EXPERTS IN IDENTITY.
ACCESS. GOVERNANCE.

Practice Guide

Privileged Access Management

Guideline for the introduction of
PAM strategies and solutions.

Data theft protection

Automated password management

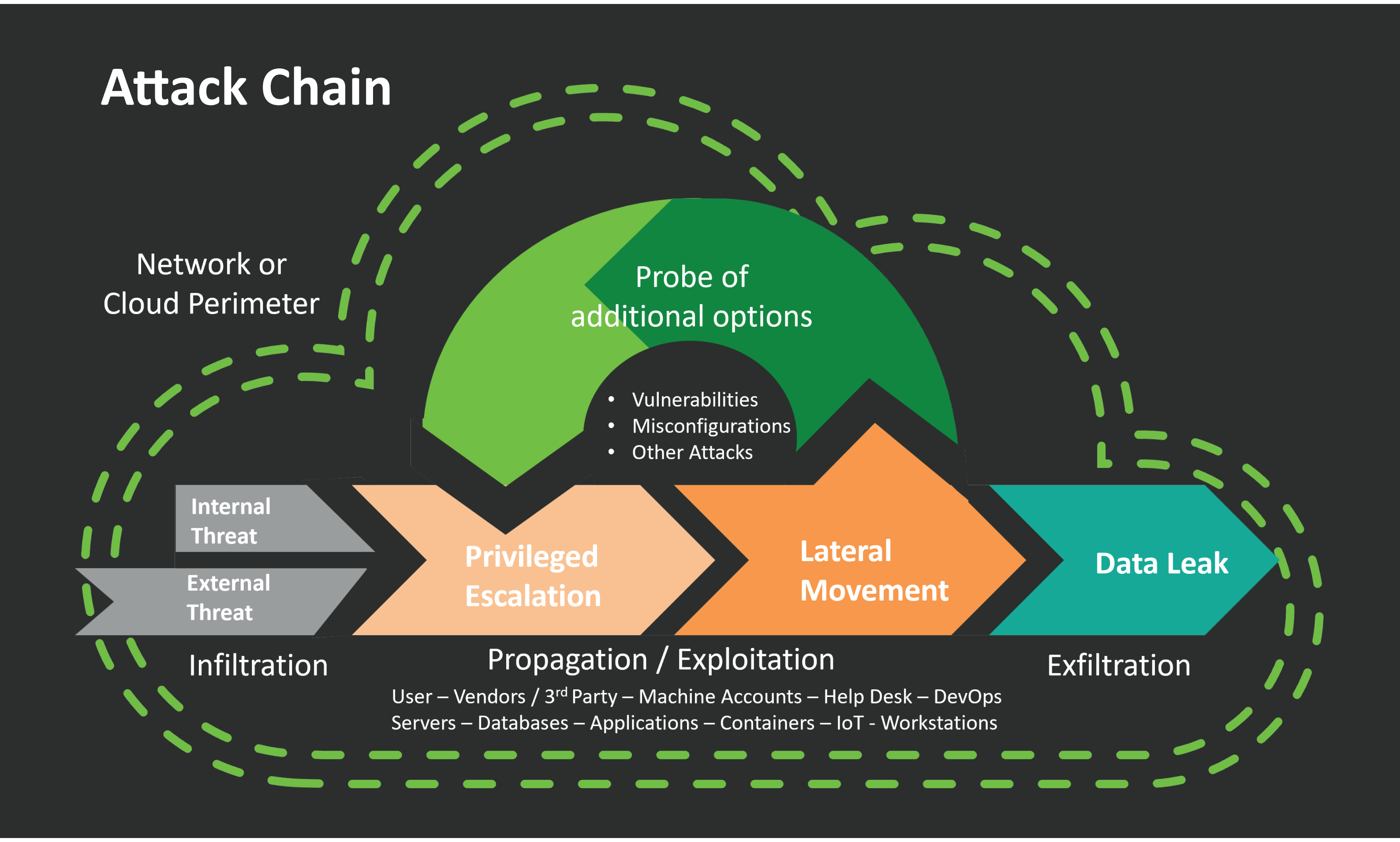
Control of privileged access

1. Introduction

Privileged Access Management (PAM) is a crucial issue for companies of any size. As an important security measure, it helps to guarantee the protection of sensitive data and systems and to avert internal and external threats.

In this Practice Guide for **Privileged Access Management** solutions, we demonstrate why it is important to operate a PAM system for IT security and how to deploy it in order to minimize risks and guarantee adherence to compliance guidelines.

We consider various PAM solutions, their functions and practical steps for implementation in enterprises.


Attack Chain
Network or Cloud Perimeter
Probe of additional options
Vulnerabilities
Misconfigurations
Other Attacks
Internal Threat
External Threat
Privileged Escalation
Lateral Movement
Data Leak
Infiltration
Propagation / Exploitation
Exfiltration
User – Vendors / 3rd Party – Machine Accounts – Help Desk – DevOps
Servers – Databases – Applications – Containers – IoT - Workstations

In today's digital world, management and control of access to IT resources is vital to avert security breaches and to prevent unauthorized users or cyber criminals from gaining access to confidential information.

The focus is on highly privileged users and system authorizations as they are prone to the highest damage risk. Companies are forced to manage privileged accounts and access rights to such an extent that they are only available to authorized users.

Implementing an effective Privileged Access Management solution enables companies to enhance their security by creating traceability and control over administrative sessions while integrating threat protection measures such as access control and user analysis into their IT systems.

2. Why Is Privileged Access Management (PAM) Important?

Privileged Access Management (PAM) is important to protect IT resources against cyber attacks and to fulfil compliance requirements.

- According to a study conducted by CyberArk, **74%** of all security breaches result from abuse of privileged access.
- A survey by Thycotic revealed that **52%** of the companies have no strategy for the management of privileged access.
- The same survey also showed that**70%** of the respondents believe that management of privileged accesses is very important or crucial for their company.
- According to Gartner, **80%** of the enterprises will deploy tools and processes for Privileged Access Management by 2025 to control access to infrastructure and applications compared to **50%** in 2020.

Business **Interruption**: Unauthorized access to systems can disrupt business operations and cause downtimes and loss of productivity. If the unauthorized user makes changes to the system configuration or settings, it may cause system failures and impair the company's ability to deliver products or services to customers.

Theft of intellectual Property: Even if the unauthorized user does not access data, he or she can view or copy protected information such as software code, product designs or business plans. This information can be used by competitors or sold to third parties resulting in a loss of competitive advantages and financial damage for the company.

Breach of **Confidentiality**: Unauthorized access to systems can also result in a breach of confidentiality. Even if no data is accessed, the unauthorized user can view sensitive information such as customer lists, price lists or financial data, which can lead to legal and regulatory sanctions against the company.

Damage of **Reputation**: The discovery of an unauthorized system access may damage the company’s reputation even if no data was retrieved or stolen. Clients, partners and investors may lose confidence in the company’s ability to protect their data which results in business and sales losses.

Violations of applicable **Regulations**: Depending on the industry and jurisdiction, unauthorized access to systems may likewise lead to violations of applicable regulations. Companies may have to meet certain data protection standards or face penalties in case of non-compliance with regulations.

2.1 Cyber Attack Protection

Privileged Access Management (PAM) plays a crucial role in cyber attack protection by controlling and monitoring access to critical IT resources and sensitive data.

An effective PAM solution identifies privileged accounts, such as system administrators or executive staff, and ensures that only authorized users are granted access to these accounts.

This limits the points of attack for hackers and prevents their unauthorized access to confidential information or systems.

An example for the importance of PAM for cyber security: In an attack on a retail company, hackers gained access to the company’s network by using login credentials of a supplier who did not have sufficiently secured privileged access rights.

By successfully compromising the login credentials, the attackers were able to steal the data of millions of customers, which caused an enormous financial loss and a significant damage to the company's image. In this scenario, a PAM solution could have helped to detect the unauthorized access to the network and to initiate countermeasures in time. Furthermore, cyber attacks are not limited to external threats. Internal threats like negligently or maliciously acting employees may also have devastating consequences for a company.

Even in such cases, PAM solutions can help to minimize these risks and ensure that employees are only granted authorizations that are absolutely necessary for their relevant areas of responsibility. This also reduces the risk of data leaks or incorrect configurations due to a human error.

2.2 Fulfilment of Compliance Requirements

Fulfilling compliance requirements is an essential aspect for companies to ensure that their IT resources and systems are in line with applicable laws, regulations and security standards.

PAM solutions for example help organizations to implement the principle of least privilege by ensuring that employees and system administrators only have access to resources that are indispensable for their work.

Another important aspect of compliance requirements is the traceability of administrative sessions. This means that all actions of privileged users in the system must be properly logged and monitored to prevent users from making unwanted changes or tampering.

PAM solutions provide comprehensive auditing and monitoring capabilities that enable security officers to gain a detailed overview of all privileged accesses and activities within their infrastructure.

Some of the most important regulatory requirements supported by PAM include:

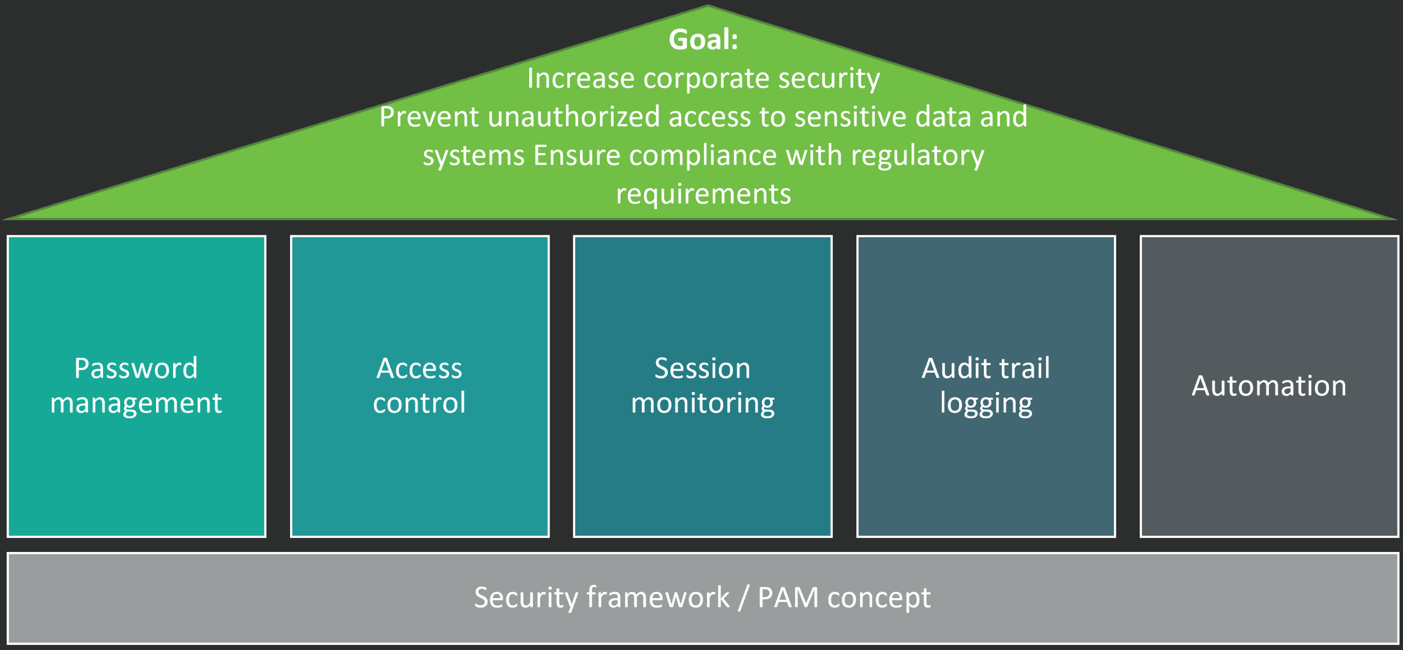
- **ISO/IEC 27001:** This international standard for information security management (ISM) provides a framework for the protection of confidential information. PAM solutions support the compliance with ISO/IEC 27001 by controlling and monitoring access to critical systems and data.
- **Health Insurance Portability and Accountability Act (HIPAA):** HIPAA is a US law regulating the protection and confidentiality of patient data in the healthcare sector. PAM solutions help to control and trace access to Protected Health Information (PHI).
- **Sarbanes-Oxley Act (SOX):** This US law aims to prevent fraud in listed companies by improving transparency and corporate governance. PAM solutions support compliance with SOX requirements by managing access to financial systems and information.
- **Payment Card Industry Data Security Standard (PCI-DSS):** PCI-DSS is a security standard for organizations that process credit card transactions. PAM solutions support compliance with PCI-DSS by restricting and logging access to credit card information and other sensitive data.

- **Data protection laws:** Data protection laws regulate the protection of data in general, in particular the protection of personal data. PAM solutions support their compliance by managing and logging access to personal data.

- **General Data Protection Regulation (GDPR):** The GDPR is a comprehensive data protection regulation by the European Union to regulate the protection of personal data of EU citizens. PAM solutions support compliance with the GDPR by managing, logging and controlling access to personal data.

3. Features of PAM Solutions

PAM solutions provide different features, including password management, access management, monitoring and auditing as well as automation of processes to guarantee the security and compliance of privileged accounts.



Goal:
Increase corporate security
Prevent unauthorized access to sensitive data and systems Ensure compliance with regulatory requirements

Password management

Access control

Session monitoring

Audit trail logging

Automation

Security framework / PAM concept

3.1 Password Management

Password protection is a crucial element of Privileged Access Management. Appropriate password management prevents unauthorized access to sensitive data and systems.

PAM solutions offer various functions to guarantee effective password management, e.g. by automatically generating passwords, enforcing regular password changes and limiting the number of possible failed login attempts. However, not only technical aspects are important, employees must also be sensitized. Regular training and awareness campaigns can make a major contribution.

Furthermore, a simple method for the improvement of password management is the introduction of single sign-on solutions, which allow users to log into the system with a single set of credentials without having to log into different locations each time.

Solid password management is therefore a significant basis for effective PAM and should be part of every security strategy.

3.2 Access Management

Access management is an important feature of Privileged Access Management (PAM) solutions. It controls and manages access to privileged accounts and systems. PAM solutions allow IT managers to restrict access to IT resources to authorized users with appropriate permissions.

Effective access management can contribute to minimizing the risk of abuse or unauthorized access to sensitive data or critical systems. A PAM solution can e.g. request a verification of the user's identity before access to privileged accounts is granted. Another example is the implementation of First-In-First-Out access restrictions to ensure that only a limited number of users are granted access at the same time.

PAM solutions also offer functions for the monitoring and auditing of privileged sessions and for the automation of processes. Monitoring enables IT managers to trace the users' activities in real time and detect unusual activities in privileged accounts. Automation, on the other hand, can help to minimize human errors in the management of access rights and facilitate repetitive tasks.

3.3 Monitoring and Auditing

One of the most important features of Privileged Access Management (PAM) solutions is the monitoring and auditing of privileged accounts. Monitoring helps the system administration team to detect unusual activities or suspicious access attempts using User and Entity Behavior Analytics (UEBA). This way, a possible cyber attack can be detected and prevented at an early stage.

Auditing allows IT managers complete traceability and control over administrative sessions, access management and password management to meet IT security policies and compliance requirements. A PAM solution provides protection of sensitive data through access restrictions, user rights and restrictions as well as confidentiality and monitoring. In summary, monitoring and auditing are an indispensable part of any PAM solution to effectively protect IT resources and meet compliance requirements.

3.4 Automating Processes

PAM solutions not only provide access and password management, but can also include process automation.

This feature helps companies to save time and costs and to enhance efficiency. An example for this automation is the automatic generation of reports or notifications in the event of unauthorized access to privileged accounts. This can help to quickly identify and solve potential problems.

Another example for process automation is the automatic rotation of passwords for privileged accounts to increase protection against cyber attacks.

Password rotation can be configured to occur in intervals and automatically without intervention from a system administrator. This ensures that passwords are changed regularly and guarantees a secure access to privileged accounts.

All in all, process automation in PAM solutions offers many advantages and can help companies to use their IT resources more efficiently while increasing their security.

Check List for PAM

Define: Define what “privileged access” implies and determine what a privileged account is for your company. Specify which IT system authorizations are to be considered privileged.

Discover: Identify your privileged accounts and implement a continuous detection to contain the proliferation of privileged accounts, identify potential insider abuse and detect external threats. It is recommended to use PAM solutions with a continuous scan function that registers all systems and applications for cataloguing and integration of privileged accounts and system authorizations.

Manage and Protect: Proactive management and control of access to privileged accounts through planning and enforcing password rotation, checking, analyzing and managing individual privileged session activities.

Monitor: Monitoring and recording activities of privileged accounts; ensure that you monitor access and activities of your privileged accounts in real time to detect suspected account compromises and potential abuse.

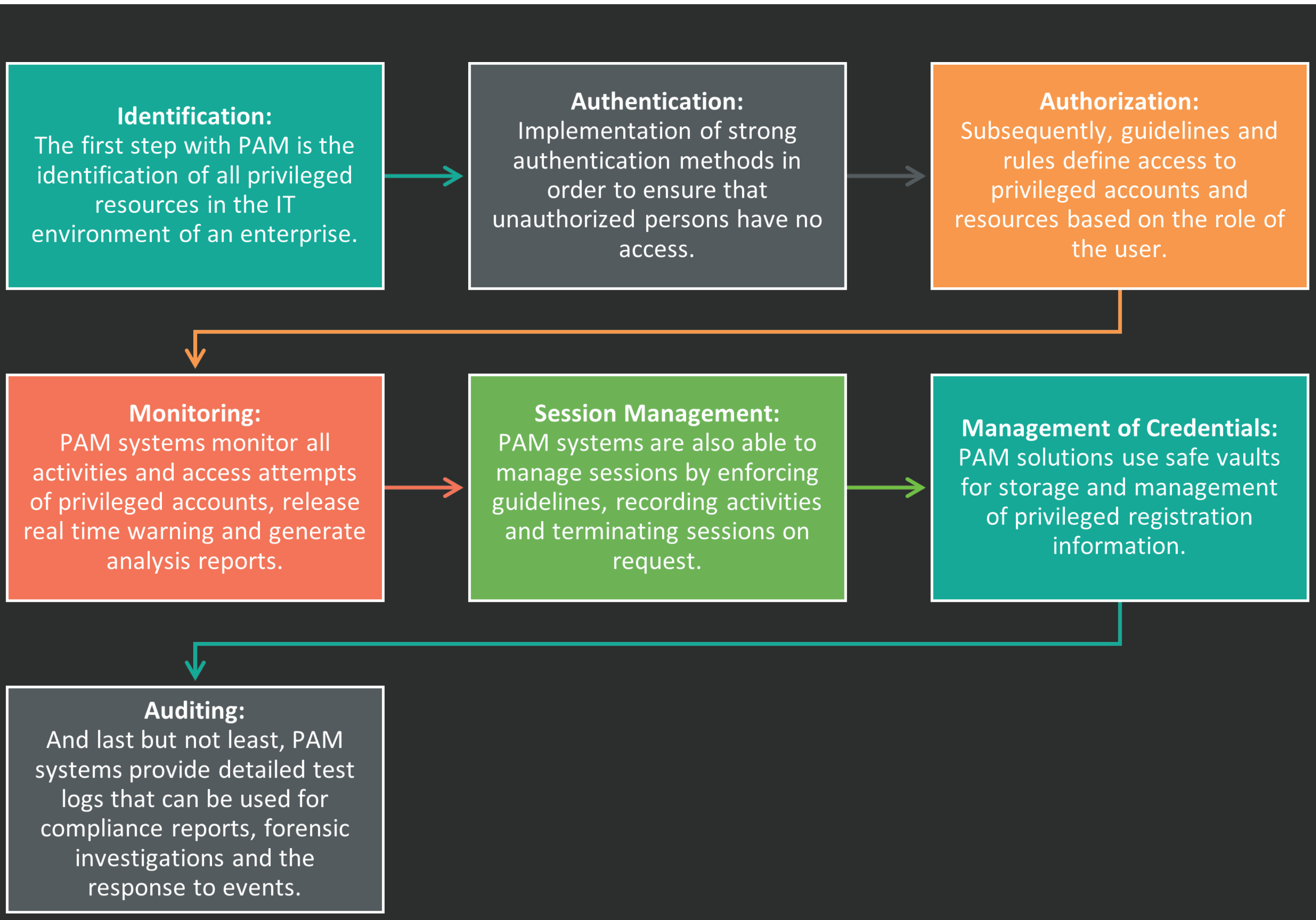
Respond: Take actions to protect compromised accounts and systems based on defined policies and information regarding security breaches.

Review and Audit: Help to identify unusual behavior that may indicate a violation or abuse by continuously monitoring the usage of privileged accounts.

4. Best Practices for the Implementation of PAM Solutions

For the successful implementation of PAM solutions, it is important to identify privileged accounts, implement the principle of least privilege and train employees

Learn more about best practices when implementing PAM solutions.



Identification:
The first step with PAM is the identification of all privileged resources in the IT environment of an enterprise.

Authentication:
Implementation of strong authentication methods in order to ensure that unauthorized persons have no access.

Authorization:
Subsequently, guidelines and rules define access to privileged accounts and resources based on the role of the user.

Monitoring:
PAM systems monitor all activities and access attempts of privileged accounts, release real time warning and generate analysis reports.

Session Management:
PAM systems are also able to manage sessions by enforcing guidelines, recording activities and terminating sessions on request.

Management of Credentials:
PAM solutions use safe vaults for storage and management of privileged registration information.

Auditing:
And last but not least, PAM systems provide detailed test logs that can be used for compliance reports, forensic investigations and the response to events.

4.1 Definition and Identification of Privileged Accounts

Identifying privileged accounts is an important part of Privileged Access Management (PAM). It involves the identification of all user accounts and IT system authorizations that have elevated rights and therefore access to particularly sensitive data and systems. These are often administrative accounts such as that of the system administrator, but also service accounts or accounts of external partners.

It is important to identify all privileged accounts as they pose a higher risk of cyber attacks than regular user accounts. Hackers often attempt to gain access to these accounts in order to obtain confidential information or to cause damage by tampering with the system. It is therefore imperative to accurately identify these accounts and closely monitor their access rights and activities.

For the successful identification of privileged accounts, companies should first perform an inventory of all accounts. They can then decide which accounts should be classified as privileged and thus be subject to increased monitoring. By effectively identifying privileged accounts, companies can increase their IT security and minimize potential risks.

4.2 Implementation of the Principle of Least Privilege

An important part of the implementation of Privileged Access Management solutions is the application of the principle of least privilege. This means that employees are only assigned those authorizations that are necessary for their work in order to prevent unintentional or malicious damages to critical IT resources. For example, an employee in the financial department should only have access to financial data, while a system administrator should only have the necessary authorizations to maintain critical systems.

However, implementing the principle of least privilege can be challenging as it requires all privileged accounts to be carefully reviewed and restricted. An effective way to identify these accounts is to conduct a thorough inventory, including recording the different access rights. In addition, companies should also train and inform their employees on the successful application of the principle of least privilege.

Overall, implementing the principle of least privilege is an important step in securing privileged access in companies. It is an indispensable part of the risk management strategy and helps to protect sensitive data as well as critical IT resources.

4.3 Employee Training

Employees are the key to successful implementation of Privileged Access Management (PAM). Comprehensive training is indispensable to ensure that all employees understand the need of PAM and assume responsibility for the management of privileged accounts.

Training should focus on the identification of privileged accounts, the implementation of the principle of least privilege and the monitoring of accesses. For example, employees should learn how to detect and communicate suspicious activities in connection with privileged accounts. In addition, they should be informed on which restrictions apply to these accounts and how they can help to ensure that these restrictions are adhered to.

Another important aspect of training is education on the importance of compliance requirements. Employees should be aware of how PAM can help to meet these requirements and of the possible consequences of non-compliance. By providing their employees with a solid understanding of PAM, companies can minimize the risk of security breaches and improve their overall IT security.

5. Evaluation of PAM Solutions

In order to guarantee that you select the best PAM solution for your company, you should carefully evaluate and compare the various providers.

Learn more about the evaluation of PAM solutions and how to make the right decision in the following sections!

5.1 Evaluation Criteria

There are several crucial criteria that you should consider when evaluating PAM solutions. First of all, it should be ensured that the solution can cover different kinds of privileged accounts, including local accounts, Active Directory accounts and cloud accounts.

A user-friendly interface and integration with other systems are also decisive factors for the selection of a PAM solution.

Another evaluation criterion is the ability for monitoring and auditing of privileged accesses. A good PAM solution should be able to monitor events in real time and generate detailed reports of activities of privileged users. User and Entity Behavior Analytics allow the early detection and prevention of potential threats.

And finally, the PAM solution should support consistent security policies and offer automation processes to enable IT managers to easily manage users' access rights while ensuring that compliance requirements are met. A good PAM solution can help your company to utilize its IT resources more efficiently while protecting itself against cyber attacks.

5.2 Selection of Providers

When selecting a suitable PAM solution for your company, careful evaluation and comparison is important as there are several providers in the market and each of them has its own strengths and weaknesses. Start by identifying your specific requirements and priorities in order to limit your search.

An important factor for selection is the provider's experience and reputation in the field of PAM security. You are looking for a provider with a proven track record and a good reputation in the field of effective security solutions. Your selected provider should also be able to seamlessly integrate the solution into your existing system infrastructure while meeting all necessary compliance requirements.

Our preferred partners like BeyondTrust, Safeguard (One Identity) or Saviynt, for example, offer a comprehensive suite of features, including password management, identity management and access control.

5.3 Implementation and Integration with Existing Systems

When implementing Privileged Access Management (PAM) solutions, an important aspect is the integration with existing systems. The integration with other security solutions and IT systems ensures the seamless integration of the PAM tool with existing processes. This not only facilitates the implementation but also improves the clarity and efficiency of the entire IT security infrastructure.

When selecting a PAM solution, IT managers have to make sure that they choose a solution which is compatible with existing systems. Ideally, the PAM tool should support APIs (Application Programming Interfaces) to facilitate seamless integration.

An example of a successful integration is the combination of PAM tools with Single Sign-On (SSO) tools to enable users to access privileged accounts without having to log in separately each time.

Close cooperation between IT managers and security managers is very important to ensure that the PAM solution is fully integrated into the existing IT security infrastructure. This is the only way to guarantee a seamless workflow for all parties involved.

6. Challenges When Implementing PAM Solutions

Due to the complexity, employee acceptance and the costs involved, implementing Privileged Management Solutions can be challenging. Nevertheless, it is essential to meet these challenges and establish an effective security solution for your IT resources.

Learn more about the best practices and evaluation criteria for PAM solutions!

6.1 Complexity

Implementing Privileged Access Management solutions can be challenging due to their complexity. This is due to the fact that these solutions must be able to control and monitor the access to sensitive systems, resources and data while maintaining a high level of productivity. The infrastructures provided by the companies are often very complex and thus may complicate an integration of the PAM solutions. Moreover, the user groups' different requirements and their specific needs in terms of access to privileged accounts and management of authorizations can become an additional challenge for IT managers.

For example, it can be difficult to create appropriate user profiles for access management or to define password policies in a way that is both secure and user-friendly.. Careful planning of the implementation and defining clear objectives and priorities are therefore crucial. A good cooperation between IT managers and security managers is also indispensable to ensure that the PAM solution meets the company's requirements and is correctly implemented.

6.2 Employee Acceptance

One of the most common obstacles when implementing Privileged Access Management solutions is employee acceptance. Many employees consider it as an unnecessary restriction if they no longer have unrestricted access to systems. Therefore, it is important to raise awareness and understanding among employees.

For this purpose, training and workshops can be offered to explain the importance of PAM solutions and address possible concerns. It can also be helpful to present some concrete examples of successful cyber attacks and illustrate the impact on the company, to demonstrate that PAM is not just an annoying restriction, but an important protective measure.

It is also useful to show employees that PAM solutions do not mean that they will no longer have access to systems. Rather, it is about using privileged accounts only when absolutely necessary and minimizing the security risks associated with unrestricted access. This allows employees to continue to be able to do their work effectively while protecting the company against potential cyber attacks.

6.3 Costs

Implementing Privileged Access Management solutions can be very cost-intensive. Procurement and integration of PAM software as well as employee training often require considerable investments. Maintaining and updating systems can also be very cost-intensive. In addition, the costs for addressing security risks due to inadequately secured accounts or data leaks can also be significant.

Despite the possible costs, it must be emphasized that an investment in PAM solutions can pay off in the long term. A successful attack on privileged accounts can have serious financial and legal consequences, including fines or claims for damages. By implementing PAM systems, companies cannot only make their systems more secure, but also minimize security risks and meet compliance requirements.

However, careful planning and assessment are vital when implementing PAM solutions. A thorough analysis of the demand and careful evaluation of the available solutions can help to avoid unnecessary costs or mistakes during the implementation process.

7. Summary and Outlook

Overall, the implementation of a Privileged Access Management solution is vital to protect a company's IT resources and sensitive data against threats. Access management is an essential part of IT security and requires appropriate control to minimize risks. PAM solutions offer various features such as password management, access management and monitoring to enhance system security.

When implementing PAM solutions, best practices should be considered. This includes identification of privileged accounts, implementation of the principle of least privilege and employee training. However, selecting a provider and integrating with existing systems can be challenging.

In the future, the complexity of PAM products will increase and it will become even more important for IT managers to educate themselves on access rights management, authorization management, security policies and compliance and take appropriate measures. User and Entity Behavior Analytics will play a central role in detecting threats and management of user rights will become easier and more intuitive.

Secure your data and protect your company with a PAM solution! Contact us today and find out how we can assist you.

Scan me

IPG AG
Theaterstrasse 17
CH-8400 Winterthur

IPG GmbH Deutschland
Hertzstrasse 20
DE-13158 Berlin

IPG Austria GmbH
Johann-Strauss-Gasse 32
AT-1040 Vienna

www.ipg-group.com

info@ipg-group.com