# Best Practices Manual for PAM

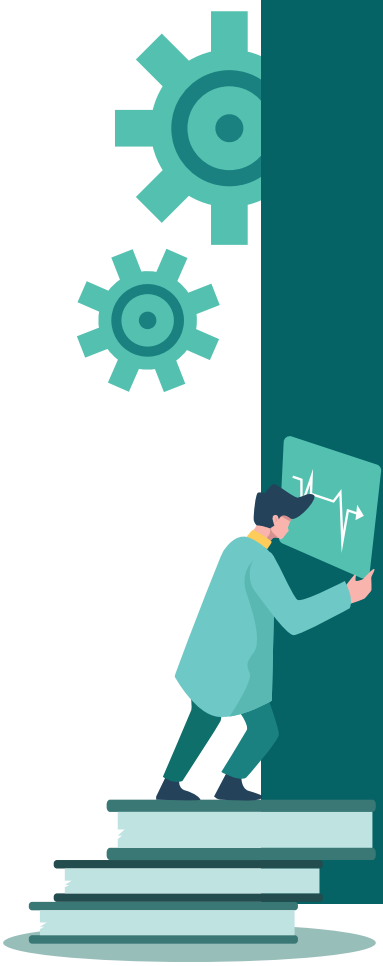
senhasegura®

# INTRODUCTION

The use of a PAM solution has become essential in companies, considering the need for all markets to stop data leaks, ensure their security, protect the development, avoid cyberattacks in their corporations, identify harmful users on the server, be in compliance with new legislation, among other points that are tackled through a PAM solution.

But with the cybersecurity boom, some gaps in the implementation of this type of technology have been overlooked in some companies. Against this background, in this e-book, we will help you identify and solve these questions.

# WHAT TO CONSIDER BEFORE GETTING A PAM SOLUTION



## Tracking and Protection of all Privileged Accounts

It is very difficult to manage access to a system without using a PAM solution. For this measure to be implemented correctly in your company, the choice of the ideal tool must be analyzed very carefully.

The first point that you should know is: getting a PAM solution does not mean ending your credential problems. Before that, the company must have a PAM-centered vision about its business.

Therefore, first of all, it is essential to define your PAM goals so that you can choose the right tools to achieve them with the implementation of new processes within the company, aiming at the Four Pillars of PAM.

## Points to note:

1. Track and protect all privileged accounts from your corporation, which include: privileged accounts, shared accounts, application credentials, service accounts, third-party accounts, etc.

2. Identify people who have access.

3. Identify which of the credentials have critical information, for example: IP, PPI, PHI, etc.; and implement privileged access security

4. Remember to monitor areas outside the IT environment, such as HR, Finances, and Marketing

# GOVERNING AND CONTROLLING ACCESS

After identifying all the points that must have a layer of protection in a credential, there must be a professional responsible for making the necessary changes and counting the privileged accesses.

**For example:**

This person could offer temporary privileged access for a user to perform a certain task, and after the specified time, the access and the credentials would expiry.

In addition to having a responsible person, the PAM system will ensure that all requests are made successfully and without deviations of information, leaving the record of all privileged accesses.

A good way to implement this process at your company is by documenting when, what, where, who, and why the user is requesting access for a specific type of task.

## Here are some extra privileged access use cases, according to Gartner:

| PAM user classes | Example users | Recommendations |
|---|---|---|
| Employees who require frequent administrative access to large infrastructure segments for a wide variety of tasks that are difficult to predict and that may require powerful levels of privileges. | System, end-point, network, database, and exchange administrators, etc. | Use operational PAM accounts combined and controlled by a PASM tool, each focused on a specific part of the infrastructure.<br><br>Use non-privileged personal accounts in combination with PEDM to elevate privileges.<br><br>Mature some activities by migrating to PAM automation and the JIT access mechanism to further reduce administrative access and user activity. |

| PAM user classes | Example users | Recommendations |
|---|---|---|
| Employees who require frequent administrative access to large infrastructure segments to perform well-defined tasks. | Service desk; operators. | Use operational accounts shared and controlled by a PASM tool, each focused on a specific part of the infrastructure.<br><br>This is a great case for automating privileged tasks.<br><br>Focus on granting access at the shell level whenever possible.<br><br>Create scripts to perform defined operations. |
| Employees who require infrequent administrative access to small infrastructure segments for a wide variety of tasks with limited privileges. | Developers who need limited access to production systems (usually, access to read-only, debugging, and tracking files). | Use operational accounts grouped and controlled by a PASM tool, each focused on a specific part of the infrastructure.<br><br>Use JIT elevation to elevate privileges. |
| Employees who require frequent access to small infrastructure segments during their working days. | IT projects, developers who need to access development and testing systems. | Use non-privileged personal accounts in combination with JIT and PEDM elevation.<br><br>Use operational accounts grouped and controlled by a PASM tool, each focused on a specific part of the infrastructure.<br><br>Use the first option for common and frequent privileged operations; use the second for special cases. |
| Non-employees who require sporadic access and need privileged access. | Contractors, consultants, suppliers, etc. that support infrastructure, platforms, software, cloud platforms, and management. | Use multiple operational accounts shared and controlled by a PASM tool. |

Source: Gartner (January 2019)

**But remember:**

**Release as few privileges as possible** so that the user can perform a certain task.

# RECORDING AND AUDITING

It is recommended that you get a PAM tool that records as much information as possible from what the user has done, so you will have greater control over the available data of your company and immediate identification of possible threats. Therefore, if a PAM solution has a **recording feature for its sessions**, its quality will be quite good.

Also, the control of logs, resources to alert harmful behaviors, and constant human monitoring of the privileged accesses that have taken place are a good way to identify possible violations in the company's data.

Therefore, you should frequently monitor recorded sessions to avoid headaches.

# AUTOMATION IN PRIVILEGED TASKS

As already mentioned, **a PAM solution can automate some functions** and decrease human need in different tasks, which maximizes efficiency and minimizes the bureaucracy in company processes.

These functions are used for recurring tasks, simple changes, software installation, etc.

**For such purpose:**

- identify which tasks can be automatically assigned;
- check what integrations your PAM solution has;
- define what functions will be available to the user when requesting permission for the privilege.