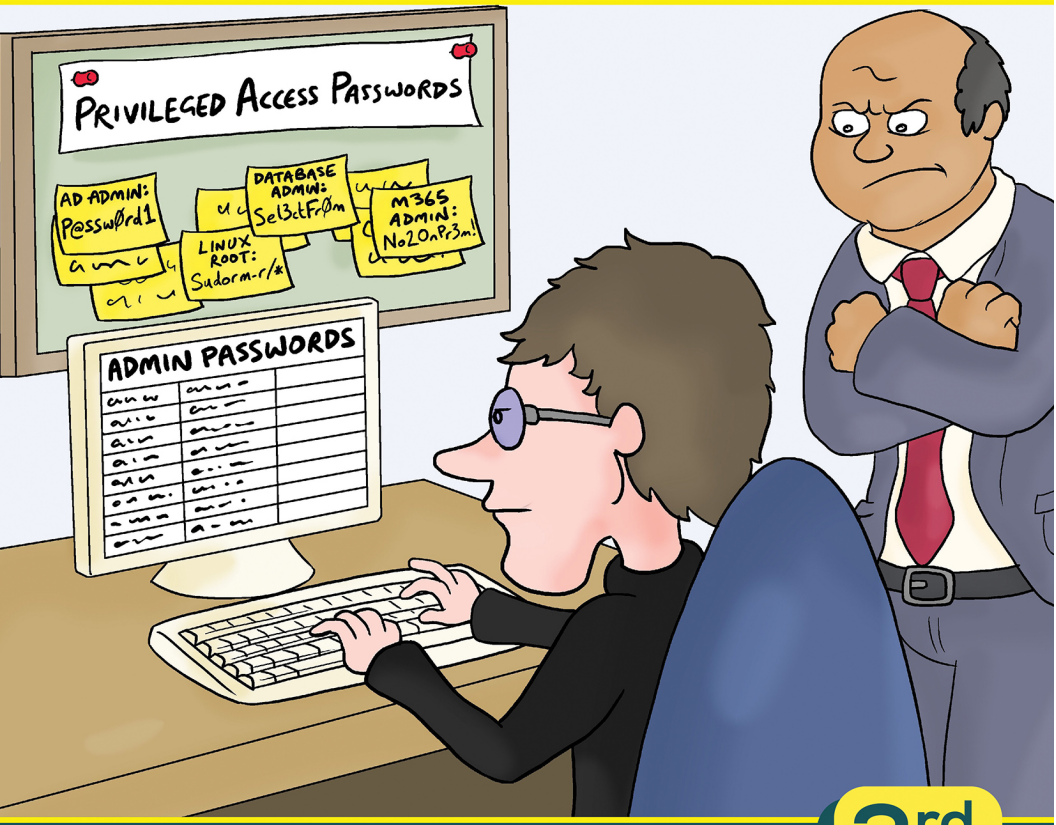
ConversationalGeek®

Conversational PAM Vault

By Nathan O'Bryan (MCSM: Messaging, and five-time Microsoft MVP)



In this book, you will learn:

- How the threatscape has changed and why privileged accounts are vital to hackers.
- What a PAM vault is and how it can protect your privileged accounts.
- The primary steps to protect privileged accounts on your organization's networks.

3rd Edition

Sponsored by Delinea

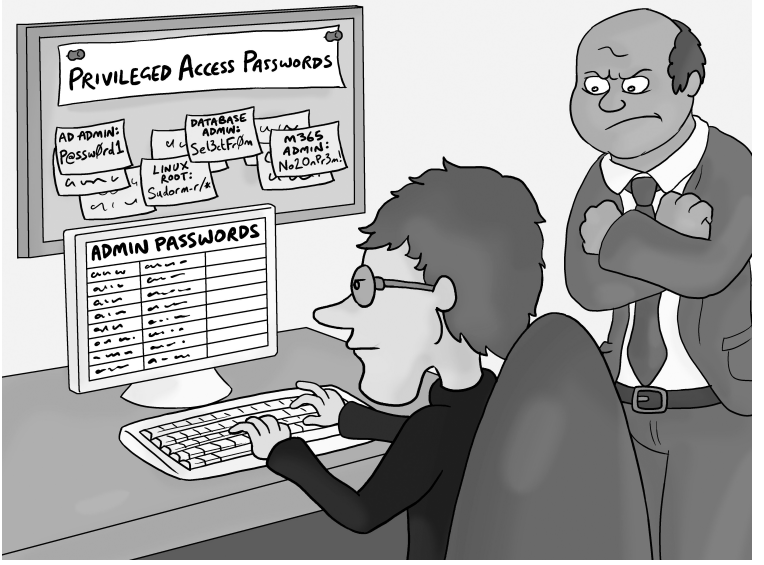
Sponsored by Delinea

Delinea is a pioneer in securing identities through centralized authorization, making organizations more secure by seamlessly governing their interactions across the modern enterprise. Delinea allows organizations to apply context and intelligence throughout the identity lifecycle across cloud and traditional infrastructure, data, and SaaS applications to eliminate identity-related threats. With intelligent authorization, Delinea provides the only platform that enables you to discover all identities, assign appropriate access levels, detect irregularities, and immediately respond to identity threats in real time. Delinea accelerates your team's adoption by deploying in weeks, not months, and makes them more productive by requiring 90% fewer resources to manage than the nearest competitor. With a guaranteed 99% uptime, the Delinea Platform is the most reliable identity security solution available.

For more details visit
delinea.com

Conversational PAM Vault

By Nathan O'Bryan



ConversationalGeek®

Conversational PAM Vault

Published by Conversational Geek® Inc.

www.conversationalgeek.com

Trademarks

Warning and Disclaimer

Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at **ConversationalGeek.com**

Publisher Acknowledgments

All of the folks responsible for the creation of this guide:

Author:	Nathan O’Bryan
Project/Copy Editor:	Ian Whiteling
Content Reviewer(s):	Colleen Lerch
	Tony Goulding

Note from the Author

I've been given the opportunity to write a bit about securing access to privileged accounts, the threats we deal with, and how you can make your organization more secure. That's a big job – much bigger than I can hope to accomplish in the small amount of space I have here.

In addition to saying something smart about IT security, I have also been charged with writing this in a way that you'll want to read it. That's the whole "Conversational Geek" model, do technical writing but in a way that you will actually want to invest 20 minutes of your busy day reading. That's my goal here, and I hope I'm able to pull it off.

In this eBook, I'm going to talk about Privileged Access Management and the need to store credentials securely. If you find my writing style a bit too flippant, I'll give you the summary now: Accounts with administrative access to your IT systems are a target. Bad actors want access to those accounts so they can use them to steal your organization's data and sell it to other bad actors. Please exercise caution with those accounts. Please make sure the passwords for those accounts are kept secure and long and complicated; so long and complicated that you can't possibly remember them.

Hopefully, you've gotten this far and found my style to be at least a little entertaining. If that is the case, I invite you to come along on a quick journey to talk about IT security and learn something new that will be helpful to you in your career.

Nathan O'Bryan

The “Conversational” Method

We have two objectives when we create a “Conversational” book: First, to make sure it’s written in a conversational tone so that it’s fun and easy to read. Second, to make sure you, the reader, can immediately take what you read and include it into your own conversations (personal or business-focused) with confidence.

These books are meant to increase your understanding of the subject. Terminology, conceptual ideas, trends in the market, and even fringe subject matter are brought together to ensure you can engage your customer, team, co-worker, friend, and even the know-it-all Best Buy geek on a level playing field.

“Geek in the Mirror” Boxes

We infuse humor into our books through both cartoons and light banter from the author. When you see one of these boxes it’s the author stepping outside the dialog to speak directly to you. It might be an anecdote, it might be a personal experience or gut reaction and analysis, it might just be a sarcastic quip, but these “geek in the mirror” boxes are not to be skipped.

Greetings. Within these boxes I can share just about anything on the subject at hand.

Read ’em!

Protecting Privileged Accounts with a PAM Vault

Ever wake up and realize you're living in an entirely different world than you expected? Of course, that whole pandemic thing happened and changed a whole lot of stuff; now AI is the thing, but also, I've been an "IT guy" of some sort or another for nearly 30 years, and man *have things changed*.

When I think about how we did IT in the early 90s, ugh, no one had any idea what was going on, right? That seems like an entirely different world, so slap-dash and unorganized. When I think about it, it's pretty impressive that we, as an industry, have come so far so fast. Back then, someone, or really a whole lot of people, thought Microsoft Bob was a good idea.

The bad guys too! They were pretty much cartoon characters. I mean, "hackers" did disruptive stuff; they broke things and caused all kinds of problems. However, as "good guys," we

didn't have to worry about "hackers" stealing anything of any real value. I survived the "Melissa" and "I Love You" viruses in 2000. Those were both bad, and they each shut down the organization where I was working for weeks at a time, but no one was trying to steal anything there. Those attackers were just dummies trying to break stuff for no other reason than to see if they could.

Now, in 2025, the threat to IT environments is much different. Threat actors are networked, stealthy, well-funded and now have access to a plethora of "cybercrime-as-a-service" and ChatGPT-like malicious AI-based tools. These new tools take what would have been a novice threat actor a year ago to someone who is quite proficient in cyberattacks. Now their primary goals are to steal data with various profit motives, gain access to financial applications to commit digital fraud and, of course, they're encrypting your entire environment and holding it for ransom.

But in each and every case, it's necessary for the threat actor to obtain credentials with enough privilege to move around within your network and gain access to protected, sensitive, and otherwise valuable data, applications, and systems so they can make more money or cause more disruption!

At the center of these attacks are *credentials*; without them, the bad actors have almost no power to do anything, let alone something malicious. It's probably the reason the use of stolen credentials is the number one threat action in data breaches today[1]. And we see the use of credentials in lateral movement activity (for the newbies out there, lateral movement is when

---

[1] Verizon, *Data Breach Investigations Report* (2024)

bad actors move from system to system within your network), something seen in over 80% of ransomware attacks[2].

This consistent set of threat actions revolving around credentials and their use has resulted in cyber insurers – who have spent the past few years gaining a better understanding of the risk in unmanaged privileged access – now requiring organizations to have more controls in place.

And while we'd all like to think our privileged credentials are secure, the human element comes into play – weak (read: *guessable*) passwords, sharing of credentials, lack of security policy designed to keep privileged credentials protected, falling for credential harvesting phishing attacks, not disabling/ deleting old third-party accounts, forgetting about old credentials left in the registry/scripts/Group Policy/etc., and more. This human element, that plays a role in 68% of data breaches today[1], includes employees, contractors, and vendors that need privileged access who are logging in from outside the organization's network.

This makes it essential for organizations like yours to find better ways to protect the access to and use of privileged credentials and stay ahead of constantly evolving bad actors who are always finding new ways to take advantage of vulnerabilities in operating systems, applications, processes, and people to gain access to the very data that you are working to protect.

The goal should be to mitigate and manage the risk that inherently exists by making the privileges inaccessible and unusable to threat actors while still allowing them to be available for legitimate access by the appropriate users – without slowing teams down. Many organizations are even incorporating the concepts of *Zero Standing Privilege* and *Just*

---

[2] Coveware, *Quarterly Ransomware Report Q3* (2024)

in Time Access into their cybersecurity strategy to help reach that goal of minimizing risk.

What's needed is a way to first extend visibility into where privileged credentials exist, and then how those credentials are being used across the enterprise. This is where a Privileged Access Management (PAM) Vault comes into play to minimize that risk of the misuse of privileged accounts.

My day job is an IT Security Consultant, a job I could not have imagined when I started my career as an "IT guy." I mostly spend my days working with large organizations trying to teach them how to secure their IT assets. This can be a difficult job, but I really do love it.

What is Privileged Access Management?

Before we can define what a *PAM Vault* is, we should all be on the same page around what *PAM* is in the first place. And getting a good definition of PAM is harder than you'd think.

Many might think a good place to start with a definition of "Privileged Access Management" would be Wikipedia, but there is no entry specifically for PAM. Then there are plenty of PAM vendors, each providing their interpretation of PAM, making it difficult to give you an unbiased definition. So, I went to Gartner[3]:

[3] "Privileged Access Management Reviews and Ratings", Gartner, www.gartner.com/reviews/market/privileged-access-management, (accessed December 4, 2024)

"Gartner defines privileged access management (PAM) as tools that provide an elevated level of technical access through the management and protection of accounts, credentials and commands, which are used to administer or configure systems and applications. PAM tools — available as software, SaaS or hardware appliances — manage privileged access for both people (system administrators and others) and machines (systems or applications).

Gartner defines four distinct tool categories for PAM tools:

- *Privileged Account and Session Management (PASM)*
- *Privilege Elevation and Delegation Management (PEDM)*
- *Secrets Management, and*
- *Cloud Infrastructure Entitlement Management (CIEM)"*

Note that Gartner doesn't focus in on simply vaulting privileged credentials – a common misconception within IT that a "vault" *is PAM*. Instead, think of PAM as a framework of solutions to help organizations systematically lower privileged account risk, increase business agility, and improve operational efficiency – with a vault serving as the foundation of any PAM strategy.

PAM isn't a "one-size-fits-all" plug-and-play solution that is just going to magically make your organization "secure." But PAM implementations all have one consistent factor – they all begin with a solid enterprise-grade vault to get started.

Then What's a PAM Vault?

If you're unfamiliar with a PAM Vault, in its purest essence, it securely stores privileged account passwords and other credentials in a database where the access is managed and monitored – something that is a subset of Gartner's definition of a PASM solution. But in reality, PAM Vault solutions do so

much more than that. For example, many PAM Vault solutions also do discovery of privileged credentials (something Gartner would expect to find in a CIEM solution), establishing privileged remote access sessions without divulging the privileged credentials (the "S" in PASM), and other functions that could be found in one form or another across Gartners four "distinct" tool categories.

Rather than provide a succinct definition of a PAM Vault here that likely wouldn't do the concept justice, I'm going to spend the remainder of this eBook diving deeper into what a PAM Vault is, what it can do for your organization, and how it helps secure privileged access. I'm going to do so by using a single coherent narrative around the steps you should be taking to *protect privileged access*, with a PAM Vault sitting squarely in the middle of it all.

Protecting Credentials

Let's start with the goal of all this, which I mentioned before: make privileged account credentials – and, therefore, the access they provide – inaccessible and unusable to threat actors while keeping them accessible and usable for legitimate use. To do this, there are several steps you'll need to take that can be met with an enterprise-grade vault. So, think of the following as both a set of steps for you to follow and a checklist of what you should be looking for in a PAM strategy.

Define "Privileged"

Generally, when we think of "privilege" we immediately go to *accounts* with elevated access – something like the *Administrator* account in Active Directory (AD). But is that where the "privilege" line should be drawn within your organization? Is privilege exclusive to accounts only? The answer is a resounding "no", as the modern thinking around PAM is the protection of *secrets* – those bits of technology that actually provide the privileged access. In reality, the privileged

account isn't the secret – case in point, everyone knows about the *Administrator* account! It's the *password* that's the secret – the protected piece of information that *enables* the privileged access. But passwords aren't the only kind of secret within your organization; there are many types – all, of which, should be considered when developing a PAM strategy:

- Passwords – Credentials for various systems and applications
- Passkeys – biometric-, app-, or physical device-based authentication methods
- SSH Keys – Secure Shell keys used for encrypted communications
- API Keys – Keys granting access to application programming interfaces
- Certificates – Digital certificates for authentication and encryption
- Database Credentials – Login details for database systems
- Cloud Access Keys – Credentials for cloud service providers
- Service Account Credentials – Accounts used by applications or services
- DevOps Secrets – Passwords, API keys, and SSH keys used by automated systems and applications within a DevOps environment

- Configuration Files – Files containing sensitive configuration details
- License Keys – Software license information
- Documents – Sensitive documents requiring secure storage

Threat actors look for ways to use any means possible that would grant them privileged access, making it necessary to protect every type of secret that may put the organization at risk.

Discover Your Secrets

You can't secure what you don't know about. So, it becomes imperative that you can identify which secrets provide access to your organization's definition of "privileged", as well as where and how they are used.

To be clear, this is much more than just "build a list"; I'm talking about performing a true discovery of what's out there in your environment. That means your vault should be able to run a 'discovery' to identify every server, script, application, database, file system, permission, etc., to determine which accounts, keys, certificates, etc. provide more access than a regular user.

Modern PAM solutions use AI, which adds value by analyzing complex permission structures and correlating across multiple accounts linked to an identity, uncovering hidden privilege escalation pathways and detecting unusual privilege combinations. AI is also used to analyze recorded sessions to detect unusual behaviors – many of which are outside the current IT staff line of sight.

Of course, undertaking this process should be an opportunity to remove accounts and other secrets that are no longer needed in your environment and clean up those you find to be

overprivileged. This type of account consolidation and maintenance will definitely make your life easier, reduce your attack surface, and make your organization more secure in the long run.

Vault Your Privileged Secrets

OK – here is the pinnacle of our narrative. All those secrets you identified need to be secured. I cannot believe I need to actually say this but you should never be using a spreadsheet, even if it is locked *(#deletethesheet!*); you need to store credentials and other secrets in an encrypted enterprise-grade vault. Your PAM strategy starts with a solid vault that facilitates access to privileged secrets, but only to those individuals approved to do so – usually based on user account.

In essence, you can define which users in your organization can access which specific privileged secrets from within the vault and on which systems they can be used. If you have not used a PAM solution that has a vault – the vault is usually accessed via a web interface where the user can request the secret they want and be provided, for example, a username and password or (as you'll see in a moment) privileged remote access to a system *without divulging the credential pair*.

Between this section and the last, I've talked about discovering secrets, securing them in a vault, and even establishing privileged remote access – all functionalities found in modern *PASM* solutions – which includes the PAM Vault functionality.

If you're new to PAM, let me make sure there's no confusion about what "vaulting" a credential means. The account is still stored in, say, AD. But a copy of the current username/ password pairing details is securely stored in the vault (NOT in

an Excel spreadsheet!) to keep it away from prying eyes. Additionally, the passwords for the vaulted privileged credentials are rotated (more on this in a moment).

Go with a Least Privilege Mindset

I'm assuming most, if not all, of you understand the Principles of *Least Privilege* – basically, reducing the privileges to only those needed to accomplish the task at hand. But in the context of PAM, least privilege isn't enough; it's possible that, say, the user account for a member of IT (because they need to accomplish administrative tasks as part of their job) is given some kind of standing administrative privileges. This creates risk for the organization (e.g., if that user's account is compromised, a threat actor now has administrative access. Just in case you're not sure – that is bad!)

Some organizations prefer to give their administrators a secondary account that is used to access privileged systems from the vault. So, you'd log on as you and can access email, your files, etc., but the moment you want to do something that requires elevated privileges, you're going to use that secondary account to do so – which you'll access via the vault.

If a user's own account is intended to be privileged (and they don't use a generic admin account to do their privileged tasks), they should still have two user accounts – one low-level and one privileged, with the privileged one being stored within the vault.

Manage Who Has Access to Your Secrets

On top of every vault is the ability to establish roles and policies around access to privileged secrets. Which user, accessing which credential, from where, when, can all be defined in most

PAM vaults. This granularity ensures that only sanctioned privileged access is possible.

Rotate Passwords (for Secrets That use Them)

In addition, passwords of privileged credentials can be *rotated* (read: updated) on a schedule or after every use to thwart misuse through something like grabbing the password hash of a privileged account using a tool like Mimikatz. Keep in mind that with password rotation, your vault will not only set the new password in AD but should also be responsible for updating the password on any services, scripts, applications, etc., or those resources using the credentials will no longer work.

Use Multi-Factor Authentication

Password rotation will likely take care of a threat actor guessing the credentials of a privileged account. However, there is still the issue of protecting the user account that has been granted access to the privileged account via the vault. Passwords are not enough – a good reminder of times changed. There are just too many things that can go wrong if your organization relies on passwords alone to secure user authentication and authorization. Let's look at an example environment where multi-factor authentication (MFA) is relatively easy to implement – Microsoft 365 – and see how much it is being used and the repercussions of not using it.

According to Microsoft, during an audit of the Microsoft 365 environment:

- 1,200,000 compromised accounts were found in the Microsoft 365 cloud
- 99.9% of those accounts did not have MFA turned on
- Statistically, one in 100 attempts at a password spray attack will work using just 15 of the most common passwords

- Another 40% of compromised accounts were found by replay attacks (where a username/password combination from a data breach is attempted against another service)

I would like you to take the time to re-read those bullet points above a couple of times. Please just sit with those numbers for a minute; I mean it.

Now apply this to your organization's environment. The point here is that when you rely solely on the traditional "username/password" combination, the users in your organization are still susceptible to credential attacks, which means access to your privileged accounts may still be at risk.

Is that enough to convince you to turn on MFA? Any account that can authenticate into your organization's IT systems without MFA is a potentially easy-to-open door for a compromise into your whole organization. So, at a minimum, every identity that has permission to access a privileged account from within the vault must, and I mean MUST, have MFA in place as part of authentication. And for those organizations that want another line of defense beyond login, consider adding a layer of MFA on access to highlight privileged secrets- now we're talkin'!

Modern CIEM solutions (and PASM solutions that offer *discovery*) can find privileged accounts that *don't* have MFA enabled as part of the discovery process.

Monitor, Audit, and Control Privileged Access

Cybersecurity is evolving at a time when we're all working towards Zero Trust (where you "never trust" any part of your IT infrastructure has not been compromised). Your default stance with privileged access shouldn't be "we trust you." After all, you've (hopefully) gone through the trouble of locking away all your privileged credentials and limiting who can access them. So, it makes sense that you will also want to keep an eye on who's using which credentials and – wherever possible – what actions are being taken with those credentials.

PASM solutions (which generally include vault functionality) manage and monitor the use of the privileged credentials from the time a requesting user launches a privileged session to when it ends, creating an audit trail.

PASM solutions can trigger alerting of potentially inappropriate actions to other members of IT, as well as kill a proxied session should it be necessary. This feature is useful in the case of a threat actor compromising a user account and then attempting to leverage the PASM to access parts of your environment as a privileged user.

Secure Remote Access

External users requiring access to the corporate network and its resources is now commonplace. Traditional remote access methods like RDP or simple VPNs won't provide the necessary control over whether a user should be allowed to access a resource using a privileged credential. Instead, vaulting those credentials adds security to privileged accounts even when accessed by users outside the network. And with privileged remote access, those privileged sessions are monitored and recorded for auditing anytime.

Automate as Much of This as You Can

I've covered a lot of work that needs to be done to protect your privileged accounts, and none of you have a lot of free time on your hands. So, consider deploying a vaulting solution that automates as much of the work outlined above; for example, some solutions can auto-vault discovered accounts and every PAM vault solution will do the automatic password rotation after a period of time or after use.

The use of automation will speed up the process of protecting privileged secrets, improve the accuracy of the work done, create a predictable level of security, and elevate the productivity of the users interacting with it across your entire organization.

The Big Takeaways

Privileged secrets that yield elevated access to an environment are key targets for threat actors. So, it's necessary to take additional steps to protect these secrets from misuse using a PAM vault as part of a larger PAM strategy. Some of your key considerations include:

- All credentials are not equal. Highly privileged accounts need to be handled differently. Identify which accounts within your environment have privileged access and take extra measures to ensure their security.

- Privileged secrets come in many forms and all need to be securely stored and protected – even when being utilized.

- A secure vault complete with access policies, password rotation (as is appropriate), and session management is an important step to achieving a good security posture..

- Use a least privileged access model. Ensure administrators have non-privileged accounts for their day-to-day access and admin accounts (or the ability to access them based on rules tied to their role) to do administrative tasks.

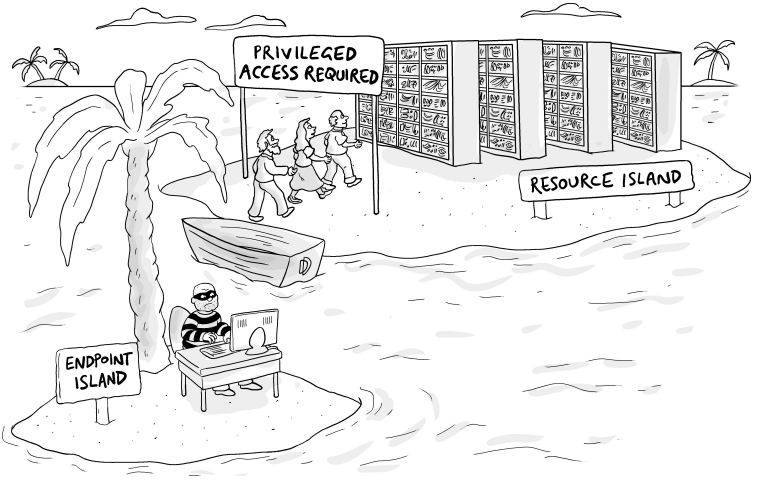
- Auditing and monitoring privileged account and secret use is necessary to ensure the actions taken are as sanctioned as the use of the privileges they enable in the first place.

- Leverage automation wherever you can. Why manage tens, hundreds, or even thousands of secrets manually when you can automate their entire lifecycle securely?

A secure PAM vault provides organizations with a means to secure privileged access by limiting who can use the credentials providing that access while managing the credentials and auditing their access and use. By leveraging PAM as part of

your layered security strategy, you eliminate the threat actor's ability to move laterally, access data and resources, and pretty much do anything malicious on your network. The key is in defining what "privileged" is and setting a solid foundation by finding a PAM solution with an easy-to-use enterprise-grade vault that provides easy access to privileged credentials while significantly enhancing their security.

Sponsor Chapter:
Keeping Privileged Access Secure with Delinea's Secret Server



The simple reality of today's cyberattacks is that bad actors are laser-focused on gaining access to privileged accounts in order to wreak havoc on unprotected organizations for monetary gain – period. Your goal, therefore, is to isolate and protect privileged access from those with malicious intent while simultaneously allowing authorized users to leverage that very same access.

To accomplish this, you need a means of identifying privileged accounts, centrally storing and securing privileged credentials that provide that access, establishing who can use the credentials and what they can do with those credentials, sharing the credentials or access (more on this later), and monitoring and auditing what's done with the privileged access when it's used.

That's a pretty tall order – especially if you haven't heeded my words and are still thinking your Excel spreadsheet is a handy way to keep track of privileged access – quick reminder here again #deletethesheet!

Organizations intent on getting a handle on securing privileged access have turned to Delinea Secret Server – a robust enterprise-grade Privileged Access Management (PAM) vault available for on-premises, hybrid, and cloud environments.

Secret Server is a very easy-to-use and deploy credentials vault that helps organizations identify, manage and secure privileged credentials for service, application, root, and administrator accounts across the entire enterprise with scalable features and functionality such as:

Discovery

You can't secure what you aren't aware of, and you can't protect what you cannot find, so uncovering every privileged account and its dependencies is imperative. Secret Server assists with automatically discovering privileged accounts, whether you know about them or not (i.e., "shadow" admin accounts), automatically vaulting the credentials so you can set policies to manage and protect them with confidence on Windows servers, within Active Directory, AWS, Azure AD, and Google Cloud, on Unix systems, and within VMware environments. Secret Server Discovery reduces sprawl and quickly gives you a full view of all privileged accounts using the least amount of human interaction. Plus, it helps with auditors – if they find an unprotected privileged account you will get "dinged".

A Centralized Vault

All those discovered bits of privileged access need to be documented, stored, managed, and audited somewhere. Secret Server secures all secrets, such as passwords, certificates, keys, files, and more, with 256-bit encryption (at

rest and in transit) and provides the option to leverage post-quantum safe encryption where needed. These “secrets” provide the holder with privileged access to technical, operational, and physical company resources – making it imperative to secure them in a vault within Secret Server. And because it’s still possible that someone in your organization with sufficient privileges can change the password on the local system (bypassing Secret Server), Secret Server utilizes *Heartbeat* to provide up-to-the-minute monitoring of credentials across your network and automatically tests a “secret’s” credentials at set intervals alerting administrators if they were changed outside of Secret Server or without their knowledge. Secret Server can then optionally reset the password to bring it back into sync with the vault.

Automating complex tasks is critical for administrators and DevOps teams to eliminate human error and allow organizations to scale. Secret Server integrates with third-party vendors so you can avoid built-in application credentials and ensure proper control and management. Having said all that, the real value in the vault isn’t only automatically rotating and securing privileged access but also allowing authorized and authenticated access to privileged accounts – which brings me to the following two critical pieces of functionality…

Secrets Management

Just like you don’t allow everyone in IT to have access to the Administrator account in AD (*you don’t, right?*), you don’t want every secret stored within Secret Server to be accessible to everyone. So, Secret Server provides flexible role-based policies and configurations with easy-to-use templates to define who can access which secrets, increased password complexity, automated password rotation, and more to make it easier for busy IT teams to control access to privileged accounts without slowing them down.

Virtually all compliance mandates and security best practice frameworks require some form of role-based access control (RBAC). Access control allows system admins to manage user roles efficiently and sustainably – reducing the on-the-fly decisions needed and extra burden on IT teams.

Access to Secrets

In the most basic of PAM implementations, users of Secret Server need to authenticate to prove who they are, at which point Secret Server will determine which secrets are accessible to the authenticated user. Leveraging multi-factor authentication, IP Address restrictions, automated approval workflows, and pre-defined access for pre-defined periods of time, Secret Server provides a layered approach to maintaining an environment with zero standing privileges while ensuring the right user is given the necessary privileged access to get their job done.

Automation

Automation within Secret Server goes beyond auto-generated passwords that are impossible to remember and includes scheduled password rotation, email alerts on specified events, and if/then automation with a series of automated follow-up actions, saving IT time to focus on alerts that may need more investigation. Integrations with Secret Server can also trigger automatic incident responses, for things like, phishing or malware.

Session Monitoring and Control

If you're going this far to lock up your privileged credentials and establish policies and controls over who can access them, you might as well go the whole nine yards and *never actually give the requesting user the privileged credential*.

Instead, Secret Server can establish a proxied session over HTTP (VPN-less), RDP, SSH, PuTTy, or Web Password Filler to connect the user wanting the privileged access to their desired

system or application – all without ever disclosing the privileged credential to them at all – reducing your attack surface, eureka!

Secret Server's session management, monitoring, and control establishes oversight and accountability for the use of PAM sessions, using AI to scan session recording for anomalous behavior, mitigating the risk of privileged account misuse. With privilege session management, the activities of your privileged users – which includes your trusted insiders, third-party vendors, and connected systems – are managed, monitored, and recorded during the entire session. Administrators have a real-time view of all privileged sessions launched from Secret Server and have the option to terminate any session that is deemed risky, suspicious, or unauthorized.

And, because Secret Server is proxying the session, each privileged session is monitored and recorded, giving security teams visibility and insight into not just *when* privileged credentials are used but *how* they are used. This monitoring also serves as the basis for detecting anomalous behavior through analysis of privileged user behavior and audit trails.

Auditing & Reporting

All activity within Secret Server is documented in an immutable audit log that serves as the basis for scheduled and custom reporting, detailed log searches, custom alerting, syslog/CEF logging, and integration with SIEM solutions to help provide additional context when involving privileged credential use. Security teams must be able to see at-a-glance how well policies are followed and where there are exceptions.

Secret Server is designed to not only keep you secure, but also to help you meet mandated requirements and easily show compliance. The audit trails help busy organizations easily meet regulatory requirements and demonstrate compliance to satisfy internal and external auditors. And because we favor

automation, you can have a scheduled report run sent to yourself and even an auditor via email – if you need it. Security and Ease-of-Use.

Disaster Recovery

No PAM strategy would be complete without ensuring its own availability during a disaster recovery scenario. Secret Server has multiple capabilities that are useful should a disaster strike, including Break the Glass functionality (which gives you access to secrets in Unlimited Admin mode), along with high availability through automatic replication to ensure Secret Server (and access to your business-critical assets) is accessible when an incident occurs.

Secret Server's resilient secrets capability ensures secrets remain secure and accessible during outages or disruptions. They leverage advanced replication and synchronization to ensure availability if the primary server is unavailable. This provides fault tolerance by distributing encrypted secrets across multiple nodes or data centers, ensuring. High availability and reducing downtime. It also ensures sensitive secrets remain protected during failover scenarios.

It Can't All Just Be About Features…

A PAM solution like Secret Server not only sounds great when you look at it through the lens of how secure your privileged access is, but – and here is the kicker – it is actually easy to put in place *and* use by the entire organization. Bad actors aren't going to give you time to get your privileged access in order, making it even more critical to secure your privileged access as quickly and efficiently as possible across the organization.

We all know the success or failure of any security solution rests in its *adoption,* and this includes a PAM and everything that is part of your PAM strategy. If your security team and organization ignore the change in process and continue to use

the (gasp!) Excel spreadsheet, you've wasted a ton of time, effort, and money.

Delinea prides itself on Secret Server being an easy-to-implement solution quickly adopted within an organization. Protecting privileged accounts from bad actors and ever-evolving threats can be complicated and convoluted, but it does not mean your solution needs to be complex and cumbersome. Secret Server is an easy-to-use, enterprise-grade solution, that is quick to implement from its wizard-based configurations to simplified setup; its APIs, custom scripts, and integrations seamlessly adapt to your environment; and its completely customizable and configurable platform.

Secret Server works the way modern IT teams work and repeatedly demonstrates its value as a secure way to manage and protect privileged access to service, application, root, and administrator accounts across your network and as the easiest way for you to do it and with the fastest ROI.

Discover and protect privileged accounts

Stop credential misuse, not company productivity, with a modern enterprise-grade vault.

Delinea Secret Server enables IT and security leaders to discover and secure privileged accounts, preventing unauthorized access with streamlined management and ensuring compliance by reducing risk to critical assets.

Key benefits of Secret Server

Discovery: Quickly identify and vault credentials for every service, application, administrator, and root account.

Automation: Automate the lifecycle of credentials with automated password rotation to reduce the risk and ensure compliance.

Session Monitoring: Monitors and records privileged sessions, providing visibility into suspicious behavior with a full audit trail.

Centralized administration: Unify the security and management of privileged credentials, reducing administrative overhead, and streamlining policies.

Leverage flexible deployment that enables you to secure privileged accounts in weeks, not months, with unmatched security controls that provide comprehensive discovery, advanced automation, and AI-driven session analysis.

Learn more about Secret Server and try it free to improve your security posture today: delinea.com/products/secret-server

Quickly become conversational about Privileged Access Management (PAM) and a PAM Vault.

By leveraging a PAM Vault as part of your organization's layered security strategy, you can effectively eliminate any bad actor's ability to move laterally, access data and resources, and pretty much do anything malicious on your network. In this eBook we will help you to define what "privileged" means for your organization and understand how a PAM Vault solution can help you get control over your privileged credentials and significantly enhance your security.

About Nathan O'Bryan

Nathan has spent almost 30 years working in IT, starting in the United States Marine Corps, and then for companies like GE Capital, and Kaiser Permanente. He specializes in Exchange, Microsoft 365, Active Directory, and cloud identity and security, and is an active author, conference speaker, and webcast presenter.