senhasegura®

PRACTICAL GUIDE TO PRIVILEGED ACCESS MANAGEMENT (PAM)

Privileged Access Management (PAM) ensures business security by monitoring privileged accounts, preventing external and insider threats that result from the misuse of administrator rights.

The concept of PAM is based on the Principle of Least Privilege, where users receive the absolute minimum access necessary to fulfill their responsibilities. If you are only concerned about intentional insider threats, you are just scratching the surface.

It should come as no surprise that administrator rights are not just abused by malicious employees. They can be used for malicious purposes by malicious hackers who break into privileged accounts and gain unauthorized access to your systems.

As a result, they can move laterally across the infrastructure, creating additional users with elevated rights or to view, edit, and delete their data as they please. But Privileged Access Management (PAM) ensures that you are the only one in charge and able to manage and mitigate threats.

WHAT IS PRIVILEGED ACCESS MANAGEMENT?

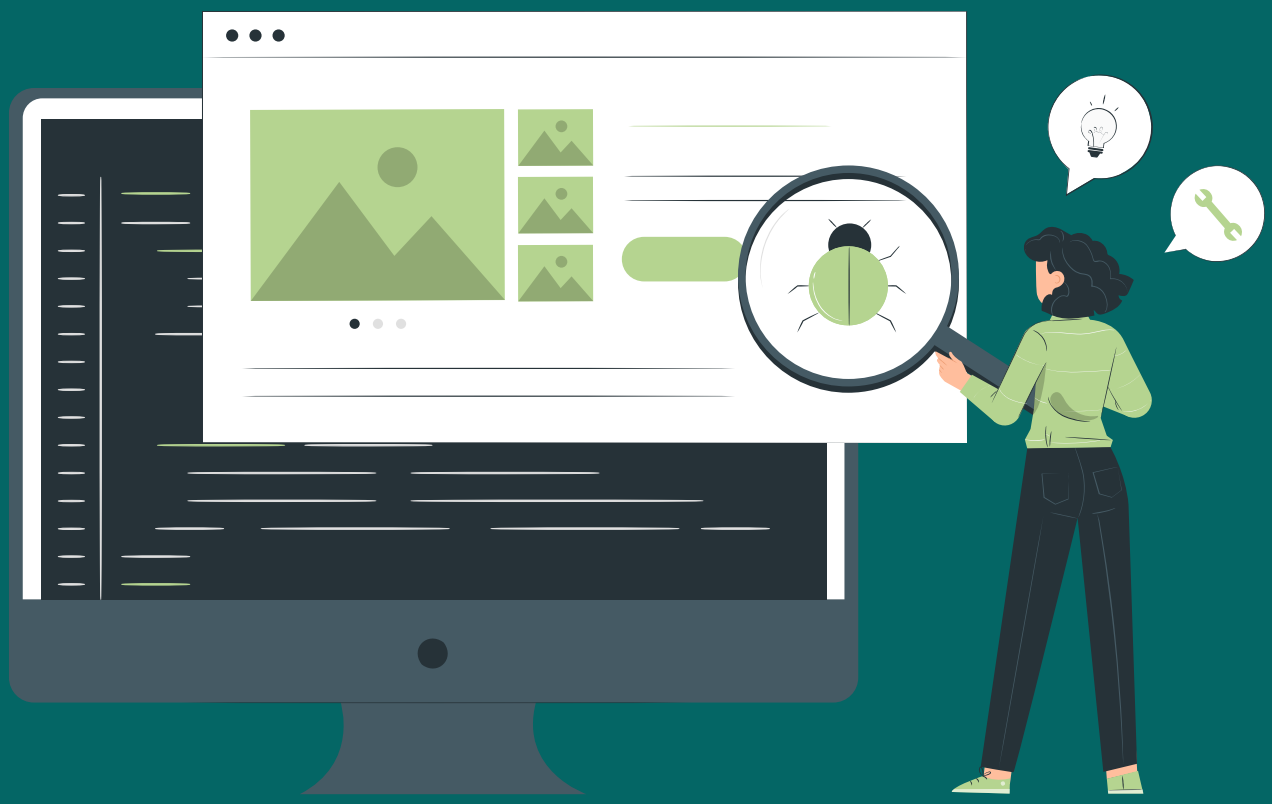
Privileged Access Management is a component of Identity and Access Management (IAM) designed to manage and monitor privileged access to accounts and applications, alerting system administrators about high-risk events.

Privileged access means higher access rights than other users. These elevated access rights are usually granted to super users and allow full control of systems, applications, and data.

The implementation of PAM is based on the principle of least privilege, guaranteeing all employees the minimum level of access with the ability to assign and elevate privileges as needed.

With measures such as proxy technology and session management, PAM secures organizational systems and devices and provides enhanced control and visibility to support audit efforts and faster incident response.

PAM adds a layer of security to reduce risk, protect against external threats, and support your organization's compliance with security policies and data protection laws.



WHAT PROBLEMS DOES PAM SOLVE?

PAM helps protect privileged access, users, and credentials from potential security threats and breaches. Moreover, PAM provides your organization with simplified integration and deactivation, increased productivity and compliance, and time savings.

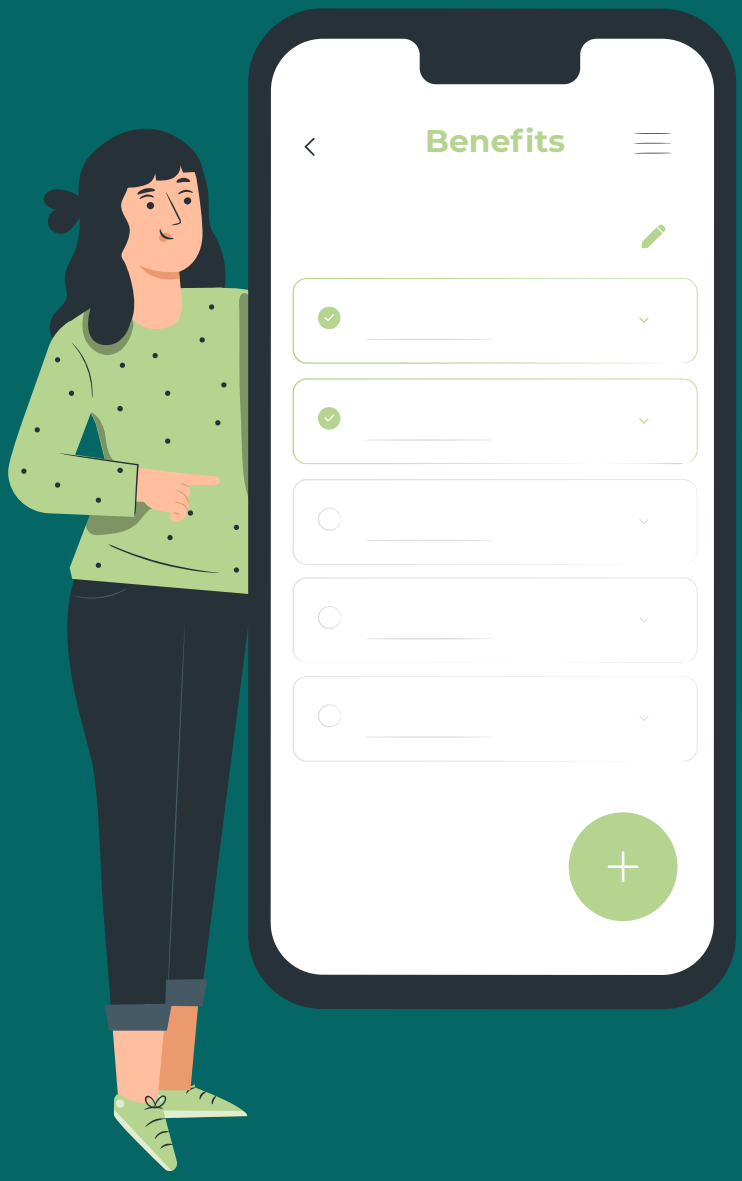
Its process automation streamlines workflows with simplified authentication and removed manual integration, allowing users to spend more time on projects, ensuring everyone has the appropriate level of access to what they need.

And with live logs and monitoring capability for sensitive information, you reduce risks and have an activity inventory prepared for internal audits and analysis.

How does PAM work?

PAM enables centralized control that scales between privileged users and accounts, with integrated password management and monitoring tools to reduce risk without sacrificing end-user experience.

Using proxy technology, PAM puts itself between the privileged user and the information they are trying to access, giving them access through authentication and authorization, without ever revealing the password to them. Proxy servers can also log privileged activity, either for later review or live auditing.



BENEFITS OF PRIVILEGED ACCESS MANAGEMENT

In a world where nearly 80 percent of security breaches involve privileged credential theft, implementing a Privileged Access Management (PAM) solution is one of the most crucial actions companies can take to protect their assets.

Privileged accounts provide special account privileges to selected users within the company to perform critical business roles such as accessing sensitive company information, resetting user passwords, and making changes to IT infrastructure systems.

However, if these accounts are compromised, they can put the company at serious risk. With a robust PAM solution, organizations can ensure that those who need privileged access get it while protecting critical business systems from destructive cyberattacks.

Here are some benefits of incorporating PAM into your identity management strategy:

Controlling Access to Privileged Accounts

Today, many organizations do not have full visibility into their privileged accounts, whether on-premises, in the cloud, or both. Many organizations manually control privileged account passwords using spreadsheets, an inefficient practice that increases risk.

Without the full visibility they need, it is difficult for administrators to know which users have access to what

information, especially as the company grows and hires employees and other users change roles or leave the company.

Using PAM, organizations can track privileged access from a single location, automatically provisioning and de-provisioning users as their roles change or they leave the company.

They can also monitor and record sessions to increase their visibility into privileged account activity. And they can keep user activities in a centralized location, allowing them to meet compliance regulations and review access if suspicious activity occurs.

With an easy way to monitor privileged accounts, companies can ensure they maintain control over their most valuable assets.

Preventing Attacks on Privileged Accounts

Privileged credentials are the main target of outside hackers, as they hold the keys to an organization's most sensitive data. These accounts are also vulnerable to misuse by unhappy former employees, which is the cause of many of the data breaches.

By storing privileged account credentials in a separate, secure repository, PAM allows companies to isolate their use and track their activities, effectively reducing the risk of them being misused or stolen.

Administrators can also configure PAM to set time limits and other rules for user access, as well as automatically remove privileges as soon as an individual moves to another role or leaves the company, which often limits access to those who really need it.

Regulating Access in One Place

Companies often manage privileged accounts and credentials within different areas, using practices in different parts of the organization. This not only makes management complex but also exposes the company to increasing risks.

With a PAM solution, organizations can manage all of their privileged accounts from one central location regardless of the platform, hardware device, application, or service in use.

Using the solution makes it easier for companies to see which users and groups have access to sensitive systems and data while maintaining control over the exact permissions allowed for each user and group.

This simplifies the management process, making it easier to grant and remove access as needs change.

Restricting Credential Sharing

Many administrator accounts are shared by multiple individuals within the organization and, for convenience, often use the same password across multiple systems.

These practices can make it impossible to determine what actions were taken by specific individuals, increasing an organization's security risk and demonstrating non-compliance with regulatory requirements.

PAM can help organizations protect against these risks by ensuring that each individual uses a unique login. PAM solutions can also require strong passwords, making routine changes based on how sensitive the account is.

Administrators can also configure PAM with single sign-on (SSO) authentication to hide user passwords and ensure password strength whenever users access valuable assets.

If you want to delve into a very interesting specific point of how Privileged Access Management can bring protection to your company, check out our article that shows you how to protect your remote accesses through PAM.

Reviewing Real-time Risk Behavior Notifications

Many PAM solutions provide administrators with real-time email and text notifications to alert them of suspicious activity.

They can configure alert settings to receive notifications whenever a privileged user accesses specific data or systems, when potential policy violations or flagged risks occur, such as too many privileges assigned to specific accounts.

With the ability to review notifications in real-time,

administrators can quickly make the necessary changes to maintain a high level of security at all times.

Quick Implementation

Unlike the first generation of PAM, modern solutions require minimal changes to an organization's existing business environment and processes, making them easy to implement.

With the increasing availability of SaaS-based PAM solutions, organizations do not have the hassle of deploying PAM software, saving valuable time. And most PAM solutions integrate well with a company's current systems and application deployment methods.

This fast deployment allows companies to gain immediate value from PAM without requiring changes to the way users work.

Integration with Identity and Access Management Systems

Today's leading PAM solutions are capable of integrating with an organization's identity and access management (IAM) systems, closing security gaps, and eliminating redundant processes for privileged and unprivileged accounts.

By combining the power of PAM with identity governance, companies can leverage automated provisioning and de-provisioning, along with faster reporting and auditing

across all of their user accounts. This in turn saves time and reduces the complexity of protecting all user identities.

PAM Subcategories

Here are the management and monitoring features PAM offers that might be a good fit for your organization.

Shared Access Password Manager (SAPM)

This measure removes the possibility of human error when storing, remembering, or creating unique passwords. It grants access to shared critical accounts with multi-factor authentication and establishes an audit trail to track activity.

SuperUser Privilege Management (SUPM)

Super Users are those who have the highest privilege level within an organization (usually IT staff) and can modify privileges, files, settings, users, or data.

The superuser privilege manager feature allows super users to designate temporary and permanent elevations of privilege while hiding the end-user account and password.

Privileged Session Management (PSM)

Privileged Session Management is an enhanced security and compliance measure. It allows for remote recording and review of active sessions and session termination capability if required. It also connects the privileged administrator

with their target information without revealing the access password.

Application Access Password Manager (AAPM)

This feature places password access in a secure, centralized location. It releases credentials at the right time using an application programming interface (API), entirely replacing the need for hard-coded passwords.

Do you want to learn about your company's maturity level and check if it is really ready for full implementation of good Privileged Access Management? Check out our article featuring **all PAM maturity levels!**

REQUEST A DEMO NOW!

senhasegura®