Protecting Your Most Dangerous Accounts: Where Are You On the 5-Tier Privileged Account Management Maturity Model?

BY RANDY FRANKLIN SMITH

Table Of Contents

INTRODUCTION

Privileged accounts are both a blessing and a curse.

Sure, privileged accounts provide elevated access to data, applications, and systems so that users can accomplish work-related tasks. But when used improperly, the accounts can be repurposed as part of espionage, data exfiltration, and ransomware attacks. Today, privileged account protection is more important than ever as threats leveraging privileged accounts in one form or another grow at an alarming rate.

Over the past year, the use of stolen credentials was the number one threat action in all data breaches[1]. The IT industry has seen a 102% increase in malware volume[2] in the first half of 2018, compared with the same period last year. The likelihood of infection rises with the presence of elevated accounts (privilege is needed to successfully install malware), as does the ability for lateral movement within an organization. Similarly, the industry experienced a 229% increase in ransomware[2] in the first half of 2018, compared with the same period last year. Some of the newest variants, such as GrandCrab, leverage SMB exploits to move laterally across unpatched machines and encrypt as much data as possible.

In each case, the more availability that cybercriminals have to privileged accounts, the easier it is for them to successfully infect, infiltrate, and laterally move across your organization while searching, locating, and either encrypting or exfiltrating data.

Clearly, many IT organizations need to boost their privileged account security. *But what's the right way to manage privileged accounts?*

This paper looks at five ways that privileged accounts can be managed, discussing the pros and cons of each and helping you find an appropriate level of security around privileged account access.

Protecting the Privileged: BeyondTrust

Privileged access is a cyber risk for most organizations. Users are granted elevated access to data, applications, and systems, often with little regulation or accountability.

BeyondTrust's Password Safe offers secure access control, auditing, alerting, and recording for any privileged account, including shared administrative accounts, application accounts, local administrative accounts, service accounts, database accounts, cloud and social media accounts, devices, and SSH keys.

Look for insights from BeyondTrust throughout this paper, highlighting how to best manage privileged accounts.

[1]Verizon, Data Breach Investigations Report (2018)

[2]SonicWALL, Cyber Threat Report, Mid-Year Update (2018)

PRIVILEGED ACCOUNT MANAGEMENT AS A MATURITY MODEL

Organizations choose to manage their privileged accounts in many ways. This paper simplifies these approaches into five categories, presented as a Privileged Account Management Maturity Model:

The sequence of tiers closely follows the progression of privileged account management history the author has observed organizations implement over the years in response to changing technologies, growing compliance requirements and the increasing sophistication of attacks. The higher the tier, the more advanced the security tactics—and the more secure each privileged credential. As we move through each tier, you will note greater realization of the following goals:

- Limit access to each privileged account to as few users as possible
- Reduce the risk of improper use of privileged accounts by cybercriminals
- Increase accountability around the use of each privileged account

BeyondTrust Insights: How Are Privileged Accounts Really Being Used?

Most organizations focus on the accounts that individuals use. But privileged accounts can also be used by services, scheduled tasks, applications, SSH keys, and hard-coded scripts. Password Safe manages privileged accounts in all these forms, including the use case that is the focus of this paper: *users*

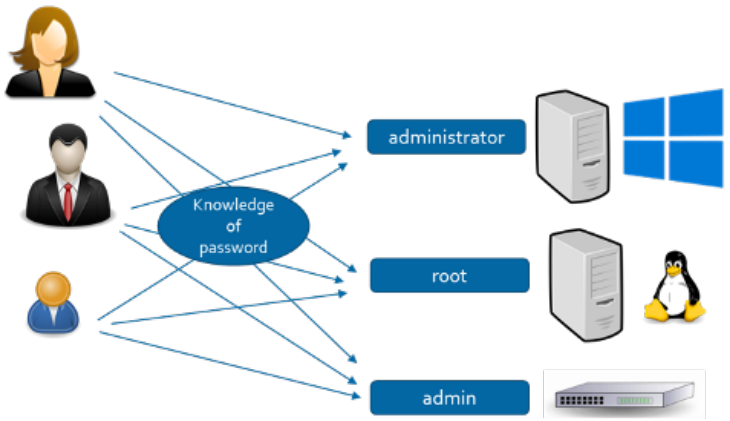
A few underlying risks apply to almost every tier of the maturity model. Consider these risks as you identify the appropriate model for your organization:

- **Credential artifacts get left behind:** Every time a privileged account is used to log on to a Windows system, artifacts are stored in the system's memory until it's rebooted. These artifacts can include cleartext passwords, password hashes, and Kerberos tickets—all of which cybercriminals can use for malicious purposes.
- **Keyloggers continue to be a threat:** Whether put in place by the user of a given endpoint or by a cybercriminal looking to compromise a privileged account, keyloggers pose a real threat in Maturity Model tiers where mandatory password rotation does not exist.

The remainder of this paper covers each tier of the Maturity Model in more detail. We believe the implementation of PAM/PSM Managing Dual Accounts is where organizations should be today to ensure IT efficiently supports business objectives while ensuring compliance and limiting the damage a rogue admin or outside attacker can cause.

SHARED BUILT-IN ACCOUNTS

Shared built-in accounts are the most common methodology for managing privileged accounts. As shown here, organizations have a limited set of privileged accounts (e.g., Active Directory *administrator*) and sparingly give out passwords to the necessary users, who have knowledge of account details appropriate to their role in the organization. You can extend this concept to organizations that have created a few shared administrative accounts (e.g., for services, backup, databases).



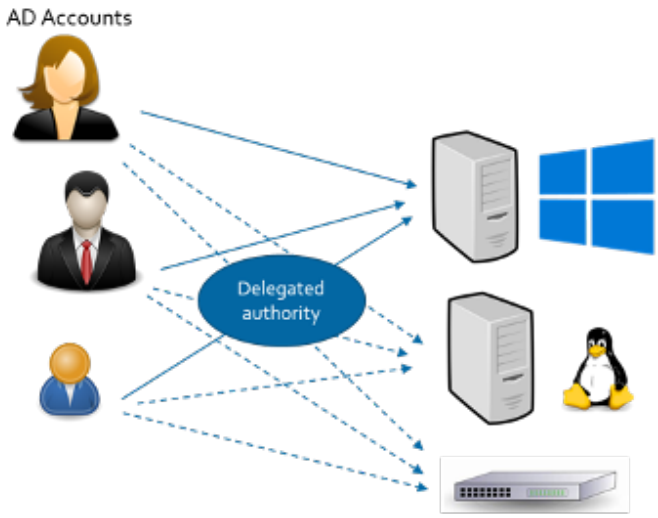
This tier of the Maturity Model presents a number of challenges:

- **Keeping track of who knows each password:** Tracking passwords is technically impossible in this tier, since you can't truly know whether or not someone has shared the password with another person.
- **Handling password change and distribution:** When a user is terminated or changes jobs, IT needs to update the password and disseminate it to the appropriate individuals to maintain proper security.
- **Keeping passwords secret:** In this tier, many people know the privileged account credentials. With an average of 49% of users sharing credentials , you should assume that your passwords are *not* a secret.
- **Accountability between admins:** Even when two or three IT pros have access to a privileged account, how do you know who logged in with that account, when they logged in, and what they did? Without some kind of logging system in place, there is zero accountability.
- **Frequent duplication of passwords:** IT pros are people, too. So, when it comes to privileged account passwords that are shared only by a chosen few and are used across multiple systems and services, the same password often ends up being used for multiple accounts.

The next tier in the Maturity Model applies the separation of users from built-in accounts.

INDIVIDUAL ADMIN ACCOUNTS

At this tier of the Maturity Model, each user that requires privileged access is given their own admin account with delegated authority, as shown here. This tier is just one step up from sharing built-in accounts, but it improves accountability, since each user now has their own account, and eliminates the need for users to utilize built-in accounts. On the "*nix" side of the house, it's important to have some form of Active Directory integration so that you aren't managing two sets of credentials.



However, several risks still accompany this tier of the Maturity Model:

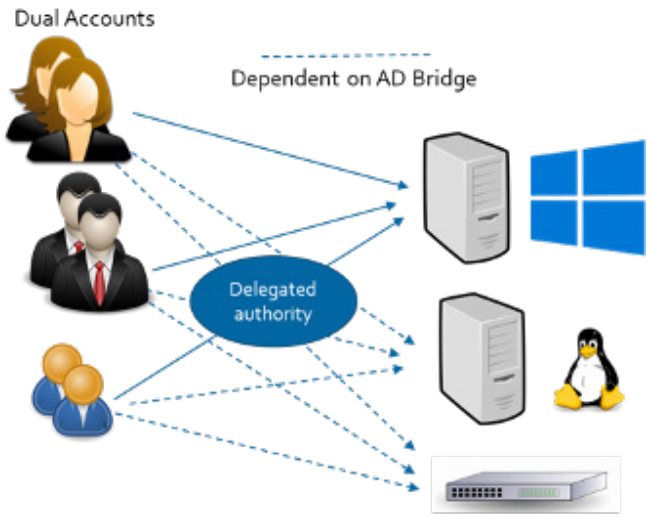
- **Admins always run with privilege:** With a "one user, one admin" type delegation, users tend to simply use their privileged account as their sole account. This leaves environments prone to accidents and creates the perfect environment for cybercriminals to find a foothold within the organization. (An already elevated account enables them to establish persistence on a compromised endpoint, and then move laterally within the organization.)
- **Privileged credential artifacts:** Every time a user logs on to an endpoint, artifacts are created and left on insecure systems.
- **Background processes running as current user:** When a logged-on user already has privileged access, attackers can leverage the user's credentials to launch malicious scripts to establish further footholds, ensure endpoint persistence, and move laterally—among other possible threat actions.

The next tier in the Maturity Model addresses the separation of users from privileged accounts.

[3]IS Decisions, Insider Threat Persona Study (2017)

DUAL ACCOUNTS WITH DELEGATION

This tier moves privileged account security further in the right direction. Users are given two accounts: one for low-level user tasks (e.g., browsing the web, using email, working in Office-type applications) and one for privileged tasks (e.g., managing a server, Active Directory). As shown here, the privileged account is still delegated authority over systems, as in the previous tier of the Maturity Model. However, the addition of the second low-level account (i.e. standard user account) helps improve overall security, since it conceptually removes the privileged account from constant use.

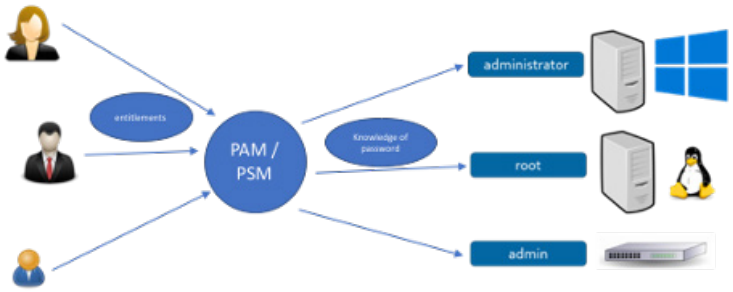


Although an improvement over the previous tier, dual accounts share the same issues around privileged credentials as individual admin accounts do when used on the same endpoint—specifically, issues around credential artifacts and background processes. These issues can be addressed by requiring privileged accounts to be used only on a Privileged Access Workstation (PAW): a separate, highly secured physical or virtual machine that is used specifically for privileged access.

The next step in the Maturity Model is to separate users from their unmanaged, continual access to a static privileged account.

PAM/PSM MANAGING SHARED ACCOUNTS

Privileged Access Management (PAM) and Privileged Session Management (PSM) solutions add a layer of security between the user and the privileged credential. PAM secures all privileged credentials in a vault, providing only approved credential access. As shown in the diagram below, users initially log in with a low-level account and then leverage PAM when they need to use shared privileged credentials (such as Active Directory's *administrator* account).



PSM further increases security by putting a layer between the user and the privileged session. By proxying access to the desired system and automatically logging in users with privileged credentials, PSM eliminates the user's need to possess the credentials at all.

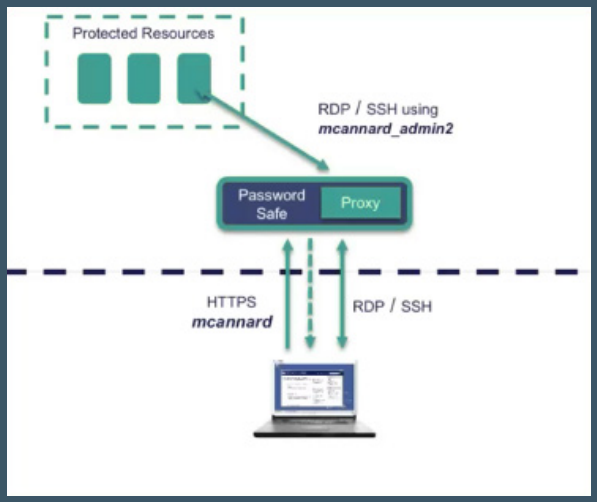
All of the risks mentioned for the previous tiers can be addressed through the introduction of PAM/PSM:

- **Eliminates persistent privileged access:** Because low-level users request privileged credential access, no user is continually logged in with privileged access.
- **Preserves unique privileged identities and a clean audit trail:** PAM dictates which users can utilize specific privileged credentials, making it possible to know exactly who has credential access.
- **Centralizes password storage and management:** Vault-based access of credentials eliminates the need to distribute passwords to approved users.
- **Enforces password security best practice across users and accounts:** PAM policy can require unique passwords, ensuring that no two accounts share a password. Password rotation can occur after each use, changing the password and nullifying the use of credential artifacts and background processes. The per-use rotation of a password can also ensure that it is known only to the next user of that credential.
- **Enforces password security best practices for applications and services:** PAM-based password rotation can include the updating of any services or applications to automate distribution of new passwords that meet the password strength, uniqueness, and other parameters as dictated by policy.
- **Reduces the threat surfaces, such as exploits from keyloggers:** Proxied privileged sessions remove the ability for cybercriminals to capture credentials with keyloggers.
- **Keeps passwords secret—even from the end users:** PSM furthers the security of the privileged credential by never presenting it to the requesting user, but simply providing the user proxied access to a remote session that has been logged on by using the requested credential.

The use of PAM/PSM can also eliminate the need for a PAW, if PSM is used to enforce human presence and off-device 2-factor authentication.

BeyondTrust Insights: Using Proxied Privileged Sessions

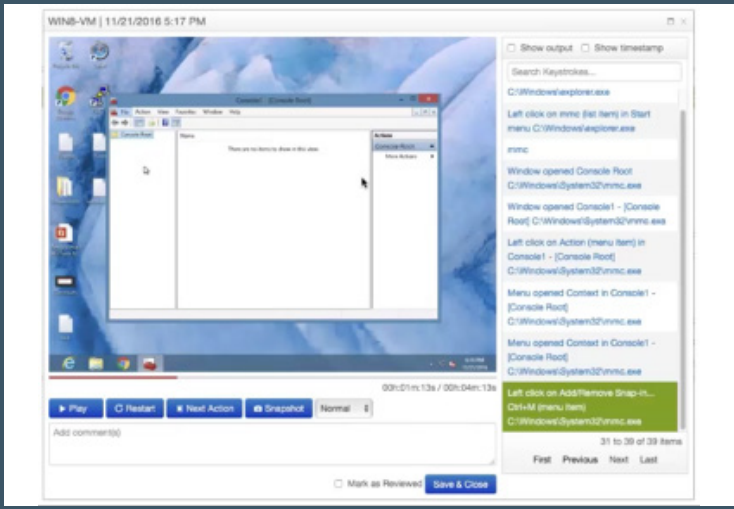
The most secure privileged environment is one in which passwords are never given out. By leveraging a proxied session between the user's endpoint and the protected system, privileged access can be provided without ever giving the user the password. Password Safe (shown here) uses credential injection when providing a proxied session, thereby eliminating the need for the user to be given the credentials. Instead, Password Safe establishes a session (complete with credentials), and the user is granted remote access to that session.



While this tier of the maturity model seems to solve every problem related to privileged access, it creates a problem around accountability. Once a user is logged on to a system with a privileged credential, native audit logs become opaque and provide no value in specifying the low-level user that leveraged the privileged account. You can still determine who did what by correlating system logs to PAM/PSM logs, but this approach becomes problematic when simultaneous sessions occur on a given system.

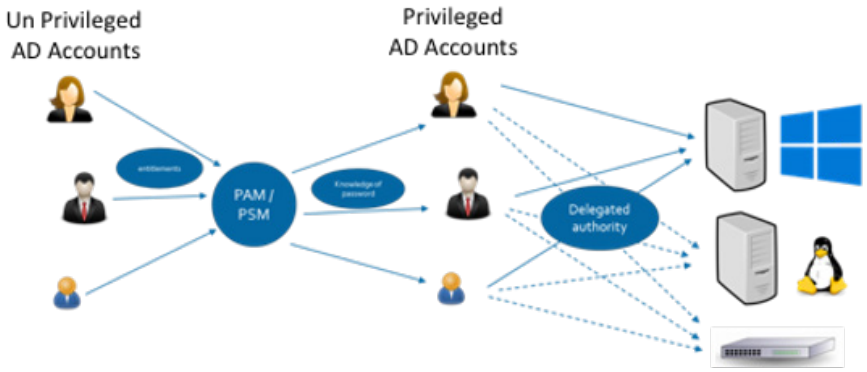
BeyondTrust Insights: Ensuring Accountability with Session Recording

Typically, accountability is established by using simple log data about which user accessed which privileged account and which system the account was used on. Although this approach provides an account-use audit trail, it fails to provide real accountability. Log data doesn't provide details about which actions were performed while the user was logged on. Password Safe's session recording creates an undisputable audit trail, complete with video playback and searchable session metadata.



PAM/PSM MANAGING DUAL ACCOUNTS

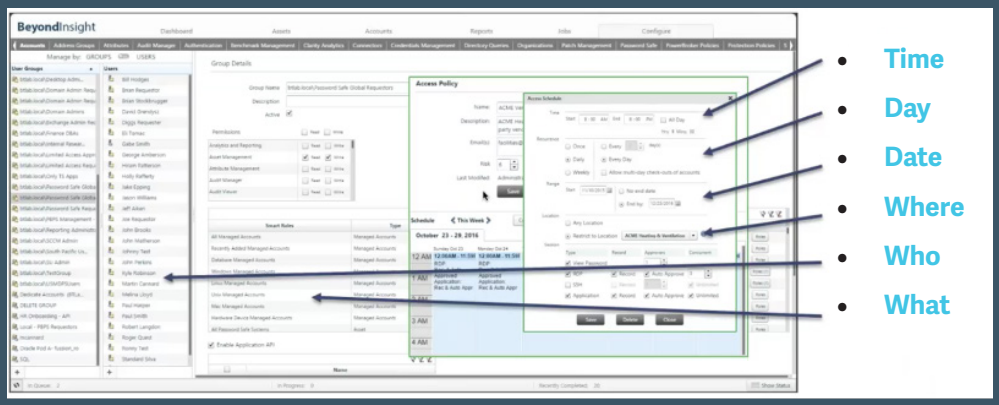
This tier mirrors the previous one in every detail, with one exception: Each user accesses their own privileged account via PAM/PSM (as shown here). This tier provides the best of both worlds: You get total isolation of privileged accounts and end-to-end accountability of individual admins from PAM/PSM, all the way down through applications and operating system logs.



The only challenge with this tier is that dual account management can become a burden on IT. With so many accounts under management, recurring manual repetitive maintenance and reverification of access might be necessary to ensure that PAM/PSM configurations and policies are current.

BeyondTrust Insights: Simplifying Account Control with Adaptive Workflow

Trying to keep PAM/PSM configured properly (so that the right mix of requesting users, privileged credentials, target systems, days of the week, times of day, and location the request came from) is enough to keep any IT pro busy full time. Password Safe uses adaptive workflow control (shown here) to establish smart policies that define when a privileged account request is and isn't appropriate.



PUTTING THE *PRIVILEGE* INTO PRIVILEGED ACCOUNT MANAGEMENT

The idea of handing someone the password to an administrator account demonstrates *privilege*—defined as "a special right, advantage, or immunity granted or available only to a particular person or group of people". As organizations mature, the ways in which they view security, grant privilege, and choose to whom, and to what level, security is applied become more restrictive and precise.

Privileged accounts need to be protected through isolation, obfuscation, and accountability. By maturing your manner of managing privileged accounts, you can meet the goals outlined in this paper:

- Limit access to each privileged account to as few users as possible
- Reduce the risk of improper use of privileged accounts by cybercriminals
- Increase accountability around the use of each privileged account

The use of PAM and PSM solutions ensures that these goals can be in effect throughout the process of leveraging a privileged account: from account request, to account logon, to account use in a privileged session. If your privileged account management falls into any of the lower tiers outlined in this paper, consider the possible repercussions and the need to implement the highest tier possible within your organization.

ABOUT RANDY FRANKLIN SMITH

Randy Franklin Smith is an internationally recognized expert on the security and control of Windows and AD security. Randy publishes www.UltimateWindowsSecurity.com and wrote The Windows Server 2008 Security Log Revealed—the only book devoted to the Windows security log. Randy is the creator of LOGbinder software, which makes cryptic application logs understandable and available to log-management and SIEM solutions. As a Certified Information Systems Auditor, Randy performs security reviews for clients ranging from small, privately held firms to Fortune 500 companies, national, and international organizations. Randy is also a Microsoft Security Most Valuable Professional.

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 78 of the Fortune 100, and a global partner network. Learn more at www.beyondtrust.com.

Disclaimer and COPYRIGHT