at the bottom shows '1' and '2' with arrows, and the version '3.100.1' is visible in the footer.

Username	Reason	Request date	Status	Duration
Workstation24\lama	Installing multiple fonts	18.12.2019 12:35 PM	Accepted	5 min
Workstation24\lama	Installing 3Ds Max plugin	18.12.2019 12:35 PM	Accepted	5 min
Workstation24\lama	Installing Panda Antivirus	18.12.2019 12:35 PM	Pending	-
Workstation24\lama	Manual drivers update to improve t...	18.12.2019 12:35 PM	Denied	0 min
Workstation24\lama	Fonts deletion for better optimisation	18.12.2019 12:35 PM	Denied	0 min
Workstation24\lama	Installing 3Ds Max extensions	18.12.2019 12:35 PM	Accepted	5 min
Workstation24\lama	Uninstall Fonts	18.12.2019 12:35 PM	Accepted	5 min
Workstation24\lama	Update the video card drivers	18.12.2019 12:35 PM	Accepted	5 min

What Does the Privileges & App Control - Privileged Access Management View Display?

All the information gathered by the Heimdal Agent from your company's endpoints can be found here. Data like history, approvals in pending status, the processes that were the most escalated, most escalating hostname.

You have also a compliance view and a display on the Zero Execution Protection that shows processes intercepted by this engine, these processes mean non-signed executable files.

These files are checked by the Zero-Trust function, and, as we mentioned before, their execution is blocked if found untrusted.

Case Study

To give you more in-depth knowledge about what exactly our PAM does, we will provide details including which apps our PAM elevates, on how many endpoints PAM ran, and more.

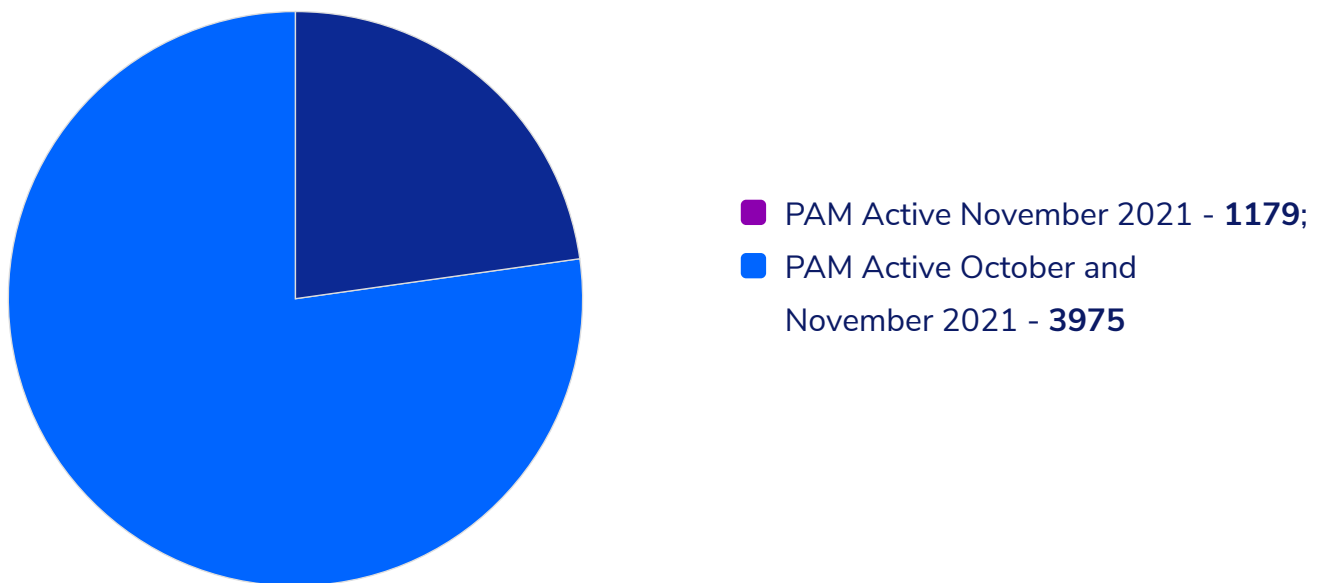
First of all, the main elevated apps from our Privileged and Access Management tool, speaking of a file elevation level, are powershell, cmd, msc like Microsoft Snap-In Control, task manager and browser. Let's shed some light on potential unknown terms. Powershell is a command-line shell and scripting language. It is designed so that both sysadmins and developers can use it for administration and automation tasks.

There are two types of commands in powershell: cmdlets, which are .NET objects, and native commands. These native commands have been carried over from the command prompt of WindowsNT 4.0, while the cmdlets come from Microsoft's background in providing web services and Active Directory tools.

Cmd aka Command Prompt is an interactive text user interface that allows you to issue commands, interact with the computer and run applications. This text-based interface is a windowed environment with a command-line interface.

The Microsoft Management Console (MMC) is a control panel where administrators can manage their resources from one centralized location. An MMC snap-in is usually a dll file which provides some sort of functionality to the MMC.

In November 2021, the number of endpoints on which PAM was active was 1179. In October and November 2021, 3975 endpoints had the PAM enabled.

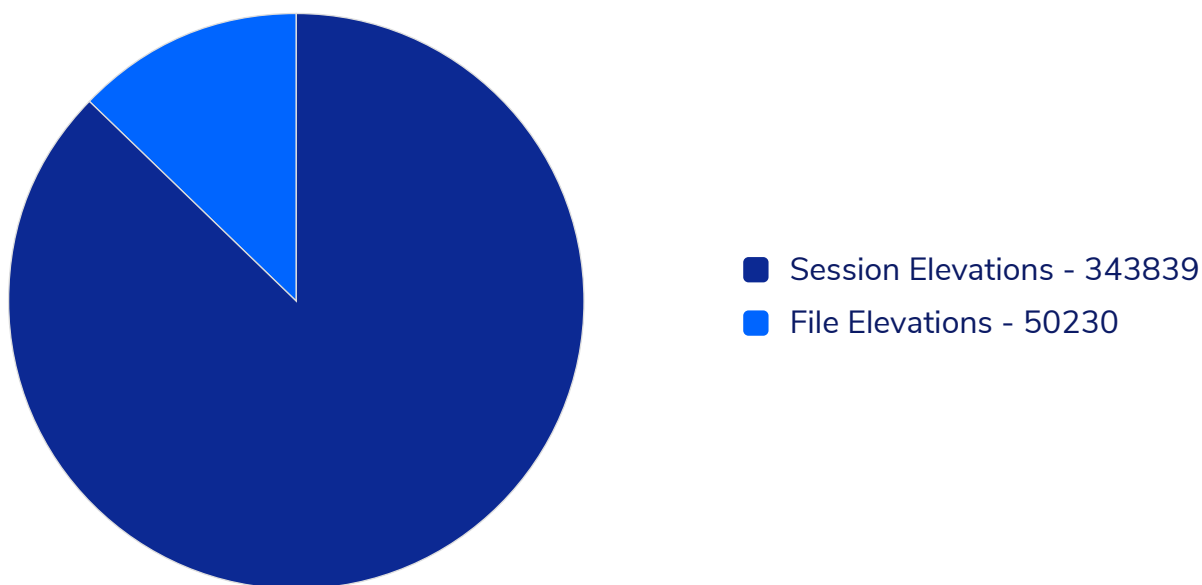


Our PEDM tool also works on two types of privileged elevations: per session and per single file. To give you a picture of all-time elevations, 404178 session elevations were performed out of which 1711 were denied and, speaking of elevations per single file, PAM performed 62093 elevations out of which 607 were denied.



This gives us a total number of all-time elevations of 466271. Almost 500k all-time elevations, isn't that cool? Now, what we've wanted to show you with all these numbers is how our tool works and what it is capable of.

Speaking only of 2021, our Privilege Elevation and Delegation Management Tool performed 343839 session elevations and 502230 file elevations.



The conclusion that can be drawn from all these is that it would have been impossible for an admin to check the user's accountability, to detect the source of an infection or to block an user from installing whatever malicious software without an automated PAM tool, as an admin can analyze the apps running during an elevated session and figure this out and also when speaking of file elevation, an administrator can see before he gives his approval what application the user wants to install.

Last, but not least, we want to also mention our [Application Control](#) Product, as the PAM solution goes hand in hand with it.

With this module, you can work on the restriction of apps that run in your system by creating customized whitelisted apps lists or backlisted apps lists.

The first list type contains only apps that are allowed by default to run in your system and everything else is blocked, the second is quite the opposite, if some app is not found on the blacklist, it can run in your system and it's not checked.

This App Control tool basically helps you speed up the approval/denial flow of files that have default ruling and you can also identify what files run in your system depending on cryptographic hash, name, path, or publisher for instance.

What's more, our APP control module can also perform gray listing because the Zero-Trust Execution Protection module was added to it too.

[Get a Demo](#)

Conclusion

Conclusion

We hope you found the contents of this Privileged Access Management eBook useful and enhanced your knowledge surrounding this sometimes-confusing concept. Now you understand how important is to prioritize the protection of privileged accounts as a core method in your cybersecurity strategy – now is the time to take action.

And remember: proper privileged accounts management cannot be done without a proper and more important, automated Privileged Access Management Tool.

Trust Heimdal to make your company trusted!

[Start Your Journey Here](#)

Featured in





Leading the fight against cybercrime.



www.heimdalsecurity.com

©2023 Heimdal®

Vat No. 35802495, Vester

Farimagsgade 1, 2 Sal, 1606 København V

All other product and company names mentioned are trademarks or registered trademarks of their respective owners.