netwrix

INFOGRAPHIC

HISTORY OF PRIVILEGED ACCOUNT MANAGEMENT

How we got to where we're today and why **Zero Standing Privilege** through **Just-in-Time** privilege elevation is the future.

START

WHAT IS PRIVILEGED ACCOUNT MANAGEMENT (PAM)?

Privileged Account Management (PAM) is a system or technology that is responsible for controlling the access, actions, and permissions for users that hold elevated (or privileged) accounts. Simply put, the more access an account has, the more security you want on that account.

Let's take a look at how PAM has evolved over the years, why this might have exacerbated the problem, and see what's in store for the future.

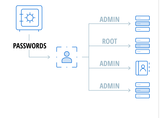
2002

Privileged ACCOUNT Management

GEN 1 - PASSWORD VAULTING

Privileged Account Management, also known as Shared Account Password Management (SAPM) became mainstream early in the millennium, 2002-2003. The objective was managing the change and release of super user accounts such as Administrator on Windows or Active Directory, and root on Unix and Linux.

- Legislative compliance
- Privileged accounts rotated on a schedule
- Granular access control



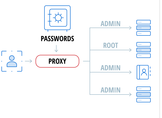
2012

Privileged ACCESS Management

GEN 2 - PROXY SERVERS

Proxy servers allows administrators to access high-value assets securely without knowledge of the password.

- The vault passes the password of the super user account directly.
- User never gets exposed to the password.
- Able to record all session data.
- Supports secure network segmentation.



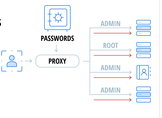
2014

Privileged ACCESS Management

GEN 2 - DEDICATED ADMIN ACCOUNTS

More recently, Microsoft Best Practice Deployments recommended administrative account separation.

- Unique accounts for each user to separate everyday tasks from admin tasks.
- Administrator and root accounts used only for "break-glass" access.

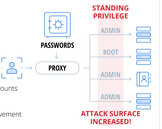


TODAY

THE PROBLEM WITH PAM

Because all privileged accounts are essentially controlled via the same vault and access policy, the use cases between super user accounts and personal admin accounts have combined, blurring the distinction between Privileged Account Management and Privileged Access Management.

- Increased attack surface from additional accounts and standing privileges.
- Privileged accounts vulnerable to lateral movement attacks (e.g. left behind Kerberos ticket).
- Overly complex access control rules.



TODAY AND MOVING FORWARD

A different approach

Netwrix Privilege Secure

Break-glass use case

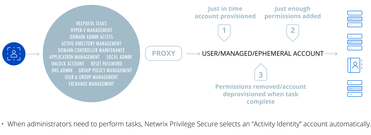
KEEP SUPERUSER ACCOUNTS SEPARATE

- PAM may be carried out via any existing password vault with limited access.
- If an existing vault is in place use it just for password rotation.
- Free solutions such as Microsoft LAPS may be used for predominantly Windows/Active Directory environments.

For day-to-day

ACTIVITY-BASED ACCESS CONTROL

For day-to-day administrative tasks, Netwrix Privilege Secure for Access Management provides a secure mechanism to get Admins from A to B without the usual privileged account overhead or complex access policies.



- When administrators need to perform tasks, Netwrix Privilege Secure selects an "Activity Identity" account automatically.
- Netwrix Privilege Secure adds permissions specific to the task.
- User is connected to a selected server to perform the task - all activity is recorded for later playback.
- Once task is completed, all permissions are removed. **No privileged attack surface is left behind.**

ELIMINATE PRIVILEGE ACCOUNT SPRAWL

With constant scanning, Netwrix Privilege Secure for Discovery helps you identify unmanaged or unknown privileged accounts, putting a halt to attackers' lateral movement within your environment by disabling unnecessary accounts.

- Discover your blind spots in minutes - Scan tens of thousands of endpoints within minutes, identifying potential entry points for attackers. Continuous scanning ensures that account sprawl won't be an issue.

- Enforce Zero Standing Privileges - Remove unnecessary administrative accounts from all endpoints in just one click, slashing the risk of malware installation or unauthorized changes to critical security settings.

- Maintain an overview of your attack surface - Utilize tailored dashboards for executives and IT professionals to visualize, analyze, and manage your environment. View all accounts and activities to stay informed about privileged actions.

LOCKDOWN ENDPOINT PRIVILEGE

With Netwrix Endpoint Privilege Manager, you can secure your endpoints, to prevent the risk of malware, ransomware, and non-compliance. By delegating only the necessary permissions to standard users, rather than providing local admin rights, you can mitigate these risks effectively on a day-to-day basis.

- Safeguard Windows endpoints from ransomware and malicious changes - Prevent users from installing unapproved software and control their usage of removable storage. Protect application settings from both malicious and unintentional changes and verify the correct deployment of Group Policy settings.

- Boost productivity wherever work is done - Deploy software and custom OS settings to any Windows endpoint, including domain-joined, MDM enrolled, or virtual devices. Consolidate Group Policy objects (GPOs), automate scripts, streamline VPN management and more.

- Modernize your desktop environment - Manage and secure your on-premises, hybrid, or remote desktop environment using a single solution.

NETWRIX PRIVILEGE SECURE BUNDLING OPTIONS

	Privilege Secure for Discovery	Privilege Secure for Access Management	Privilege Secure for Access Management Enterprise	Endpoint Privilege Manager	Privilege Secure Complete
Continuous discovery	●		●		●
Privilege Visualization	●		●		●
Remediate Privilege Sprawl	●		●		●
Access Control		●	●		●
Session recording		●	●		●
Account lifecycle management		●	●		●
Credential management		●	●		●
Access Certification		●	●		●
Desktop Activity launch		●	●		●
Endpoint least privilege control				●	●
Modern endpoint management				●	●

CONCLUSION

Most Privileged Account Management (PAM) vendors typically just focus on controlling access to managed privileged accounts such as Domain Admin and local server Administrator. While this approach provides just-in-time access for system administrators, the accounts still retain their privileges while not in use (also known as standing privileges) resulting in a widespread attack surface that easily be compromised using modern attack techniques; this situation is compounded as organizations assign more managed accounts to each administrator. Furthermore, many PAM vendors have engineered their products around password vaults rather than treating the vault as a component of the overall solution. This results in unnecessary complexity.

THE IDEAL SOLUTION

JUST-IN-TIME TASK-BASED APPROACH

Provides the exact level of privileges needed, exactly when they're needed, for only as long as they're needed.

SCALE-OUT ARCHITECTURE

Economically viable to deploy and priced in a clear manner that is easily understood.

COMPLEMENTS INCUMBENT SOLUTIONS

Compatibility with existing solutions for out of the box value and faster ROI.

ACTIVELY REDUCES ATTACK SURFACES

Removes artifacts commonly used to compromise accounts or reduces Standing Privilege.

LOCKS DOWN DOMAIN ADMINISTRATIVE PERMISSIONS

For Active Directory

Learn more or request One-To-One Demo

Corporate Headquarters: 6160 Warren Parkway Suite 100, Frisco, TX, US 75034

Phone: 1-949-407-5125 **Int'l:** 1-949-407-5125 **Toll-free:** 888-638-9749 **EMEA:** +44 (0) 203-588-3023 netwrix.com/social

Copyright © Netwrix Corporation. All rights reserved. Netwrix is trademark of Netwrix Corporation and/or one or more of its subsidiaries and may be registered in the U.S. Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are the property of their respective owners.