PATECCO
dynamic identity systems.

PATECCO
dynamic identity systems.

September 2021

PATECCO BEST PRACTICES IN PRIVILEGED ACCESS MANAGEMENT

WHITEPAPER

- Privileged Access Management as a cyber security top priority
- Features of a Privileged Access Management Solution
- Management and protection of Privileged Accounts
- Best practices in Privileged Access Management

Table of Contents

1.Introduction

Privileged Access Management is principal to controlling access and delivers the required balance between system administrators and users. In contrast to Identity Management solutions, often confused with PAM, a Privileged Access Management solution offers a secure way to authorise, track, and protect all privileged accounts across all relevant systems, which ensures absolute control and visibility. That process allows the organisation to control users' access and it is considered to be its most valuable asset. This process also proves the fact that PAM is one of the most important areas of risk management and data security in any enterprise.

In a time of digital transformation, business models are constantly changing which leads to more numerous and widespread privileged accounts. When they are not managed securely, businesses are exposed to the risks of abandoned accounts, unmanaged shared accounts. That is a favourable situation for criminals and hackers to steal and to use credentials for privileged accounts to gain access. To reduce this risk, implementing a cost effective PAM solution is essential.

The modern PAM implementations focus on implementing and maintaining a least privilege model and monitoring activity with advanced data security analytics. Least privilege gives users the access they need to do properly their job. Monitoring and data security analytics detect changes in behaviour that could indicate external or insider threats at work. Those two paradigms keep your business well protected.

According to Gartner's 2019 Best Practices for Privileged Account Management, a quality PAM solution should be based on four pillars: Provide full visibility of all privileged accounts, Govern and control privileged access, Monitor and audit privileged activity and Automate and integrate PAM tools. In this article, we list the most essential features that can help you secure privileged access to your company's sensitive data according to these four pillars.

2.Why Privileged Access Management Should Be a Cyber Security Top Priority For 2021

Cyber security is a hot topic for every enterprise in today's hyper connected world. With the fast-growing technologies like cloud, mobile and virtualization, the security boundaries are a little bit blurred and not each organization protects its valuable and sensitive information properly. As a result, cyber attacks and data leakages occur more often and that's why they are no surprise in the Information Security field. With the increasing sophistication of attacks on organizations of all sizes, the question is not whether the company will suffer a cyber attack, but when that attack will take place, and what its consequences will be.

Controlling privileged actions in a company's infrastructure enables IT systems to be protected from any attempt to perform malicious actions such as theft or improper modifications to the environment – both inside and outside the company. In this context, a Privileged Access Management (PAM) solution can be considered as an important tool to speed up the deployment of a cybersecurity infrastructure.

Privileged Access Management is an area of identity security that helps organizations maintain full control and visibility over their most critical systems and data. A robust PAM solution ensures that all user actions, including those taken by privileged users, are monitored and can be audited in case of a security breach. Controlling privileged access not only reduces the impact of a breach, but it also builds resilience against other causes of disruption including insider threats, misconfigured automation, and accidental operator error in production environments.

Here are the top 7 reasons why Privileged Access Management (PAM) should be your highest cyber security priority:

- **PAM ensures high level of security for privileged credentials**

PAM has drastically changed the way enterprises protect access to critical systems. Using credential vaults and other session control tools, PAM has allowed managers to maintain privileged identities while significantly decreasing the risk of their compromise. By centralizing privileged credentials in one place, PAM systems can ensure a high level of security for them, control who is accessing them, log all accesses and monitor for any suspicious activity.

- **Secure Passwords**

A privileged account is a door to a company's valuable assets, therefore it demands a high level of security. Multi-factor authentication protects the login attributes of privileged accounts. The admin or user's identity verify to authenticate more than one independent credential. Adding layers of security to the credentials in the form of OTP, biometrics, response questions, etc., make it highly difficult for hackers to access the data.

- **Monitor Access**

Only a certain number of specific people have privileged access to the account. PAM can help you detect any unauthorized access, by giving you a clear picture of who can access and who can not. Privileged Access Management also has the capability to detect and alert on malicious activity which helps in enhancing the overall cybersecurity.

- **Keeping track of users**

Privileged Access Management always keeps track of users who access the accounts. It is possible to record any request for password change or update along with the user's details. Besides, it can generate an extended report of the users

along with the number of times they logged in to any application. This provides the organization a clarity on usage and security of the account.

- **PAM enhances compliance**

A large number of corporations have to comply with industry and government regulations and that leads to more challenges. Coming with strong security control recommendations, Privileged Access Management can help get ahead quickly and develop a strong baseline. For better compliance, strong policies have to be in place that cover privileged accounts, monitoring usage and secure logons amongst others. In this case a PAM solution enables you to get in control of managing and securing privileged accounts to meet the needs of the access control requirement for a good number of the regulations, fast-tracking your way to being compliant.

- **PAM enables fast recovery from cyber attacks**

In case of a cyber-attack your Privileged Access Management solution gives you the opportunity to quickly audit privileged accounts that have been used recently, to discover whether any passwords have been changed, and to determine which applications have been executed.

Professionally-designed PAM software also lets you restrict access to sensitive systems, require additional approval processes, force multi-factor authentication for privileged accounts and quickly rotate all passwords to prevent further access by the attackers. Moreover, PAM can help compare a baseline to before and after the incident, so you can quickly determine which privileged accounts might be malicious and audit the lifecycle. This is a good way to ensure recovery and maintaining the integrity of your privileged accounts.

- **PAM provides a high return on investment (ROI)**

One of the main reasons that Privileged Access Management should be a top priority for organizations in 2021 is that it could save them time and money. On one hand, most cyber security solutions only reduce risk and a lot of enterprises spend valuable budget on security solutions that actually add no additional business value. On the other hand, the right PAM solution makes employees more productive by giving them access to systems and applications faster and more securely.

Implementing a proper PAM solution protects the access to sensitive systems and reduces the risk of getting compromised by disclosed passwords on the dark web. PAM also minimizes the cyber fatigue and simplifies the process of rotating and generating new complex passwords. All of these core features save valuable employee time which leads to cost savings for the business.

3. How to Manage and Protect Privileged Accounts?

In recent times a great number of organizations are highly concerned about the evolving threat landscape of cyber-attacks. This is due to the fact that large well-known enterprise organizations have fallen victim to cyber-crimes. Every year billions of records are stolen, identity theft increases, more credentials are abused and financial fraud is now extending into billions of dollars. This is the reason why senior executives are deeply involved in cyber security than ever before. While executives and CISOs continue trying to reduce the risk of these threats, compliance requirements are increasing, as well. The defence against cyber-crime should not rely on technology, but it must involve people, and therefore needs to be less complex and quick to value.

Start from the basics. Define what "privileged access" means in your organisation

The problem for many organizations is that they are not aware where to start and how they can easily adopt a privileged access solution that will lead them to success and maturity. Most of the companies are just getting started with protecting and securing privileged access need to identify which privileged accounts should be targeted as well as ensuring that those who will be using those privileged accounts are clear on the acceptable use and responsibility.

Before implementing a privileged access management strategy it is recommended to identify what a privileged account is for your organization and to map out what important business functions rely on data, systems and access. A good practice is to classify or categorize privileged accounts. This helps for the clear identification of the privileged accounts' importance to the business and makes future decisions easier when it comes to applying security controls. Like any IT security measure designed to help protect critical information assets, managing and protecting privileged account access requires both a plan and an ongoing program. You must identify which privileged accounts should be a priority in your company, and ensure that those who are using these privileged accounts understand acceptable use and their responsibilities. After defining and discovering your privileged accounts, it is time to focus on their protection. The privileged account access must be constantly and proactively managed, monitored, and controlled.

In what ways privileged accounts could compromise your security?

- **Unintentionally**

Compromising the security is supposed to happen unintentionally. Unauthorized modifications to critical data can happen without thinking at any time. Besides, the files that store sensitive data can be shared without checking the legitimacy of the business need, getting you in serious trouble.

- **Maliciously**

Privileged accounts have legitimate access rights, so if they engage in malicious actions, they would be quite difficult to spot. Malicious use of privileged accounts is a serious threat, since these users' activity may not be closely monitored or they usually have the expertise to dodge controls and do maximum damage without leaving any trace.

- **By attackers**

Cyber attackers use different kinds of techniques to obtain the powerful credentials of privileged accounts. Phishing, brute force or coercion are the most familiar.

Despite the steady recommendations and strict regulations, many privileged accounts still remain poorly protected, ignored, or mismanaged, making them easy targets. Having that in mind, here's a number of essential policies that every IT manager or security administrator should follow to avoid compromised privileged account management:

1. Provide training to all your employees

It is important for all your employees to be able to recognize suspicious or unsecure behaviour. This aspect is crucial nowadays, since phishing and social

engineering attacks are getting more sophisticated and more personal devices are being used for business purpose.

2. Limit IT admin access to systems

Developing a least-privilege policy is another good tactic. That means that privileges are only granted when required and approved. Enforce least privilege on endpoints by keeping end-users configured to a standard user profile and automatically elevating their privileges to run only approved and trusted applications. For IT administrator privileged account users, you should control access and implement super user privilege management for Windows and UNIX systems to prevent attackers from running malicious applications, remote access tools, and commands. Least-privilege and application control solutions enable seamless elevation of approved, trusted, and whitelisted applications while minimizing the risk of running unauthorized applications.

3. Develop a privileged account password policy

It's critical to create clear policies that everyone who uses and manages privileged accounts can understand and accept. Put in place a privileged account password protection policy that covers human and non-human accounts to prevent unauthorized access and demonstrate compliance with regulations. It is better to use long passphrases and multi-factor authentication for human accounts. For non-human (services and applications) accounts, passwords should be changed frequently. PAM controls automatically randomize, manage, and vault passwords, and enable you to update all privileged account passwords automatically and simultaneously.

4. Choose the right solution

There are various PAM technology providers to choose from, offering different kinds of features and deployment options. Before choosing, it's important to define use cases for privileged access in your environment and preferred solution capabilities such as service account management, discovery functions, asset and vulnerability management, analytics, file integrity monitoring, SSH key management, and more. Some organizations prefer a vendor-independent technology partner to help them test and evaluate potential solutions. When it comes to a successful deployment, professional security assessments are helpful, by identifying what your privileged accounts are protecting and objectively detailing current security policies, controls, and processes.

5. Monitor accounts with analytics

Privileged accounts should be monitored continuously in order to identify outsiders leveraging stolen credentials, insiders that are not following policies and procedures, and malicious insiders. Privileged user behavior analytics solutions help you gain insight into privileged activity with a behavioral baseline based on machine learning algorithms that consider user activity, account behavior, access behavior, credential sensitivity, and similar user behavior. In case a breach occurs, monitoring privileged account use helps digital forensics identify the root cause and identify critical controls that can be improved to reduce your risk of future cybersecurity threats.

6. Implement multi-factor authentication for employees and third parties

According to Symantec's Internet Security Threat Report, 80 per cent of breaches can be prevented by using multi-factor authentication. Implementing two-factor or multi-factor authentication for both PAM administrators and end users will guarantee that only the right people have access to sensitive resources.

7. Audit and analyze privileged account activity

Continuously observing how privileged accounts are being used through audits and reports will help identify unusual behaviors that may indicate a breach or misuse. You should capture every single user operation and establish accountability and transparency for all PAM-related actions. The automated reports also help track the cause of security incidents, as well as demonstrate compliance with policies and regulations. Auditing of privileged accounts will also ensure you cybersecurity metrics that provide executives with vital information to make more informed business decisions.

8. Prepare an incident response plan

An incident response plan is urgently needed in case a privileged account is compromised. When an account is breached, simply changing privileged account passwords or disabling the privileged account is not acceptable. If compromised by an outside attacker, hackers can install malware and even create their own privileged accounts. If a domain administrator account gets compromised, for example, you should assume that your entire Active Directory, so the attacker cannot easily return.

The execution of these eight policies are not supposed to be an end-all solution to security – there's always more to be done. The proper management of privileged access helps organizations prevent devastating data breaches and comply with regulatory requirements. But at the same time it can be difficult for security teams that are understaffed and struggling to maintain access information across complex IT infrastructures. By providing comprehensive and clear visibility into privileged accounts, implementing least privilege, investing in the right solutions, and monitoring activity, you can be able to prevent privileged accounts from being abused and effectively tackle security risks both inside and outside your organization.

4.7 Important Features of a Privileged Access Management Solution

Nowadays IT organisations are under increasing business and regulatory pressure to control access to privileged accounts. Establishing controls for privileged access continues to be a focus of attention for organisations and auditors. Prevention of both breaches and insider attacks has become a major driver for the adoption of privileged access management (PAM) solutions, in addition to compliance and operational efficiency.

But what is actually Privileged Access Management?

PAM is a set of technologies designed to help organisations address the inherent problems related to privileged accounts. According to the analyst company Kuppingercole, Privileged Access Management has become one of the most relevant areas of Cyber Security associated with Identity and Access Management that deals with identifying, securing and managing privileged credentials across an Organization's IT environment. Once considered a technology option for optimizing administrative efficiency by managing passwords and other secrets, PAM has evolved into a set of crucial technologies for preventing security breaches and credential thefts. PAM today concerns Security and Risk Management leaders as well as Infrastructure and Operation (I&O) leaders across the industries for several security and operational benefits.

To effectively and efficiently control privileged accounts, it is required a combination of adaptive access management features. In this article, we list the most critical features that can help you secure privileged access to your company's sensitive data.

- **Privileged Session Recording**

It is important that the privileged access management solution has the privileged session recording feature to record the actions performed by the user within the system while using a privileged credential. This is one of the main tools to check if users are performing actions relevant to their tasks, ensuring the confidentiality of the company's sensitive data and that all actions are tracked and audited.

Next-generation privileged session management should enable you to observe the date, time, and location of each session. Moreover, you will have a visibility over their very keystrokes to ensure the authenticity of each privileged user. This can prevent insider threats and hackers alike by making sure users use their permissions according to business processes.

- **Multifactor Authentication**

Despite the availability of multiple security protocols, there is still a possibility for privileged accounts to be breached. That is why PAM software must have an additional layer of security with multi-factor authentication protocols when a user requests access. Multifactor authentication can include passwords, hard tokens, time of access monitoring, and behavioural analysis. The last of these proves especially important; it allows your cybersecurity to conduct continuous authentication even after the initial log-in.

- **Centralization**

You should take into account all users, applications, databases, and everything else that could comprise your IT environment. For that reason you need to keep an eye on all of these moving parts simultaneously to ensure proper permission and privileges policies.

Legacy identity management solutions cannot possibly provide your IT security team with the centralized view necessary. In this case Privileged access management can help, because it centralizes your view, controls, and authority over users' identities.

- **Backup**

One of the most important elements of a PAM solution is to have automatic backups. Even with all the security locks, the backup appears as one of the last information security features. This ensures that even with leaked and/or deleted data, the company is able to have access to all data protected by the privileged access management solution.

- **Access Reporting**

Access reporting is also a key feature, so that the responsible person has a complete view of the actions performed through privileged sessions, allowing the identification of security breaches and points for improvement. A complete set of reports optimizes time and work, as there is no need to conduct audits from session to session.

- **Real-time notifications**

It’s critical to stop the attack in time. And the earlier it is prevented, the lesser its consequences will be. So, to be able to respond to a possible security incident in a timely manner, you need to be notified in a real-time. That’s why, when selecting a privileged access management solution, you should make sure to check if it has a fine alerting system.

Most PAM solutions offer a set of standard rules and alerts. For example, responsible security specialists will be notified every time the system registers a failed login attempt for a privileged account. To go further, you can create custom alerts for specific events, activities, or even groups of users.

- **Centralised Audit Logging**

Protecting privileged accounts includes centralized audit logging with a detailed record of user activities. Effective PAM solution could deliver consolidated audit logs and reports from across your server domains and be kept on a separate security domain.

The misuse of privileged access can lead to disastrous consequences, allowing attackers to easily get the most valuable and sensitive information. Deploying a quality PAM solution is a crucial step for every modern organization, which needs secure and properly managed privileged access.

5.Which Are the Best Practices in Privileged Access Management?

The digital world often faces problems of abused privileges or stolen credentials which are seen as the main cause of data breaches. The reason is that many companies do not track how their employees use shared privileged credentials and do not engage in privileged user monitoring. These risks can be reduced through effective privileged access management (PAM). PAM is a set of policies and processes for assigning, controlling, and monitoring administrator-level privileges and should be a major focus for Security and IT management who are looking to mitigate the risks of data breaches and insider risks.

Why companies need strict access control?

As mentioned above compromised credentials are a main cause the vast majority of security breaches. Attackers cannot easily get around modern security mechanisms, so they find a way out and steal credentials by getting into the network. Usually, an attacker aims to get privileged credentials through the network by gaining low-level access to steal data, disable systems, and cover their tracks.

When it comes to controlling access to a company's cloud workloads, big data projects and network devices, the practice shows that most enterprises are not doing enough to address modern security concerns. Today's environment is much different than when all privileged access was constrained to systems and resources inside the network. Privileged access management not only covers infrastructure, databases and network devices, but is extended to cloud environments, big data, DevOps, containers and more.

Basically, PAM includes a collection of practices, policies and technologies that protect administrative or "privileged" access to the back ends of critical systems. Privileged users operate privileged accounts, where they are authorized to set up, configure, reconfigure or delete systems, servers, databases and storage volumes. Privileged users are necessary for the proper functioning of the IT departments, but their features makes them very attractive targets for hackers. Some of the worst data breaches in recent times were a result from the abuse of privileged accounts and the impersonation of privileged user identities. Protecting privileged credentials is a major goal of cyber security policy and security operations.

PAM Best Practices

There are companies still using spreadsheets and common sense to manage privileged accounts, but this is no longer a viable and efficient approach. Such companies should take PAM seriously and to integrate that solution within their Identity and Access Management system. Below is presented a set of PATECCO privileged access best practices which all organizations should follow:

1. Identity Consolidation

The management of privileged identities and their access to critical systems only makes sense if all identities that are to be managed are unambiguously recorded in the context of an initial survey. For this reason, PATECCO recommends starting a PAM project with an analysis, cleansing and consolidation of existing identities, roles, permissions, and local accounts across all, especially heterogeneous, resources.

Only if a uniform and unambiguous collection of all these identities is guaranteed, the next step can be taken meaningfully regarding the consideration of privileged access. Specifically, this means that all identities can also log into the system in a personalized manner, so that authorizations can then be granted to this unique identity even in administrative systems.

As best practices from the PATECCO project experience, an Active Directory is used to consolidate UNIX, Linux, and LDAP identities with a single, unique ID for centralized identity, role, and permission management and for Kerberos-based authentication

2. Privileged Access Request

The central challenge for any privileged access management system is the use of a (minimum) four-eyes principle that uniquely identifies the requestor and the approver and enables traceability. A workflow-based request and approval mechanism for privileged access is usually used for this purpose.

Access to and use of privileged accounts is a key focus for regulators in many industries, but access to critical corporate resources should also be controlled,

documented, and monitored in every other organization to improve security, governance, and compliance.

3. Super User Privilege Management (SUPM)

PATECCO calls the ability to enable a "least privilege" access model for authorized users via authorization extension tools SUPM, Super User Privilege Management. The aim of this procedure is to assign only the minimum set of authorizations at session runtime. An interactive session starts with as few authorizations as possible and is only elevated when required. In particular, the aim is to avoid the necessity of accessing shared accounts through a modified authorization model.

For this PATECCO uses the combination with Identity Consolidation in Active Directory. This provides further administrative advantages so that roles and authorizations for administrative users can be managed centrally. In addition, global changes can be made quickly and consistently under Windows, Linux and UNIX.

4. Shared Account Password Management (SAPM)

When implementing PAM projects, PATECCO puts great emphasis on the protection of the assets of the respective organization. Shared accounts ought to be prevented conceptually, because the containment of data protection violations is most effective if the attack surface can be reduced.

The aim is therefore to reduce the number of privileged accounts as far as possible towards zero and to use SAPM only for emergency login scenarios such as "Break Glass". This applies to legacy and emergency scenarios in which privilege elevation cannot be reached sensibly and in which direct logon as administrator (for example, root) must be allowed in exceptional cases.

5. Application to Application Password Management (AAPM)

A key design deficiency in programs that require automated access to critical systems (such as provisioning systems or other programs that use service accounts) is the use of hard-coded credentials in application code, scripts, and other configuration files. AAPM tools provide a workaround by providing a mechanism (typically APIs) to make credentials securely available on demand by accessing a secure password vault. PATECCO supports during the execution of a

PAM project in implementing AAPM as an extension of the SAPM tools. This helps in managing accounts used by applications or systems to communicate with other applications or systems (such as databases, web services etc.).

By implementing PAM capabilities and following PAM best practices, privileged users have efficient and secure access to the systems they manage, while organizations can monitor all privileged users for all relevant systems. PATECCO supports in ensuring that audit and compliance requirements are met and can support in implementing privacy policies adherent to regulatory and legal requirements, e.g. EU-GDPR.