ManageEngine

PAM360

Privileged access management 101: A comprehensive guide to building a sound PAM strategy for your enterprise

www.manageengine.com/pam360

Privileged access management (PAM) refers to a set of IT security management principles that help businesses isolate and govern privileged access, control who can be given what level of administrative access to which endpoints, and monitor what authorized users do with that access.

Before discussing privileged access management as a security discipline, its importance, and the implementation measures, let's return to the basics. First, we'll define what privileged access means, and then learn more about securely managing privileged access.

What is privileged access?

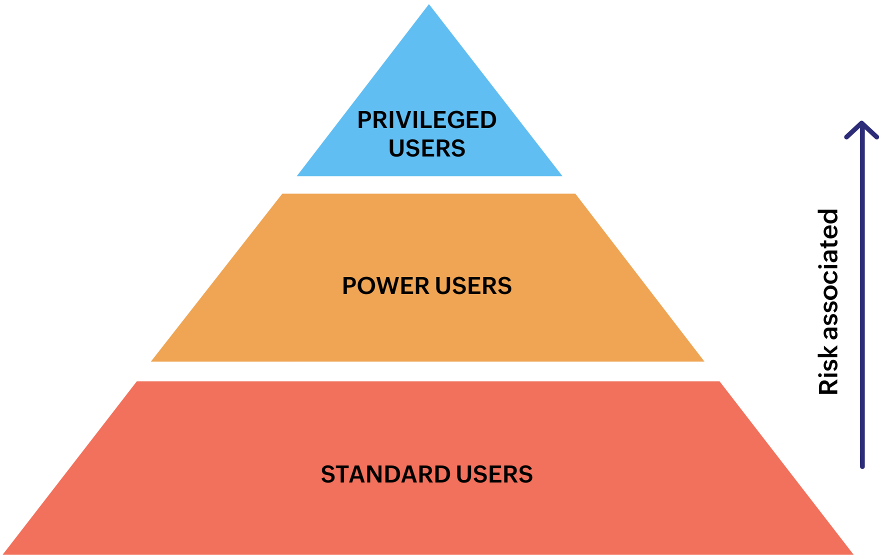
Privileged access, broadly speaking, is a type of IT system access that grants special rights to the access holder. Users with privileged access can execute actions that a standard user cannot. Actions that generally qualify as privileged operations include the ability to modify server settings, access business data systems, install a new program, run critical services, add user profiles, conduct maintenance activities, or alter network configuration. Today's enterprise IT teams largely rely on critical user accounts, called "privileged accounts" to delegate users with privileged access to various information systems in the network.

While privileged accounts remain the top choice for privileged access provisioning in the current IT scenario, other rarely used options include biometric authentication and smart cards. In some cases, organizations completely secure a physical server, a workstation, a data center device, or any system that has sensitive information, and prohibit direct access to the machine. In such circumstances, direct physical access to the machine will mean that the user has privileged access.

Who is a privileged user?

Users who are authorized for elevated access to part of or the entire IT infrastructure network—via possession of one or more privileged accounts or any other mode—are called "privileged users." Commonly known privileged users include IT workers like system administrators, network architects and administrators, database administrators, business application administrators, DevOps engineers, and other IT heads. At times, a third-party contractor helping out with a firm's IT operations, or liaising for business requirements and maintenance, may also have inside access to the firm's network. Typically, privileged users are a specific type of enterprise IT user.

Other IT users include standard users and power users.



Types of enterprise IT users

Standard users: These are regular users who have non-powerful accounts to access business applications on a daily basis to perform routine operations. Standard users normally do not have access to any sensitive information systems.

Power users: Power users have some additional permissions compared to standard users. A common example is the in-house IT staff who helps out with end-user workstation management. Such users receive a marginal account access elevation, which provides them with specific permissions, like remote access to local workstations and databases, so they can be termed power users.

Privileged users: These are your all-important users. Privileged users are usually limited in number. They carry the highest risk to an IT environment and require 24/7 surveillance.

Privileged access management is the process of entrusting selective users with the least required privileged access that their job warrants by securely sharing specific privileged accounts with them. It also involves continuous monitoring of the privileged users to ensure they do not misuse their access rights. This requires regular review of assigned privileges and revoking excessive rights whenever a user's role in the organization changes.

Why is privileged access management important for enterprises?

Because privileged access to a critical information system is the crown jewel in a cyberattack, a privileged user account in the wrong hands is a deadly weapon that can easily bring down an enterprise.

Unchecked privileges are a silent threat to today's businesses. In fact, the 2019 Thales Data Threat Report ranked privileged access as one of the top five factors in its "Greatest Data Security Threats" list. Additionally, a 2019 report by Verizon states that privileged access misuse is at the root of most security incidents and data breaches across industries. Furthermore, it is also one of the most difficult attack vectors to discover; some breaches resulting from privilege misuse can actually go undiscovered for months or more.

Poor management of privileged access and user accounts can expose enterprises to the following perils:

1. Exploitation of unsuspecting employees by hackers:

Privileged user accounts are a favorite among attackers looking to gain full access to sensitive data servers without attracting suspicion. Hackers usually manipulate gullible, esteemed users (with phishing, spoofed websites, and other tactics) into giving up information that allows the attacker to circumvent the firm's security and gain network access. Once inside, hackers immediately prowl around for unmanaged privileged credentials and escalate themselves to domain administrator status, which provides them with unrestricted access to highly sensitive information systems. The best way to tackle this threat is to completely lock down all privileged credentials in a central, encrypted vault, enforce role-based controls, mandate multi-factor authentication for vault access, and log all incoming requests.

2. Privilege abuse by rogue insiders:

At times, the biggest threats are the ones that are closer to home. Likewise, insider privilege misuse is a rapidly growing concern today in organizations of all sizes. The Cybersecurity Imperative Pulse Report released in June 2019 by ESI ThoughtLab states that "the impact from malicious insider threats has doubled, with 57 percent of the surveyed firms now citing a large or very large impact, versus 29 percent in our 2018 survey." Internal privileged users with the wrong intentions for personal gain can cause more damage than external parties. The inherent trust placed in insiders enables them to take advantage of their existing privileges, siphon off sensitive data, and sell it to a external party without getting noticed until it is too late.

The 2019 Insider Threat Report by Verizon notes that, over the firm's previous five Data Breach Investigation Reports (2014-2018), only 4 percent of insider privilege misuse breaches were uncovered. To protect critical information assets from such malicious internal actors, it is vital to constantly monitor every privileged user's activities in real time, and leverage behavior anomaly detection and threat analytics.

3. Hazardous practices by negligent employees:

Careless employees are a difficult threat to manage without proper privileged access management. These are users who do not understand the significance of cybersecurity. They recklessly leave critical user credentials lying around for hackers to find, or sometimes share their access privileges with unauthorized employees. A typical example is DevOps engineers dumping their codes (which contain authentication tokens for internal servers) on open platforms like GitHub and forgetting about them. Such dangerous practices can be controlled only by robust privileged access governance that ensures, with comprehensive auditing, that every privileged activity is accountable to a certain user.

4. Remote vendors and ex-employees abuse their rights:

Remote vendors make up the extended business network of an organization. They usually include contractors, consultants, partners, third-party maintenance teams, and service providers who require privileged access to your internal infrastructure for a variety of business needs. Almost every organization depends on multiple contractors to get work done. In today's digital world, this means third-parties have access to your internal network for business requirements, and therefore pose as equal a threat as insiders. Another external insider who presents the same risk is an unhappy or financially motivated ex-employee. Disgruntled employees who have moved on from the firm but still posses access rights can leverage them to carry out illegitimate access, steal data, and sell it to hackers. Handling such threat scenarios requires a regular review of employees' and contractors' privileges, and removing needless rights.

5. More privileges than necessary:

More often than not, users are over-privileged, i.e. they have access rights that are far more than what they need to perform their job duties. As a result, there is a gap between granted permissions and used permissions. In such instances, it's important to apply the principle of least privilege—providing only the minimum required permission to complete a work task. Without a proper privileged access management system to enforce least privilege security and monitor user actions, over-privileged user accounts can be leveraged for illegitimate access.

6. Privileges, once granted, are never rescinded:

Forgotten privileges are dangerous. IT administrators often provision users with privileged access to data servers and then fail to revoke them. Without a tool to track who has been given what privileges, retracting permissions can be a cumbersome task. This means users continue to hold privileges even after their job is done, and they have the opportunity to execute unauthorized operations. In this case, a privileged access management tool can help IT managers delegate the least required privileged access for users with timing presets. Once the stipulated time is up, the tool revokes the privileges automatically.

7. No clear track records when an investigation is called for:

This is a subtle threat that can emerge as a huge disadvantage in case your organization undergoes a data breach. Without comprehensive privileged activity logs and clear evidence that can provide context to the incident in question, forensic investigations can fail and, in turn, destroy the trust and brand reputation you have built with your customers.

Privileged access, unless completely managed with powerful controls and constantly monitored, can subject your organization to the risk of data overexposure and consequently result in business disruption, lawsuits, investigation costs, and reputation damage. Like Gartner says, **privileged access management should be one of your top long-term security projects** to eliminate weaknesses in your cybersecurity posture and successfully neutralize emerging privileged access risks .

Common best practices to include in your privileged access management program.

Privileged access management best practices can be classified into three phases: before, while, and after provisioning privileged access to a certain system.

1. Security best practices to follow before delegating privileged access

The privileged access management agenda before providing access typically begins with taking stock of active critical endpoints across on-premises, cloud, and virtual platforms in your network. Upon asset discovery, the next step is consolidating the associated privileged accounts and SSH keys (or any user authentication entity that provides elevated permissions such as smartcards) in a secure, central vault. This vault must be protected with multiple layers of encryption with military-grade algorithms like AES-256 or RSA 4096. Other measures include:

- Validating vault login requests before approving them by cross-checking with user profiles in the in-house identity governance, and provisioning service to ensure the concerned user's role necessitates privileged access.
- Enforcing multiple layers of strong authentication for vault login, including one-time passwords (OTP), two-factor authentication (2FA), and single sign-on (SSO).

- Enabling a user to check out a privileged account or other credential only upon approval by IT managers or IT admins.
- Imposing time-based access restrictions on the checked out credential, which enables automatic revoking of delegated permissions after a specific period.
- Logging all credential requests with a time stamp.

2. Security best practices to follow while delegating privileged access

Next, while assigning a party with privileged access, the chief principle is to enforce the least privilege model built upon role-based controls. This ensures that the user, who has already proved their identity with multiple authentication levels, is provisioned only the minimum amount of rights needed. This usually means implementing the following measures:

- Tunneling privileged sessions through gateway servers and encrypted channels to avoid direct connection to the target information systems from the user device. To enhance security further, enable users to log in to the privileged access management solution and launch privileged connections with a single click upon which the tool authenticates the user in the background. This practice bypasses the need to disclose the privileged credentials to the user.

- Using ephemeral certificates to authenticate and authorize privileged sessions. They are automatically generated and provisioned during privileged access so users don't have to input the credentials while connecting, and automatically expire after the session is complete.

- Supplying limited privileges, such as application-specific access permissions during an RDP session, or allowing only certain commands in an SSH terminal session.

- Enforcing just-in-time (JIT) elevation controls. Elevating privileges for employees only when required can help prevent the buildup of unused or unneeded access rights, reducing risk. JIT controls enable users to log in as themselves instead of relying on a shared privileged account, which greatly increases accountability. This method is also referred to as privilege elevation and delegation management. For an ideal JIT least privilege model, you can set up a privileged access management system that interfaces with your in-house identity governance tool. This coalescent structure can make implementation easier with role-based controls.

- Record all privileged sessions, and archive them as video files. It is also beneficial to simultaneously oversee ongoing sessions—either manually or automatically—to detect any anomalies in real time such as the passing of malicious commands.

3. Security best practices to follow after delegating privileged access

The foremost thing to remember in this phase is that after the job is done, privileged access should be revoked. Once permissions are rescinded, the privileged credential—password or SSH key, should also be automatically checked back in to the vault and immediately reset using strict policies to ward off any unauthorized access in the future.

Additional initiatives for solid security are as follows:

- It is imperative to implement a comprehensive privileged user activity logging capability as part of your privileged access management program. The audit trails should instantly capture all events around privileged account operations, user logon attempts, workflow configurations, and task completion, along with a time stamp and an IP address. Integrating your privileged access auditing platform with your

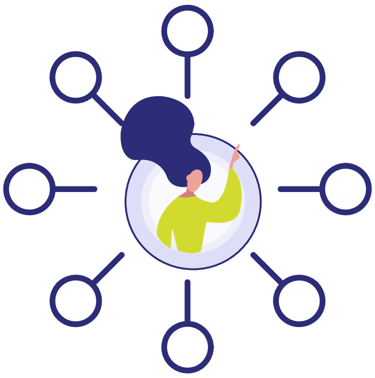
- in-house event logging service can help correlate endpoint and privileged access data. This gives your IT teams a consolidated dashboard for mapping privileged access with overall system operations, increasing visibility, and situational awareness about privileged user monitoring. The combined logs give you more context, which can aid in decision-making while responding to security incidents within the network.

- Tie in artificial intelligence (AI) and machine learning (ML)-driven anomaly detection to identify threats from unusual behavior. An effective privileged access management tool should help spot hidden threats even before they take shape. For a more proactive stance, make your privileged access management solution work with anomaly detection capabilities. Establish a baseline behavior for privileged operations in your network, and then leverage new-age AI and ML technologies to incorporate risk scoring for every user action. This enables the tool to pick up outliers based on location, time, or role, using them to calculate a weighted risk score. When an action's risk score is higher than the norm, automated alerts to IT admin can help you stop any potentially harmful activity right in its tracks.

- Leverage blended analytics for intelligent risk insights affecting business. Audit logs are most useful when studied by an advanced analytics platform that presents insights based on all the facts at hand. Similarly, your privileged access audits and reports can offer better insights when you correlate them with business services. For instance, mapping privileged access requests raised in your privileged access management tool to network issues or incidents in your IT service desk can offer a deeper understanding of what's going on within your environment, enabling meaningful inferences and quicker remedies.

What are the top benefits of a robust privileged access management program?

Life cycle management of privileged access in an organization includes secure credential vaulting, granular access controls, approval workflows, continuous monitoring of users with authorized privileges, regular review of assigned privileges, and behavior analytics. Proper life cycle management thwarts risks and provides the following benefits:



Central control

As enterprise infrastructure setups continue to expand, it is crucial to implement strategic controls at a macro-level. Privileged access management can help establish complete authority over your high-value assets, and hold a tight rein on privileged access provisioning.

Clear accountability

Make privileged access subject to the approval and review of managers. Leverage clear usage-tracking by associating every access request with a valid user profile; trace administrative operations back to privileges exacted through multiple shared accounts.

Maximum visibility

Discourage casual use of privileged accounts for routine tasks by recording activities as time-based logs. Provide a credible knowledge base with valuable information to incident response and control teams, helping mitigate insider threats and the exploitation of privileged access.

Meet compliance audits

Prove compliance with privileged access control standards set by the GDPR, NIST, FISMA, HIPAA, SOX, PCI DSS, NERC CIP, ISO/IEC 27001, CCPA and other regulations. Produce audit-ready compliance reports that relay privileged access management best practices adhered within your organization.

Safeguard brand reputation

Adopt a proactive security posture. Improve resilience against focused cyberattacks, and shield your enterprise from reputation damage and substantial financial losses. Build confidence among your customers, and run your business without disruption.

www.manageengine.com/pam360

4141 Hacienda Drive Pleasanton,
CA 94588, USA
US +1 888 204 3539
UK : +44 (20) 35647890
Australia : +61 2 80662898
www.manageengine.com/pam360

ManageEngine
PAM360