ManageEngine
PAM360

An IT admin's guide to privileged account governance

Keep your business safe from privilege misuse and insider threats by securing your privileged accounts.

www.manageengine.com/pam360

Privileged account management is the part of privileged access management (PAM) that deals exclusively with the protection of privileged accounts in an enterprise, including those of operating systems, databases, servers, applications, virtual machines, and networking devices.

In this guide, we will cover:

- An introduction to privileged accounts.
- What privileged account management is.
- Why privileged account management is important for organizations.
- Business benefits of privileged account management.
- Best practices for effective privileged account management.

What is a privileged account?

The term privileged account includes the most powerful accounts spread across an IT environment, such as the UNIX root, Windows administrator, database administrator, and even business application accounts. These accounts are normally used by information and communications teams to set up the IT infrastructure, install new hardware and software, run critical services, and conduct maintenance operations. In short, privileged accounts are master keys that can access an organization's highly classified IT assets along with the sensitive information stored within them.

Types of privileged accounts

Local or built-in administrator accounts are accounts on member servers and clients that grant absolute control over their hosts. This also includes the default login accounts that come built in with operating systems, application software, and services. If local administrator passwords are weak, left unchanged, or repeatedly used on multiple accounts across hosts, malicious users could easily gain unauthorized access to workstations.

In the worst-case scenario, an attacker with access to a local admin account or a forgotten built-in system account could navigate across the network and even elevate their privileges to that of a domain administrator.

Domain administrator accounts are powerful accounts with the widest range of control over every object in a domain. These accounts provide administrative privileges on all workstations, servers, and domain controllers. Only a few, trusted administrators should use domain administrator accounts. On top of this, they should only use the account to log on to the domain controller systems that are as secure as the domain controllers themselves, especially in a Windows ecosystem.

Administrative service accounts are privileged accounts used by system programs to run application software services or processes. At times, these accounts may possess high or even excessive privileges when a certain dependent service requires it. This also goes for local or domain Windows accounts used to run Scheduled Tasks. Typically, such service account passwords are set to never change due to the difficulty in discovering all dependent services and propagating the password change, which could, in turn, delay business service continuity. However, static service accounts can make your enterprise an easy target for hackers.

Root accounts are superuser accounts that carry administrative privileges to manage Unix and Linux resources, which are typically used by system administrators to perform core IT operations. Root accounts have unrestricted access to all files, programs, and other data on a system, and therefore pose an enormous risk when mismanaged.

Application accounts are accounts used by organizations to automate communication between various applications, web services, and native tools to fulfil business and other transaction requirements. Application credentials are usually embedded

in clear text within unencrypted application configuration files and scripts to achieve this business communication interfacing.

Embedded application accounts are used in many DevOps environments where credential hard-coding is commonly followed to expedite software development phases and automate service delivery cycles. Administrators usually find it difficult to identify, change, and manage these passwords. As a result, the credentials are left unchanged, which makes them an easy entry point for hackers.

Why privileged account management is an essential component of your security infrastructure

In the wrong hands, a privileged user account is a deadly weapon that can easily bring down an enterprise. Lax management of privileged user accounts can expose enterprises to the following security risks:

1. Privileged accounts are one of the top targets of hackers who are looking to gain unrestricted access to a corporate network. The 2020 Data Breach Investigations Report by Verizon states that use of stolen or lost credentials is the second leading method employed by hackers among the breaches included in the study. Past high-profile data breaches, such as the OPM hack or Three UK attack revealed that hackers used compromised employee credentials as entry points. In fact, a recent security breach that the hotel chain Mariott suffered was also the cause of stolen privileged credentials.

Hackers usually use methods like spear-phishing, malware distribution, and credential stuffing to steal weak or overlooked credentials. They then leverage the stolen identity to enter the network, establish persistence, and laterally move across systems unnoticed, siphoning off sensitive information such as customer records without raising an alarm.

2. Aside from external threat actors, malicious insiders and careless employees pose a serious risk to privileged account security. In fact, the insider threat is perhaps the biggest peril organizations face in terms of privilege misuse and unauthorized actions, because it's the hardest to detect since firms inherently trust their workforce. Rogue employees are normally those who are underappreciated at work, have been slighted or disrespected, or have joined forces with an external party for monetary gain.

Negligent employees are the other set of insiders whose reckless practices, like openly sharing credentials with colleagues and leaving password files unattended, can eventually lead to cyberattacks and corporate data exposure. It makes matters worse when that careless employee is a system administrator who has too much access and shares that access with others without limitations.

With the majority of today's enterprises around the world riding the digital transformation wave and investing heavily in IT infrastructure expansion, privileged account proliferation is inevitable. As IT environments become overrun with privileged account credentials, it's important to institute a comprehensive privileged account management program to avoid password fatigue among employees, adopt a disciplined approach to privileged account protection, and mitigate cyberattack risks.

Business benefits of privileged account management

The cybersecurity benefits that a robust privileged account management solution delivers are:

Centralized management

Take complete control of privileged accounts by storing them in a secure repository with a single access point fortified with multi-factor authentication.

Reduced risk exposure

Shrink the attack surface and effectively combat growing risks of external attacks, identity theft, and insider threats.

Improved incident response

Establish security controls to detect and prevent privileged account misuse through approval workflows and real-time alerts.

Enhanced security and compliance

Effectively prove compliance with various industry and government regulations, like HIPAA, PCI DSS, the GDPR, NERC-CIP, SOX, and more.

Increased visibility

Acquire a comprehensive overview of privileged account activity across the network with extensive audit logging and informative reports.

Automated cybersecurity

Boost IT productivity by relieving IT teams of time-consuming manual tasks such as bulk password updates using automation schedules.

Best practices for effective privileged account management

- Maintain a complete list of all active privileged accounts in your network and update that list whenever a new account is created.
- Store privileged identities like passwords, SSH keys, and SSL certificates in a secure vault using standardized encryption algorithms such as AES-256.
- Enforce stringent IT policies that cover password complexity, frequency of password resets, strong SSH key pair generation, time-limited access to privileged accounts, automatic reset upon one-time use, and other robust controls.
- Share privileged accounts with employees and third-party users in a secure way, such as granting privileged access with the minimal permissions required to carry out the job.
- Audit all identity-related operations such as privileged user logins, password shares, password access attempts, reset actions, and so on.
- Monitor and record all privileged user sessions and activities in real time.

ManageEngine PAM360

ManageEngine PAM360 is a complete privileged access management solution for enterprises. It enables IT administrators and privileged users to gain complete, granular control over critical IT resources, such as passwords, digital signatures and certificates, license keys, documents, images, service accounts, and more.

Recognized by Gartner and Forrester as one of the top PAM vendors of 2020, ManageEngine PAM360 includes contextual integrations with SIEM, ticketing, and analytics solutions to help IT teams build user behaviour models to identify and terminate anomalous activities, generate comprehensive audit and compliance reports, and make data-driven security decisions.

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