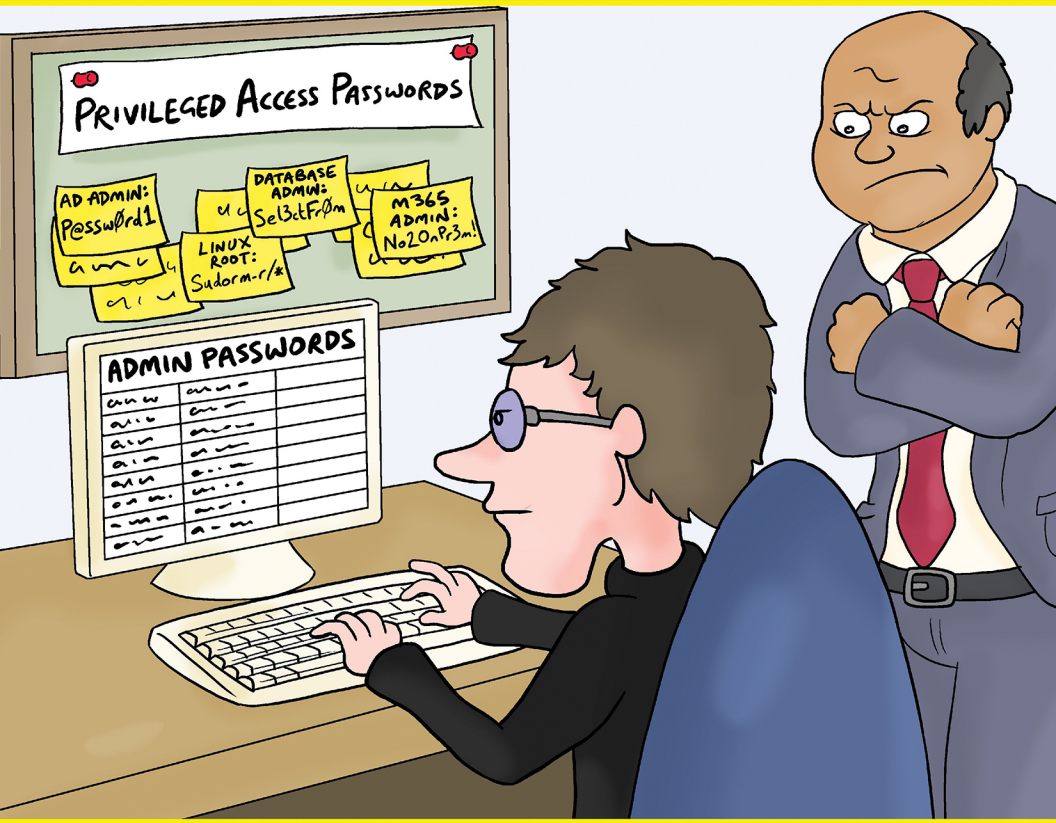
ConversationalGeek®

Conversational Privileged Access Management

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 important to hackers.
- What Privileged Access Management is and how it can protect your privileged accounts.
- How to define and discover the privileged accounts in your organization's networks.

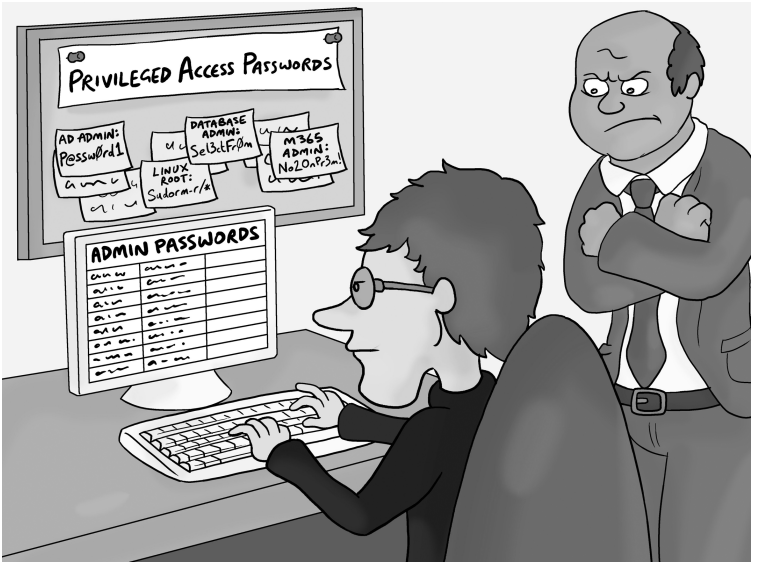
Sponsored by Delinea

Delinea is a leading provider of privileged access management (PAM) solutions that make security seamless for the modern, hybrid enterprise. Our solutions empower organizations to secure critical data, devices, code, and cloud infrastructure to help reduce risk, ensure compliance, and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide, including over half of the Fortune 100. Our customers range from small businesses to the world's largest financial institutions, intelligence agencies, and critical infrastructure companies.

For more details visit
delinea.com

Conversational Privileged Access Management

By Nathan O'Bryan



ConversationalGeek®

Conversational Privileged Access Management

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:	Pete Roythorne
Content Reviewer(s):	Colleen Lerch
	Barbara Hoffman

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 PAM

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; 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 2022, the threat to IT environments is much different. Bad guys no longer want to break your stuff. In fact, their goals tend to be rather the opposite. Now the bad guys want your IT systems to remain up and available so they can steal data with various profit motives. Instead, the goal is to obtain enough privileges to move around within your network and gain access to protected, sensitive, and otherwise valuable data they can steal to sell on the Dark Web, threaten to publish the data in exchange for a paid ransom, or – even worse – both.

At the center of these attacks are credentials; without them, the bad actors have 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 bad actors move from system to system within your network), something seen in over 70% of ransomware attacks[2].

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 contractor accounts, forgetting about old credentials left in the registry/scripts/Group Policy/etc., and more. This human element plays a role in 82% of data breaches

---

[1] Verizon, *Data Breach Investigations Report* (2022)

[2] Coveware, *Quarterly Ransomware Report Q1* (2022)

today[1]. This makes it essential for organizations like yours to find better ways to protect 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 you're working to protect.

What's needed is a way to make privileged credentials inaccessible and unusable to bad actors while still allowing them to be available for legitimate access by the appropriate users. This is where Privileged Access Management (PAM) comes in.

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?

Getting a good definition of PAM is harder than you'd think. As I started writing this eBook, I wanted to ensure we were all on the same page about the topic we were covering, which turns out to be a much bigger task than I expected.

I suppose a good place to start with a definition of "Privileged Access Management" would be Wikipedia, but there is no entry specifically for PAM. There are plenty of PAM vendors,

each providing their interpretation of PAM, but I wanted to give you an unbiased definition. So, I went to Gartner[3]:

"PAM tools help organizations provide secure privileged access to critical assets and meet compliance requirements by managing and monitoring privileged accounts and access. PAM tools offer features that enable security and risk leaders to:

- *Discover privileged accounts on systems, devices, and applications for subsequent management*
- *Automatically randomize, manage and vault passwords and other credentials for administrative, service, and application accounts*
- *Control access to privileged accounts, including shared and "firecall" (emergency access) accounts*
- *Isolate, monitor, record, and audit privileged access sessions, commands, and actions"*

In more straightforward terms, PAM is a framework to help organizations systematically lower privileged account risk, increase business agility, and improve operational efficiency.

Another hurdle to a good definition of PAM is that it will look different in every organization. There isn't a "one-size-fits-all" plug-and-play solution that is just going to magically make your organization "secure."

So, I'm going to try to talk about many of the concepts that PAM covers and wrap them into a single coherent narrative

---

[3] "Privileged Access Management Solutions Reviews and Ratings", Gartner, www.gartner.com/reviews/market/privileged-access-management, (accessed June 23, 2022)

that is entertaining to read, and will hopefully get you started and headed in the right direction.

Safety Third

I'm going to start on a bit of an aside here, but bear with me. We are coming back to talking about Privileged Access Management, I promise. I just want to make a point with a (hopefully) fun analogy.

I am a fan of the long-running TV show "Dirty Jobs." The host, Mike Rowe, joins people on jobs that need to be done but that he feels don't get enough attention or appreciation.

While filming the show, the cast and crew need to attend a lot of safety briefings. Almost every new job means they need to attend another briefing. Fairly early on, Mike noticed that a lot of the safety briefings were giving the same information, and he didn't feel they were conveying good and useful information to the people they were intended to protect.

One platitude he reports hearing a lot of is "Safety first". His response is brilliant, insightful, and true.

"Safety is not a thing to be 'ranked', but rather a state of mind, to be applied as needed to a myriad of situations in varying amounts. But if we were to rank it, it would rarely be 'first'. Were safety truly 'first', no level of risk would ever be encouraged or permitted, and no work would ever get done."
– Mike Rowe

Bringing that idea back to this book's topic, I feel much the same about IT Security!

IT Security is not a thing to be ranked. If you are a Chief Information Security Officer (CISO) or a Chief Technology Officer (CTO) and you are telling your staff, "IT Security is our number one priority", I believe you are wrong.

IT Security is important. IT Security is very important. Just please don't try to rank it like that.

End-user access is important too. Having people come into the office, remote or in-person, every day and do their jobs is important. If we're ranking things, the jobs those people do to generate money for the company and pay your check is probably more important than IT security.

Your organization needs people logging into IT systems and accessing data daily to get their jobs done and keep the lights on. As an IT security professional, you are charged with not only making sure that process is secure, but also that it can occur in a reasonable manner.

I believe organizations can improve their overall security posture by making end users and administrators partners in the journey (and yes, it is a journey), not by making their jobs harder with overly restrictive policies. In the rest of this book, I'm going to talk about ways I believe you can make your organization's IT assets more secure with good Privileged Access Management processes and tools.

I'm asking that you please don't fall into the habit of ranking IT security as "priority #1". Help everyone in your company understand that IT security is critical, but so is their ability to do their jobs. Together we can find ways to ensure users have the access they need to do their jobs as securely as possible!

Now let's get to the business at hand, talking about IT security and how to safely store and use privileged credentials.

Protecting Privileged Access

Let's start with the goal of all this, which I mentioned before: make privileged accounts – and, therefore, the access they provide – inaccessible and unusable to bad 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 in PAM solutions. So, think of the following as both a set of marching orders for you to follow and a checklist of what you should be looking for in a PAM solution.

Define "Privileged"

When considering which of your accounts are "privileged," the easy answer is something like the Administrator account in Active Directory (AD). Active Directory has a handy built-in designation for accounts with admin rights, Admin Count 1. This is a flag that is added to accounts so that they can be protected by the AdminSDHolder process.

But is that where the "privilege" line should be drawn within your organization? Is an account with administrative access to a server "privileged"? What about an account that can manage the user accounts in a part of AD? Or an account with administrative access to an application? You need to define what "privileged" means in your organization.

At a minimum, this should include accounts with the following types of access:

- Service accounts
- Those that manage any part of AD
- Those being used in scripts or applications with elevated privileges
- Those with admin-type access to applications, environments, and platforms

- Those with access to your critical data
- Those being used to enable API access

Discover Your Privileged Accounts

You can't secure what you don't know about. So, it becomes imperative that you can identify which accounts meet the definition of "privileged" and where/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 looking at every server, script, application, database, file system, permission, etc., to determine which accounts have more access than a regular user – which will serve as the basis to compare against your definition of "privileged."

Of course, undertaking this process should be an opportunity to remove accounts that are no longer needed in your environment and clean up accounts you find to be overprivileged. This type of account maintenance will definitely make your life easier in the long run.

Vault Your Privileged Credentials

All those accounts you identified need to be secured, so you should never be using a spreadsheet that only a few people can access (#deletethesheet!); you need to store the credentials in an encrypted vault. PAM solutions offer a vault that facilitates access to privileged credentials, but only those approved to do so. In essence, you can define which users in your organization can access which specific privileged credentials from within the vault. If you've not used a PAM solution, the vault is usually accessed via a web interface where the user can request the credential they want and be provided either the username and password or (as you'll see in a moment) access to a system using the desired credential.

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.

Go with Least Privilege

I'm assuming most, if not all of you, know what Least Privilege is. But in the context of PAM, Least Privilege ensures that the users that wish to leverage privileged credentials do so using an account that in and of itself has no privileged access. 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 need a separate credential 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 Your Credentials and Access

On top of every vault is the ability to establish policies around access to privileged credentials. Which user, accessing which credential, from where, when, with whose approval, etc., can all be defined in most PAM solutions. This granularity ensures that only sanctioned privileged access is possible. In addition, passwords of privileged credentials can be rotated on a schedule or after every use to thwart misuse through something like grabbing the password hash of a privileged account using Mimikatz. Keep in mind that with password rotation, your PAM solution 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 credential will simply no longer work.

Use Multi-Factor Authentication

Password rotation will likely take care of any bad actor guessing 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. 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 MFA is relatively easy to implement – Microsoft 365 – and see how much MFA 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, 1 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.

How does your stomach feel at this point? Mine is queasy, and I know every account in my Azure AD tenant has MFA turned on.

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 account that has permission to access a privileged account from within the vault must, and I mean MUST, have MFA in place as part of its authentication.

On the same note, of better protecting the user accounts that access the vault, you'll want a stronger password policy. There's solid detail in NIST Special Publication 800-63B ("Digital Identity Guidelines"), but you probably still won't really know what a good password policy looks like after reading it, as it's more than a little bit dry.

Password policy recommendations have changed over time, and current recommendations may not be what you would expect. Short version: design your password policy around long passphrases that end users will remember and keep unique and keep them secure.

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.

With most PAM solutions, this is called Privileged Account Session Management (PASM). PASM is a fancy way of saying the user requesting a credential is not given the username and password; instead, they are logged onto the system they want to work on using that credential via proxy so that the user context and associated privileges are established. The requesting account that's doing the work never has access to the raw credentials themselves.

This proxy-based access also allows for monitoring and auditing of actions taken in that session. 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 bad actor compromising a user account and then attempting to leverage the PAM/PASM to access parts of your environment as a privileged user.

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 solutions that automate any of the work outlined above to speed up the process, improve the accuracy of the work done, create a predictable level of security, and elevate the productivity of the users interacting with the vault and PASM environment.

The Big Takeaways

The username and password model of authentication isn't going away anytime soon. And, while I think we can all agree that passwords are not the greatest way to verify the correct person is authenticating into your organization's IT system, they are still necessary and will be for the foreseeable future.

But because privileged accounts are targets for bad actors, it's necessary to take additional steps to protect these accounts from misuse. These include:

- Don't think of any aspect of IT Security as "the most important" thing in your organization. IT security is vitally important, but so is privileged access. If you try to rank one of those as "more important" than the other, you will be setting yourself up for failure.

- All credentials are not the same. Highly privileged accounts need to be handled differently. Make sure you know what accounts within your environment have privileged access and take extra measures to ensure their security.

- A secure password vault is an important step to achieving a good security posture. A secure password is going to be difficult or impossible to remember. So, using a secure password vault allows your organization to enforce much more secure passwords for users, administrators, and service accounts.

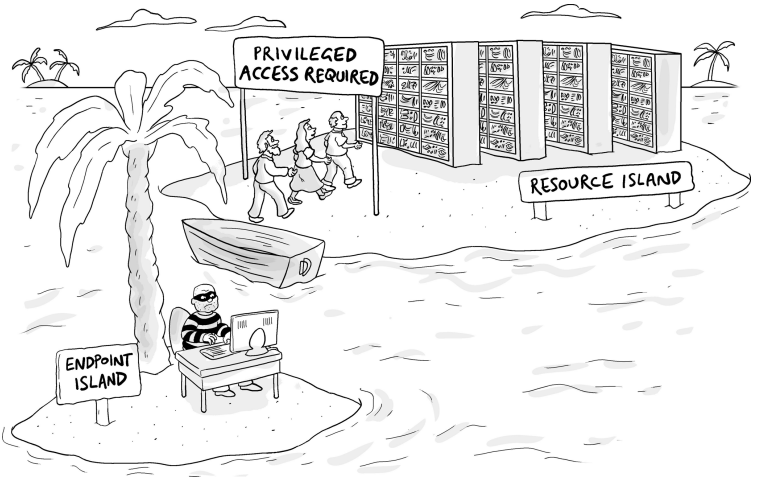
- Use a "least privileged" access model. Ensure administrators have non-privileged accounts for their day-to-day access and admin accounts (or the ability to request just-in-time rights elevation) to do administrative tasks.

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

- Leverage automation wherever you can. Why try to manually manage complex passwords on hundreds of service accounts when you can automate that process securely?

PAM 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 effectively eliminate the bad 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 finding a PAM solution that provides easy access to privileged credentials while significantly enhancing their security.

Sponsor Chapter: Keeping Privileged Access Secure With Delinea 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, where your privileged access is, centrally storing privileged credentials that provide that access, establishing who can use the credentials, 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!

Organizations intent on getting a handle on securing privileged access have turned to Delinea's Secret Server. A robust enterprise-grade Privileged Access Management (PAM) solution for on-premises, hybrid, and cloud environments. Secret Server helps organizations manage and secure privileges 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, so you can set policies and 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.

A Centralized Vault

All those discovered bits of privileged access need to be documented, stored, managed, and audited somewhere. Secret Server's 256-bit encrypted vault secures all your "secrets", such as passwords, certificates, keys, proprietary files, and more. 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 can change the password to a privileged credential that, say, is used as a Service Account,

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.

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 locking away privileged access but 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 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.

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, and approval workflows, Secret Server provides a layered approach to ensuring the person requesting use of privileged access is authorized to do so – Multi-factor authentication ensures that even if a password is stolen, a malicious user can't use it to access Secret Server.

It also is valuable in rapid account recovery.

Automation

Automate as much as possible, as often as possible, to save your IT team time and effort. Automation within Secret Severs 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 to go 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 RDP, SSH, PuTTy, or Web Password Filler to connect the user wanting to make use of the privileged access to their desired system or application – all without ever disclosing the privileged credential to them at all.

Secret Server's session management, monitoring, and control establish oversight and accountability to the use of PAM sessions, 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 controlled 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 or unauthorized.

And, because Secret Server is proxying the session, each privileged session is monitored and recorded, providing security teams with 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 Delinea's Privileged Behavior Analytics solution 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 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 and sent to yourself and even an auditor via email – if you need it.

Disaster Recovery

No PAM solution 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 is accessible when an incident occurs.

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 entire organization.

We all know the success or failure of any security solution rests in its' *adoption,* and this includes a PAM solution. 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 a simple-to-use and sophisticated solution, from its wizard-based configurations to simplified setup; its APIs, custom scripts, and integrations to seamlessly adapt to your environment; and its completely customizable and configurable platform. Secret Server 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.

Secure privileged access, secure your entire organization

If you could make privileged credentials inaccessible and unusable to bad actors while making it easy for legitimate users to access and use — would you?

Secret Server is a fully-featured Privileged Access Management (PAM) solution empowering security and IT ops teams to confidently secure and manage all types of privileged accounts in any environment.

Secret Server empowers organizations to:

- Improve security
- Unburden IT teams
- Meet compliance needs
- Scale with your teams
- Minimize complexity
- Maintain productivity
- Boost performance
- Realize fast ROI

Secret Server works the way you work, starting with the most rapid deployment in the industry and giving you direct control to customize as you grow.

Learn more about Secret Server and try it free to improve your security posture today.

Delinea

Download now: delinea.com/products/secret-server

Quickly become conversational about Privileged Access Management.

By leveraging Privileged Access Management 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 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.