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.

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.

START

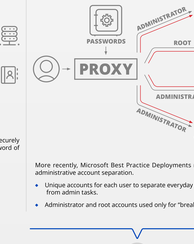
2002

Privileged ACCOUNT Management

GEN 1 - PASSWORD VAULTING

Privileged Account Management, also known as Shared Account Password Management (SPAM) 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

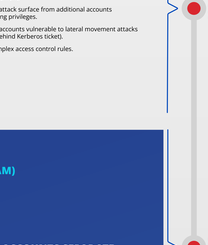
GEN 2 — PROXY SERVERS

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.

Privileged ACCESS Management

GEN 2 — DEDICATED ADMIN ACCOUNTS

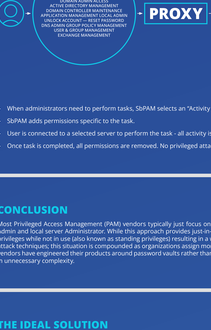


More recently, Microsoft Best Practice Deployments recommended administrative account separation.

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

2014

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.

2018

A different approach

STEALTHBITS PRIVILEGED ACTIVITY MANAGER (SbPAM)

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.

СЬОГОДНІ І В МАЙБУТНЬОМУ

For day-to-day

ACTIVITY-BASED ACCESS CONTROL

For day to day administrative tasks (Privileged Access Management), SbPAM 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, SbPAM selects an "Activity Identity" account automatically.
- SbPAM 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.

CONCLUSION

Most Privileged Access 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

ГОЛОВНІ ПЕРЕВАГИ NETWRIX sbPAM

EPHEMERAL PRIVILEGED ACCOUNTS

ACCESS APPROVAL AND CERTIFICATION

SESSION MONITORING AND RECORDING

CLEANUP OF PRIVILEGED ACCESS ARTIFACTS

SERVICE ACCOUNT MANAGEMENT

ZERO TRUST PRIVILEGED ACCESS

HOW IS NETWRIX sbPAM DIFFERENT?

ZERO STANDING PRIVILEGE

Other privileged account management solutions attempt to slap band-aids on the inherently risky approach of using standing admin accounts. With Netwrix SbPAM you can minimize your attack surface by replacing standing privileges with on-demand accounts.

LOW TOTAL COST OF OWNERSHIP

Save time and money with a solution that installs in minutes and typically runs on existing infrastructure. Everything you need is included in one reasonable license — you won't face extra fees for add-ons for databases, appliances, proxies, high availability or other common needs.

LEVERAGE THE INVESTMENT YOU'VE ALREADY MADE

Keep using the tools you know, such as RDP/SHH clients, Local Administrator Password Solution (LAPS) or your current password vault, but make your processes more secure by integrating these products with Netwrix SbPAM.

LEARN MORE AT NETWRIX.COM

IDENTIFY THREATS. SECURE DATA. REDUCE RISK.

Stealthbits Technologies, Inc. is a customer-driven cybersecurity software company focused on protecting an organization's sensitive data and the credentials attackers use to steal that data. By removing inappropriate data access, enforcing security policy, and detecting advanced threats, our highly innovative and infinitely flexible platform delivers real protection that reduces security risk, fulfills compliance requirements, and decreases operational expense.