Garantir

Simplifying Privileged Access Management For The Enterprise

Privileged Access Management (PAM) is a crucial component of every enterprise's cybersecurity posture. This e-book discusses strategies that will both simplify and strengthen the security of PAM.

Table Of Contents

Introduction

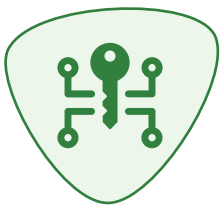
Imagine the perfect Privileged Access Management (PAM) solution, where access to any type of resource is centrally managed and integrated with the enterprise identity provider. Access to applications, email, servers, and even locally stored files is controlled via group membership, all done transparently to end users. Advanced security controls such as multi-factor authentication, device authentication, and approval workflows are seamlessly integrated whenever a user attempts to access a privileged resource. Employees who switch jobs or leave the company immediately have their permissions changed, and everything is auditable from a central location. With a proper PAM solution in place, this is all possible without requiring any custom software development or changes to the tools your end users use.

Privileged Access Management (PAM): The Basics

From a very high level, Privileged Access Management (PAM) refers to the set of strategies and technologies that an organization uses to secure and restrict access to critical servers, systems, infrastructure, and data. There are four tenants often associated with PAM, which are described in detail below.

1. Strong Authentication

The term strong authentication refers to any method of verifying the identity of a user or device that is sufficiently thorough to ensure security. Common security controls used to implement strong authentication include multi-factor authentication, device authentication, and IP address whitelisting.

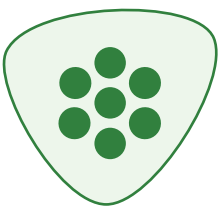


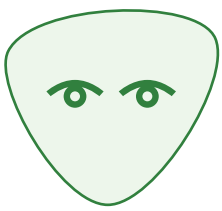
2. The Principle Of Least Privilege

The principle of least privilege mandates that every user should only have access to the systems and resources they need to perform their duties, and nothing more.

3. Zero Standing Privileges (ZSP)

The principle of zero standing privileges states that no user should have permanent access to critical systems and servers. Instead, the users who do occasionally need access to critical systems should be granted Just-in-Time (JIT) access.





4. Visibility On Privileged Users

When an end-user begins a session with a critical system, the enterprise must have complete visibility on who the end-user is, why they are connecting to that system, and what actions they take while administering that system.

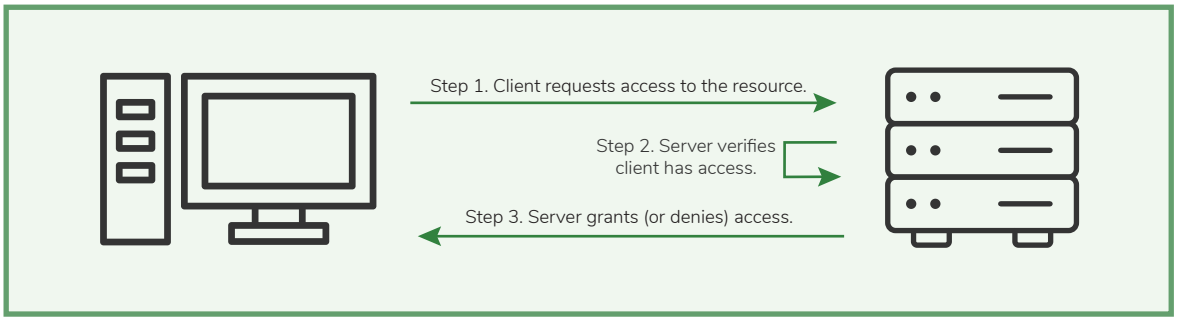
A Closer Look: PAM Under the Hood

There are many varieties of resources to which an enterprise must control access, but, generally, access is controlled with one of two methods: rule-based access control or cryptographic access control (or both).

Rule-Based Access Control

When most people think of rule-based access controls, the client-server model comes to mind, but rule-based access controls are also applied to locally-stored resources, with the operating system enforcing control. In either case, an enforcer decides whether a user will be granted access to the resource based on a set of rules. These rules typically use some combination of group memberships, roles, attributes, etc., that map users to resources and the permissions they have on those resources.

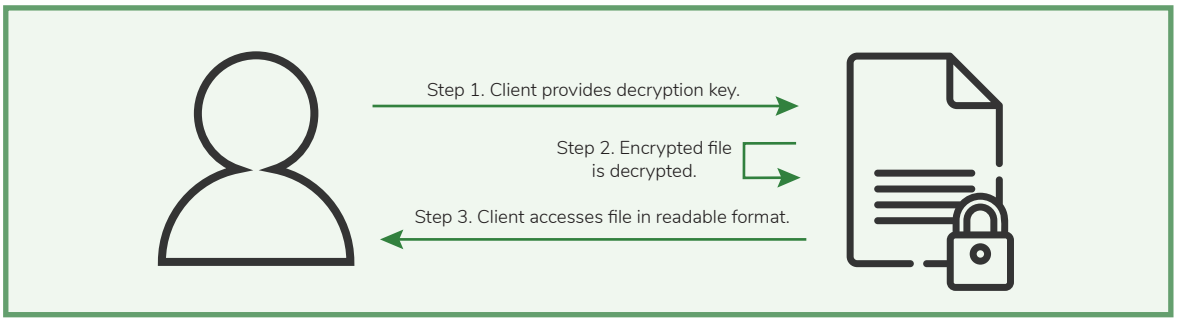
- *Client-Server Example: An end-user with normal privileges can only see their own files and files shared with them on the file server, but an administrator may be able to see every file on the server.*
- *Locally-Stored Resource Example: Operating system only allows administrators to access certain folders.*



Cryptographic Access Control

Alternatively to restricting access to the resource, the resource can be encrypted. Since the resource can only be decrypted by those with access to the decryption key, this effectively moves the access control from the resource to the decryption key. Of course, this approach can be used in combination with rule-based access controls.

Example: An end-user encrypts a PDF and stores it on a publicly-accessible server. Anyone can retrieve the encrypted file but only those with the decryption key can actually decrypt and read the file.



Challenges With PAM

According to a 2018 report from Forrester, “80% of data breaches have a connection to compromised privileged credentials, such as passwords, tokens, keys, and certificates.” This figure underscores the importance of protecting privileged credentials. However, there are several major challenges that enterprises face in improving Privileged Access Management.

Indexing Privileged Accounts

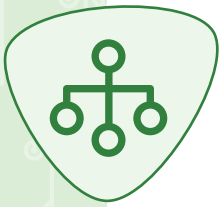
The first step to controlling access to privileged systems is generating an exhaustive inventory of all privileged user accounts throughout the enterprise. In many cases, this is not an easy task. Some enterprises simply do not have visibility on all privileged user accounts, presenting major challenges to strengthening PAM.

Managing Credentials

In a typical IT environment, credentials are often scattered across the enterprise, stored in software on end-point devices and servers. Some of these credentials are neither visible nor auditable. As a result, it’s extremely difficult to keep them secure and to grant and revoke privileges when needed.

Strengthening Security Controls

Enforcing stronger security controls, such as multi-factor authentication and device authentication, is often a complex and time-consuming task. It may require manually reconfiguring servers and modifying applications. Some existing tools and applications may not support these features at all.



Managing Access

In the absence of tools that enable centralized management of credentials, it’s difficult to ensure that only authorized personnel are using those credentials to access privileged resources. Additionally, any credentials that are exported to clients can be easily copied for future use or stolen by attackers.

Monitoring Access

Without an exhaustive inventory of privileged user accounts and centralized management of credentials, it’s not possible to monitor all privileged access. Instead, organizations are left to aggregate logs from a constantly growing set of servers and analyze them in real time.

Supporting All Access Methods

Many enterprises employ some elements of PAM for one or two use cases (e.g., SSH) but overlook the other methods used to access privileged resources in their environment. A proper PAM solution should cover every use case within the enterprise today, as well as all use cases that may emerge in the future.

1. “The Forrester Wave: Privileged Identity Management, Q4 2018” by Andras Cser. Published November 14, 2018.

A Novel Approach To Improving PAM

To improve PAM, a more systematic method is required. Underpinning all modern protocols and use cases is public-key cryptography (PKC). Using PKC, it is possible to deploy a passwordless and SSO-enabled PAM solution that applies to all use cases while being minimally disruptive to existing infrastructure and processes.

Tether Identity To Cryptographic Keys & Certificates

The first step to shoring up PAM is to translate identity, for both humans and machines, to a common medium that all client-server protocols understand: cryptographic keys and certificates. Every user and server is assigned a cryptographic identity in the form of a public-private key pair and certificate. Each user receives a standard identity key-pair and a privileged access key-pair. These certificates (or public keys) uniquely identify the user and whether they are accessing a resource as a privileged user or a standard user.

Centrally Manage All Keys & Certificates

It is poor security practice to export credentials to end-users because these keys, passwords, etc., can be easily copied and stored for use later on. Additionally, exported credentials are a treasure trove for cyber criminals looking to access your privileged systems while masquerading as your legitimate users. A better approach is to centrally store the identity keys in a non-exportable manner (preferably in an HSM or enterprise key manager) and only allow for proxied use of the keys to authenticated and authorized users. This way, legitimate users can use their keys (when the enterprise allows them to) without ever possessing the actual key bytes.

Enforce Granular Access Controls

In addition to ensuring that only authenticated users can use the keys for which they have authorization, the system must be able to enforce strong security controls when needed. With the keys centrally managed, the server proxying the identity keys can easily enforce any policy on users, such as multi-factor authentication, device authentication, approval workflows, IP address whitelisting, and more.

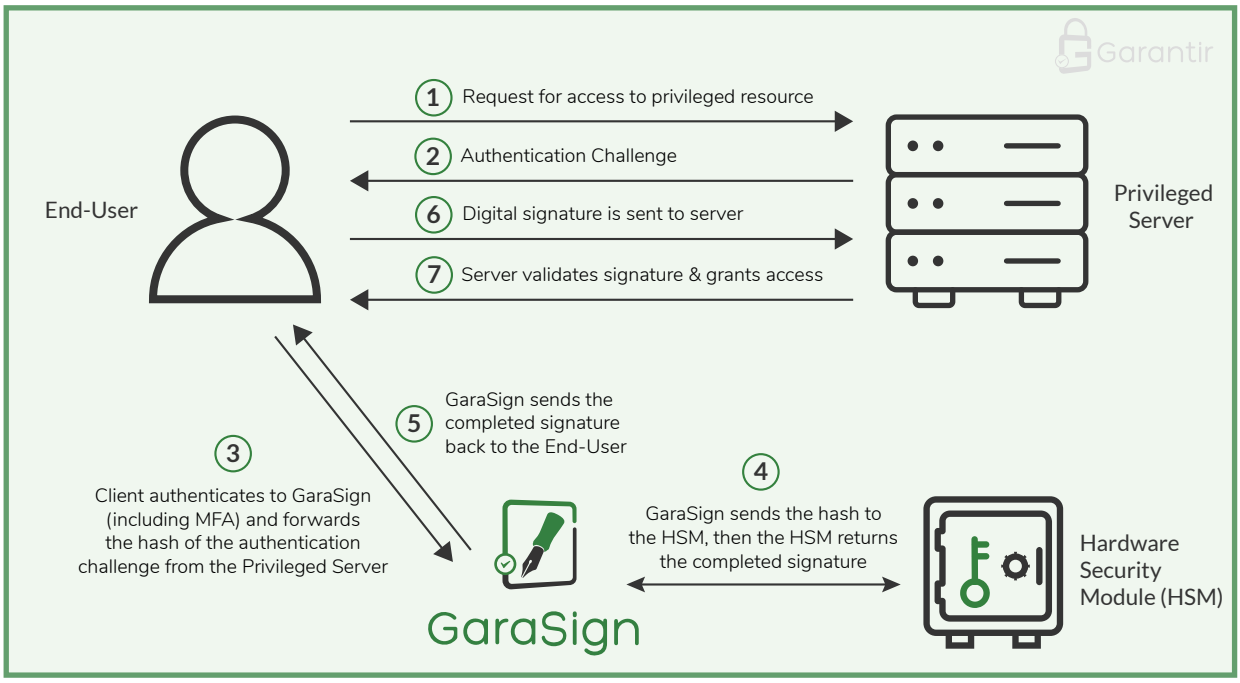
Furthermore, enterprises can keep privileged identity keys disabled by default and only enable them when the key needs to be used (e.g., triggered by a ticket request being approved), enabling Just-in-Time access. Since the resource server only receives the result of using the key (e.g., the signature response during a challenge-response handshake), something it supports natively, it does not have to be reconfigured in order to support these more advanced security controls.

Maintain Full Visibility & Auditing Capabilities

With all cryptographic keys centrally managed and secured, monitoring and auditing usage of these keys is simple. CISOs, security engineers, and auditors are able to see which keys were used, by whom, and at what time. Audits can easily be performed whenever needed, simplifying compliance with various data security regulations.

GaraSign: Simplifying & Strengthening PAM

GaraSign is a secure platform for cryptographic operations that is compatible with every public-private key use case, from SSH and TLS to code signing, document signing, and more. GaraSign facilitates Privileged Access Management and supports Single Sign-On by enabling fast and seamless key-based authentication with private keys that are secured within hardware security modules (HSM) at all times.



Secure

• Granular security controls, such as multi-factor authentication, device authentication, approval workflows, JIT access, and IP address whitelisting, are all supported.

• Administrators can quickly and easily generate an audit on every use of every key.

• Cryptographic keys always remain secured in a centrally-managed hardware security module (HSM).

Fast

• Sub-second digital signatures are made possible through a client-side hashing architecture.

• Hosted on customer-managed infrastructure, GaraSign can be rapidly deployed on-premises, in the cloud, or in a hybrid environment.

• Support for Single-Sign On (SSO) using existing identity providers, resulting in fast adoption.

Easy

• Administration is performed from a single pane of glass, simplifying privileged access management.

• A multitude of native client integrations allows customers to use the same tools they use today.

• Supports many protocols and use cases, including SSH, TLS, VPN, RDP, S/MIME, GPG, PDF Protection, File Encryption, and more, without requiring application modification or reconfiguration of servers.

Garantir is a cybersecurity company that provides advanced cryptographic solutions to the enterprise. The Garantir team has worked on the security needs of businesses of all sizes, from startups to Fortune 500 companies. At the core of Garantir's philosophy is the belief that securing business infrastructure and data should not hinder performance or interrupt day-to-day operations. With GaraSign, Garantir's flagship product, private keys remain secured at all times, without limiting the performance of cryptographic operations, including code signing, SSH, S/MIME, document signing, TLS, secure backup, and more.

Garantir

1041 Market Street #302
San Diego, CA 92101
(858) 751-4865
https://www.garantir.io