ConversationalGeek

Conversational Zero Trust Privileged Security

By Brien Posey (Microsoft MVP, Commercial Scientist Astronaut Candidate)

In this book, you will learn:

- The dangers that privileged access can pose to organizations
- What privilege sprawl is and why companies need to control it
- How to attain a stronger state of Zero Trust by moving from PAM to Zero Standing Privilege

2nd Edition

Sponsored by netwrix

Sponsored by Netwrix

Netwrix empowers information security and governance professionals to identify and protect sensitive data to reduce the risk of a breach.

Our solutions also limit the impact of attacks by helping IT teams detect, respond and recover from them faster and with less effort.

Over 13,500 organizations worldwide rely on Netwrix solutions to strengthen their security and compliance posture across all three primary attack vectors: data, identity and infrastructure.

For more details visit
www.netwrix.com

Conversational Zero Trust Privileged Security

By Brien Posey

ConversationalGeek®

Conversational Zero Trust Privileged Security

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:	Brien Posey
Project/Copy Editor:	Ian Whiteling
Content Reviewer(s):	Valeriya Rozhko
	Martin Cunnard
	Hano Grimm

Note from the Author

Hi, I'm Brien Posey, a 22x Microsoft MVP and commercial astronaut candidate. It's a weird career mix for sure, but it seems to work. Just recently for example, I did a Webcast on Azure Conditional Access one morning and then did an underwater spacewalk later that same afternoon.

In this particular Conversational Geek book, I wanted to talk about privileged accounts and some of the problems that they pose. The problem is that credential theft has reached epidemic proportions. It has gotten to the point that it is nearly impossible to guarantee the security of an organization's accounts. And of course, if an attacker gains access to a privileged account they can take over the network and do anything that they want.

Traditionally, privileged access management (PAM) comes into play here, but it has its downside as it still leaves accounts with standing privileged access in place. Zero Standing Privilege is a much more effective approach to zero trust that can be used to separate permissions from their associated accounts, providing just-in-time access to the account when legitimately needed, so that even if an account becomes compromised, it is useless to the attacker because the account's permissions are no longer standing. In this book, I will tell you all about it.

Brien M. Posey

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!

Shifting from PAM to Zero Standing Privilege: The Path to Zero Trust Privileged Security

"Hold on there, buddy! Not so fast!

There was a time in the early days of the PC when rights and permissions really weren't a thing. A user who sat down to use the PC had full, unrestricted permission to do anything they wanted. Sure, there were a few applications that were password protected, but at that time, security was built into the individual application, not the PC or its operating system.

Networks and multi-user systems put an end to the concept of unrestricted access for everyone. Suddenly, user accounts

became a necessity, as did implementing permissions that kept one user from accessing another user's data.

Eventually, these permissions evolved into not just a mechanism for controlling access to data, but also for controlling access to administrative controls. After all, it would be hugely problematic for a standard user to have an unrestricted ability to create and delete user accounts, grant rights to other users, or to reconfigure mission-critical systems. Having the ability to perform such tasks eventually became known as privileged access.

Privileged access is what allows network administrators and IT pros to do their jobs. Without privileged access, IT pros would be unable to set up user accounts, join PCs to a domain, install applications, or perform countless other administrative tasks. Although privileged access is essential for IT pros to have, however, it is not without its problems.

The Perils of Privileged Access

The main problem today with accounts having privileged access is that privileges can be abused by threat actors.

Nearly every type of cyberattack that involves gaining access to the victim organization's environment requires compromising a privileged account. For example, in 70% of ransomware attacks, lateral movement (the logical "jumping" from system to system) occurs[1]. This is only possible by compromising one or more privileged accounts that have access to multiple systems. It's generally accepted today that attackers seek to compromise administrative credentials to gain access to Active Directory to create additional accounts and grant further access to data, applications, and systems throughout the organization. In fact, use of stolen credentials is the number

---

[1] Coveware, *Quarterly Ransomware Report, Q2 2022* (2022)

one threat action in data breaches[2], with 84% of organizations having experienced this kind of identity-related breach in the past 12 months[3].

All of this is to say that privileged accounts, while necessary for day-to-day IT operations, can create risk if not properly secured because of the ways such accounts can be exploited.

The Status Quo for Protecting Privileged Accounts

Entirely eliminating privileged accounts is simply not an option for an organization since IT pros cannot do their jobs without these accounts. As such, organizations must carefully consider how best to protect privileged accounts. Unfortunately, this is one area where most organizations (and the IT industry as a whole) have fallen short.

As a general rule, technology evolves and improves over time. There are countless examples of this. Consider firewalls for example. At one time, firewalls were relatively unsophisticated and served only to block packets on specific ports. Over time, however, firewalls improved gaining the ability to perform stateful packet inspections and to block or allow traffic on a per application basis. Some firewalls even leverage machine learning in an effort to more accurately distinguish between an organization's normal traffic patterns and traffic patterns that might signal an attack.

One would probably expect the mechanisms that are used to protect privileged accounts to evolve in a similar way. Unfortunately, most organizations really have only had three

---

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

[3] Identity Defined Security Alliance, *Trends in Securing Digital Identities* (2022)

basic options historically for protecting these accounts (these three options are often used together):

- Least Privilege – The idea behind the principle of *least privilege* is that it is relatively rare for an administrator to need access to absolutely everything. Rather than giving an administrator unlimited access to everything, you can instead give an administrator limited administrative access. Suppose for example, that a particular administrator is responsible for maintaining an organization's email system. There is no reason for that administrator to have privileged access to the organization's file servers or its document management system. As such, least privilege would commonly be used to designate that administrator as a local admin (or something similar), which would give the administrator the permissions required to do their job, but nothing more.

Even when an organization adheres to the concept of least privilege, privilege sprawl can still occur. Privilege sprawl refers to an unintended accumulation of privileges that can happen as a result of a user or administrator being granted privileges, but not having those privileges revoked once they are no longer needed.

- Password Strength – Additionally, conventional wisdom has long held that, because the misuse of a privileged account can have such devastating consequences, privileged accounts should be

protected with far longer and more complex passwords than standard user accounts.

In 2022, a combination of a longer password (say, 10-characters) that has a mix of numbers, upper- and lower-case letters, and symbols would take five months to crack.

- Multi-Factor Authentication (MFA) – Lastly, the use of MFA helps ensure the user of a given privileged account is actually the credential's owner.

On the surface, these methods *do* provide additional protection to an organization's privileged credentials. However, when privileged accounts (even those limited through least privileged efforts) need to be used by multiple individuals, MFA becomes tough, and so does managing and maintaining complex passwords across so many users.

The point is that while it is important to protect user accounts with strong passwords, cybercriminals have any number of different techniques for gaining access to the account regardless of how strong or weak its password might be.

Privileged Access Management

The past few years have seen advances in protecting privileged accounts through the use of Privileged Access Management (PAM) solutions. These solutions generally include the following features:

- A Secure Vault – privileged credentials are stored within a secure database inaccessible to cybercriminals.

- A Policy Engine – This defines who has access to which credentials, when they can be used, and on which machines.

- Password Rotation – Rotating (that is, changing) the password after a set period of time or after each use of a credential helps to minimize the credential's misuse since cyber criminals won't necessarily have access to the current password or hash.

- An Authentication Interface – This is the sole means by which a sanctioned low-level user can access the requested privileged account from the PAM solution.

Use of PAM is a significant advancement over the initial three methods I previously mentioned, as PAM adds an element of actually *managing* the privileged credentials and their use that least privilege, strong passwords, and MFA don't offer.

So, you have some pretty viable options – the seemingly strongest, of which, is PAM – when it comes to protecting your privileged credentials. But how do these protective measures fare as your organization seeks to implement a state of Zero Trust?

Enter Zero Trust

One initiative that has been gaining momentum in recent years is the adoption of Zero Trust. The phrase "Zero Trust" is like countless other IT buzzwords that have been so overused that they have become almost ambiguous. That being the case, I want to spend a moment talking about what Zero Trust is and what it is not.

Buzzwords have become so pervasive throughout the IT industry that IBM once ran a commercial showing a group of conference attendees playing Buzzword Bingo. The attendees were given Bingo cards – like the one found at goto.cg/3SBNhTg – listing common IT buzzwords. Every time the speaker used a buzzword, the attendees marked it on their cards until someone eventually shouted BINGO.

First off, there is no product that you can buy to make your organization "Zero Trust". Certainly, there are some really good products out there that can help with your organization's Zero Trust initiatives, but you can't just install a piece of software and then consider your organization to be Zero Trust with no further effort.

So, if Zero Trust isn't software, what is it?

Zero Trust follows the cybersecurity philosophy of "*Never Trust, Always Verify*". It's the idea that nothing on your network should be implicitly trusted and provided access until it has been proven to be trustworthy. Although my definition of Zero Trust is really simple, that simplicity means that there is no such thing as a standard way of implementing Zero Trust.

Sure, there are some Zero Trust best practices that you can follow, but ultimately every organization will approach Zero Trust in a different way. Some organizations might adopt a few Zero Trust principles and stop there, while others may take Zero Trust to the extreme. There are also, of course, differences in the products, tools, and techniques that organizations use to create their Zero Trust architecture.

NIST created a *Zero Trust Architecture* special publication (SP 800-207) that does provide some solid guidance on what it takes to implement Zero Trust. You can find it at **goto.cg/3ducD67**

Zero Trust and Privileged Access

Now that I have spent a few moments discussing what Zero Trust is all about, let's revisit the concept of protecting privileged accounts to limit their misuse by cybercriminals through the lens of Zero Trust.

It's evident that, of the options covered in this eBook so far, PAM provides organizations with the greatest ability to protect against the misuse of privileged accounts. But how does PAM perform as you work towards a state of Zero Trust?

The answer lies in defining goals for your privileged access based on Zero Trust principles and then determining the appropriate technologies and policies to ensure privileges cannot be abused.

Setting Privilege Goals From Zero Trust

Since Zero Trust becomes the overarching aim, it's important to set high-level goals that will best protect privileged access through your adoption of Zero Trust. Although goal-setting sounds somewhat of a cliché, it's important nonetheless. After all, without having clearly stated goals an organization has nothing to work toward and no way of quantifying its success. There are a few goals you should aim for as you look to implement Zero Trust that will reduce (and potentially eliminate) the risk of privilege misuse.

Stop Lateral Movement

The first goal that an organization should set with regard to Zero Trust and privileged accounts is to prevent attackers from being able to perform lateral movement.

Oftentimes an attacker will not initially be in possession of privileged account credentials. Instead, the attacker might only have access to a standard user's credentials. These credentials usually do not allow the attacker to gain access to the critical resources that they are most interested in, but they can be used as a steppingstone in the quest to gain access to a privileged account that will in turn allow them to access what it is that they are truly interested in.

Additionally, one of the most common methods used by cyber criminals is *credential theft*. It's simple, it's efficient, and it works. Typically, all an attacker has to do is display a fake login screen and trick the privileged user (usually via phishing attack) into entering their credentials. As an alternative, an attacker may resort to installing a key logger that will record the password when it is typed.

Another way that attackers gain access to privileged accounts is by extracting password hashes (which is relatively easy to do with tools like Mimikatz and LaZagne) from compromised endpoints – either using it as part of a Pass the Hash attack or by comparing extracted hashes against a database of leaked accounts. Keep in mind that the account's password may be in the leaked password database even if the account has never been compromised. All that is required is for someone else in the world (whose account has been compromised) to have used the same password. It doesn't matter that the person's username is different. The only thing that matters is that there is a matching password hash in the cyber criminal's database.

What makes lateral movement possible is the standing privileged access that exists in all the accounts compromised along the way that provided the attacker with access to

systems, data, and Active Directory. It's an all-too common tale of threat actions used in data breaches, ransomware attacks, cyber fraud attacks, island hopping, and more.

Because this technique makes it so easy for an attacker to gain access to privileged accounts, an organization must look for ways to prevent attackers from making lateral movements throughout the network.

There are plenty of other ways threat actors address lateral movement's requirement for privileged credentials. A full list can be found in the MITRE ATT&CK Framework at goto.cg/3RZBPQc

Eliminate Privilege Sprawl

Another major goal for an organization's Zero Trust initiatives should be to put an end to privilege sprawl. As previously explained, privilege sprawl refers to the accumulation of privileges that occur over time: privileges accrue by virtue of new users wanting privileged access to data, applications, or systems, that often remain in place even after the user no longer needs those privileges. Users change roles within the organization, so new access is granted, but rarely – if ever – are privileges taken away.

Think of the last time you went through a group's membership – whether in Active Directory or on a Windows server's local Security Accounts Manager (SAM) database – to validate that it was correct? Probably never. Over time, it's possible to see hundreds and even thousands of unnecessary privileged accounts on systems across the enterprise.

Some organizations create multiple accounts for each member of the IT staff – a privileged account for performing administrative tasks and a standard account for more mundane tasks such as checking email. While this approach can improve security it's also cumbersome and leads to a lot of frustration due to the fact that an IT pro may have to log out and log in with a different account every time they have to do something.

The Real Goal: Eliminate Standing Privilege

NIST defines one of the major tenets of Zero Trust to be (emphasis is mine):

> "**Access** to individual enterprise resources
> is **granted** on a **per-session** basis."

PAM seems to fit the bill in that it provides temporary access to a privileged account. But there is no way of 100% guaranteeing that an account will *never* be compromised. And, while you can use PAM to lockdown access to a privileged credential, no matter what you do to protect an account, there is always a chance that a determined attacker will somehow gain access to that account *outside of PAM.*

For example, a member of IT could check out a privileged credential from a PAM solution and use that credential for an 8-hour period, and then check the credential back in – at which time the password would be rotated to a new one. If an attacker was to compromise one of the managed systems within the 8-hour period, the normal previously mentioned methods to attain credentials would still be viable – despite having PAM in place. And with their Access Token being issued at logon, there may be quite a lot they can do with that compromised account while still logged on.

The reason this is possible is *standing privilege* – the idea that you have accounts that have been granted privilege to data, applications, and systems regardless of whether the accounts are in use or not. What PAM does is to separate the attacker from the credential, but should an attacker gain access to the credential, they get the standing privileges assigned to it. This is in direct conflict to the Zero Trust tenet I just mentioned – if an attacker has any ability to compromise and misuse a privileged account, *you never had Zero Trust to begin with.*

That being the case, the best thing that you can do to protect privileged access is to completely *remove the privileges from privileged accounts*. Normally when privileges are assigned to an account, those privileges are persistent. In other words, the privileges are granted and are valid 24/7, and available whenever that account is used. Since you can never completely do away with privileges, your goal should instead be to get rid of *standing privileges* that are always associated with an account, turning that admin account into a regular user. This way, should an attacker gain access to what would normally be a privileged account, they can't use it for anything because all of the privileges have been removed.

This idea of removing privileges from privileged accounts represents the very essence of Zero Trust. The idea is that you do not trust the account, and therefore do not assign any standing privileges to it – only "trusting" the account to have privileges once the user of the account is "verified". As previously noted, however, privileges are necessary in order for the IT department to do their jobs and for keeping the network healthy.

So how can you remove standing privileges without undermining your own ability to be able to manage the network in the process?

Privileged Access Management and OnDemand Privilege

Although Privileged Access Management is a good idea (and does bring organizations closer to Zero Trust), it isn't perfect. There is a transformative new approach, OnDemand Privilege, which combines traditional PAM capabilities with a Zero Standing Privilege approach. It ensures the right person gets the right level of privilege at the right time. That's the privilege they need when they need it, and not when they don't, delivering the best possible protection for privileged accounts.

Implementing OnDemand Privilege could be summarized as a three-step process:

Step 1: Discover Where You Have Privileged Access

The first step is a comprehensive permissions audit of every endpoint. The goal here is to identify the privileged access currently assigned to all of your existing systems. Doing this facilitates visibility into existing privilege sprawl and can serve as the basis for determining whether the environment is becoming more secure as you implement the remaining parts of OnDemand Privilege.

Step 2: Establish Just-In-Time Administration (JIT)

Do all those accounts discovered and documented have privileged access to your endpoints, servers, and Active Directory? That's all your standing privilege. The next step towards OnDemand Privilege is to shift your privileged access from *standing* to *just-in-time* (JIT). This requires a solution enabling OnDemand Privilege. The result is that privileged access inventory (who has access where) remains within the OnDemand Privilege solution, but the actual access within your environment is *stripped away*. This requires that anyone wanting to use their privileged access will need to request it from the OnDemand Privilege solution.

Some PAM solutions use the term "just-In-time" to mean granting a low-level account access to a separate privileged account. This leaves your environment with all of its legacy standing privilege and doesn't get you any closer to Zero Trust.

At the time of request, the privileged permissions are *assigned* on a temporary basis to the account and are usually only in effect for a limited period. The idea is to grant the account the required permissions just long enough to allow the administrator to do their job, and then revoke those permissions, preventing the account from being misused.

Now, you should be asking the question "exactly how are these privileges granted?" After all, if OnDemand Privilege is, say, adding users to groups dynamically, you'd need to wait for AD to fully propagate to every Domain Controller before the user could actually use the privileged access. True JIT is achieved by leaving the group memberships in place and removing the permissions from the endpoint or system itself, making the JIT assignment by granting local permissions in real-time.

Step 3: Establish Zero Standing Privilege (ZSP)

In the end, you really only want a few instances of standing privilege and your local and domain (built-in) Administrator accounts should only be treated as a "break glass" option. So, anytime a new assignment of privileged access is made, it's managed and audited by OnDemand Privilege, requiring the admin to request their privileged access, and eliminating any standing privileges.

This is really important; if you aren't working to establish ZSP, you're not stopping the bleed. PAM solutions are only effective if *every* credential (over time) is managed and audited within the solution. OnDemand Privilege works to ensure that no new

outside privilege exists, stopping the bleed and keeping privilege controlled.

ZSP is also the end result of implementing OnDemand Privilege. An attacker who gains access to a (normally) privileged account would be incapable of leveraging anything other than the account's low-level capabilities. This helps achieve the goals of Zero Trust while both eliminating privilege sprawl and – more importantly – stopping lateral movement.

Remember, no elevated privileges, no lateral movement.

But since legitimate users still need to do their job, they use a portal to access OnDemand Privilege and request elevated permissions for just long enough to create the required accounts. In this case, permission might be granted for 10 minutes. At the end of those 10 minutes, the permissions are revoked and the account is no longer able to exercise privileged access until the next time they request (and are granted) permission to do so.

Zero Trust: It Takes More Than Just PAM

PAM alone doesn't help to achieve a state of Zero Trust; the standing privilege that continues to exist flies in the face of Zero Trust's desire to make the granting of access 100% dynamic in nature. To achieve a true state of Zero Trust, it's necessary to achieve ZSP while using JIT to empower sanctioned users to do their job while making the environment useless to cybercriminals.

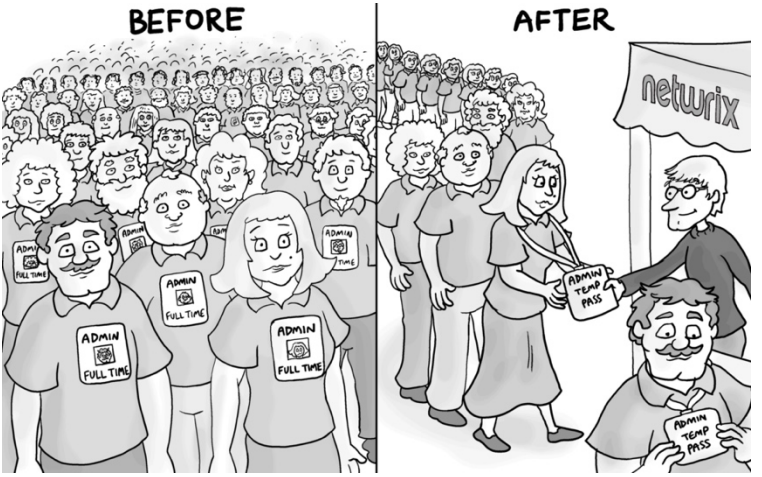
The Big Takeaways

Privileged accounts pose a major threat to an organization's overall security. At the same time though, these accounts are necessary in order for IT pros to be able to do their jobs. Previously, eliminating privileged accounts was not an option. In addition, organizations have explored various techniques – including the use of traditional PAM – for reducing the risk posed by privileged accounts, but the standing privileged access and privilege sprawl that remains in the environment actually further puts it at risk of a successful cyberattack.

Since there is no way to 100% guarantee that an account will remain secure, as organizations work to adopt Zero Trust principles, the best thing that you can do is to shift to an approach where privileged identities and permissions are orchestrated on demand and removed when no longer required. That way, if an account does become compromised, it will be useless to the attacker.

While there are any number of ways to accomplish this, one of the best approaches involves the use of ephemeral accounts. An ephemeral account is essentially a temporary account that is created on demand. The idea is that when privileged operations are required, an account will be dynamically generated, and then automatically removed once the task is complete. Because the account no longer exists, it cannot be compromised. These ephemeral accounts typically exist as activity tokens, and are transparent to the administrator who is performing the privileged operation.

Sponsor Chapter: Achieving Zero Trust and OnDemand Privilege with Netwrix Privilege Secure



The biggest problem with privileged access today is that once it's been granted, the user account afforded the elevated privileges (whether directly or via group membership) continually maintains those privileges in what we've referred to as *standing privilege*, which is what separates traditional PAM implementations from Zero Trust.

The concept of Zero Trust holds that *no access* should be granted until the account requesting it is validated and approved. While modern implementations of Zero Trust leverage a traditional PAM solution to store and hand out privileged credentials on an as-needed basis to only those sanctioned by policy, there's still the issue that there are many credentials that have standing privileged access: accounts persist on systems even if their credentials are vaulted. Even with system-generated strong passwords and password

rotation, the fact remains that standing access for these privileged accounts presents a massive attack surface that attackers routinely exploit.

If you're not using a traditional PAM solution, you're in even worse shape from a Zero Trust standpoint, as the passwords for your privileged credentials likely aren't changed on a regular basis and, therefore, are susceptible to brute force, pass the hash, and other types of attacks aimed at misusing credentials.

And to make matters worse, no organization is safe from privilege sprawl that exists over time due to the repurposing of groups, a lack of group attestation, and the likely nonexistence of actually *removing* an account's permissions. All of this only makes the case that any standing privilege that is assumed to exist within an organization is far worse than believed.

So, a far more mature implementation of Zero Trust holds that the *standing privilege itself* afforded the privileged credentials (regardless of whether they reside within a PAM solution or not) shouldn't exist either – that is, until access is needed.

This is where the concept of Zero Standing Privilege (ZSP) comes into play – to heighten the Zero Trust level, it's necessary to augment any management of privileged accounts with an ability to minimize privilege sprawl and make lateral movement by threat actors all but impossible.

To accomplish better Zero Trust security, organizations must turn to solutions like *Netwrix Privilege Secure* that enable organizations to achieve an OnDemand Privilege state.

Netwrix Privilege Secure is an agentless *Lateral Movement Prevention* solution that helps customers achieve ZSP across all

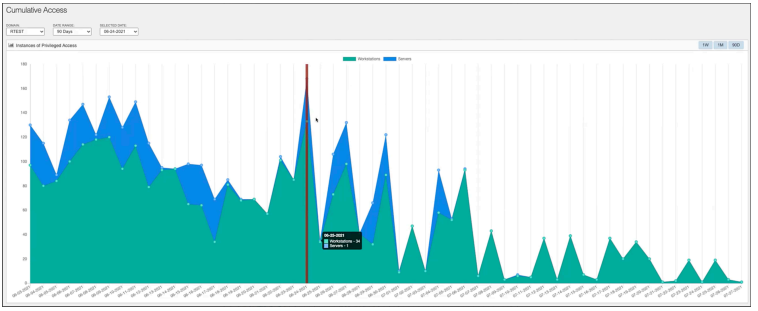
systems on the network or in the cloud while still facilitating privileged access just-in-time for administrators to get their job done across operating systems, directories, cloud databases and network devices.

It accomplishes this in a number of ways:

Eliminate Privilege Account Exposure

Netwrix Privilege Secure starts by creating visibility into your privileged accounts. By inspecting your Active Directory domains and scanning every Windows, Linux, and Mac computer, *Netwrix Privilege Secure* identifies every single user and group that has direct or nested admin access to your systems. This is your attack surface, as threat actors can use these accounts to move laterally between systems.

By maintaining this degree of visibility into privileged accounts within an environment *Netwrix Privilege Secure* can help visualize privilege sprawl, both as a point in time, and as a trend to help organizations understand whether they are reducing their privilege sprawl and, therefore, their attack surface.



Netwrix Privilege Secure dashboard showing a reduction in privilege sprawl

Next, *Netwrix Privilege Secure's* protect mode facilitates the removal of privileged access granted through the use of the

Local Admins group to remove the enterprise-wide privilege sprawl.

In the same manner, *Netwrix Privilege Secure* takes advantage of integration with an XDR solution's REST APIs and response capabilities to run tasks on any remote systems that are not connected to the corporate network. This ensures every system in the environment has been scanned, accounts have been identified, and standing access has been removed.

In the end, only your "break glass" admin accounts (e.g., Administrator) are left with standing privileges – along with *Netwrix Privilege Secure* having administrative access to all your endpoints either directly or via XDR solutions.

But, now that you have, in essence, documented all the access that *was* in place and then removed it, how do you still maintain an ability to use privileged access in a way that adheres to the principles of Zero Trust?

Orchestrated Privilege Access

Netwrix Privilege Secure keeps track of the previously granted access and now administers just-in-time privileged account access; a user authenticates to *Netwrix Privilege Secure* using their own user account and MFA, requests privileged access to a particular system, and they are dynamically added as a privileged user on that system. Once finished, *Netwrix Privilege Secure* can either manually be instructed by the user to remove the privileged access, or *Netwrix Privilege Secure* can do it automatically – and the user goes back to being a low-level user account.

The end result is zero standing privilege, and yet everyone is able to request the needed privileged access and get their job done – all while minimizing the attack surface.

Achieving a State of Zero Trust

The goal of Zero Trust is "never trust, always verify". The use of methods like least privilege, the use of separate user and admin accounts, and even locking up privileged accounts in a traditional PAM vault all get you closer to Zero Trust. But to truly be in a state of never trusting, there can't be *any chance* that an account with privileged access can bypass security controls and be misused to gain access to systems, applications, and data within your environment.

The use of *Netwrix Privilege Secure* puts an extra emphasis on Zero Trust's "*never*". Traditional PAM's standard of verifying the user of a privileged credential as the owner of it (or the sanctioned user, in the case of traditional PAM) and granting the use of a privileged account is one example of how the use of the privileged access isn't trusted until the authentication is verified.

But *Netwrix Privilege Secure* goes a step further with its "*never*", taking a next generation approach by completely eliminating standing privileges, adding in just-in-time orchestration to reduce the attack surface to an absolute minimum.

To sum up, with *Netwrix Privilege Secure* you enjoy:

- Better security with a Zero Standing Privilege approach, removing privilege and dynamically creating it on-demand as required. This reduces the attack surface and enforces the principle of least privilege.
- Ease of use – a key requirement, particularly when end-users are brought in as stakeholders. Netwrix Privilege Secure is designed around workflow for the administrator setting up and maintaining the product, and the end-users who all have different standard operating procedures.

- Time to value – a key factor where many projects are typically time sensitive. Netwrix Privilege Secure is quick to implement and easy to use, so organizations can start realizing the benefits of Zero Standing Privilege quickly.

Find out more about *Netwrix Privilege Secure* at https://www.netwrix.com/privilege_secure.html

Minimize the risk related to privileged access with Netwrix Privileged Access Management software

- Gain dynamic and continuous visibility into privileged accounts across your systems with live and retrospective session monitoring.
- Replace privileged accounts with just-in-time privileged access to slash your attack surface area.
- Clean up unnecessary administrative accounts before they can be exploited by attackers.
- Further secure privileged access with multifactor authentication (MFA).
- Get detailed audit trails and reports to prove regulatory compliance with SOX, PCI-DSS, HIPAA, and GDPR.

Request One-to-One Demo

https://www.netwrix.com/pam

Quickly become conversational about Zero Trust Privileged Security and Zero Standing Privilege.

Over the years permissions have evolved into not just a mechanism for controlling access to data, but also for controlling access to administrative controls. Without privileged access, IT pros would be unable to perform countless administrative tasks. However, privileged access can be abused. In today's security-conscious world organizations need to move beyond simple role-based privileges to Zero Standing Privilege. Over the course of this ebook we'll look at how you can achieve that.

About Brien Posey

Brien Posey is a 22-time Microsoft MVP and an internationally published author and conference speaker with over two decades of IT experience. In addition to his technology work, Brien is also a Commercial Scientist Astronaut candidate.