WHITE PAPER

Remediant

A STEP-BY-STEP GUIDE: ACHIEVING ZERO STANDING PRIVILEGE

A STEP-BY-STEP GUIDE:
ACHIEVING ZERO STANDING PRIVILEGE

INTRODUCTION

The credential has become a commodity that will be breached. 74% of breached organizations admitted the breach involved access to a privileged account. In addition, *The Verizon Data Breach Investigations Report* (DBIR) found that out of all attacks, 29% of total breaches involved the use of stolen credentials, second only to phishing. Once a credential is compromised, privileged access management solutions are rendered useless.

The underlying reason behind this (and why administrator credentials continue to be low hanging fruit for attackers) is the access the credentials provide. Specifically, it is the 24x7x365 always on, high levels of access that these administrator credentials provide that can be used to move laterally across a network, steal sensitive data, or deploy ransomware. The average privileged access management or endpoint privilege management solution was not purpose built to address this risk.

This key risk is called "standing privilege" and the emerging security model that addresses the risk is called Zero Standing Privilege.

WHAT IS STANDING PRIVILEGE?

Standing privilege refers to administrator accounts with "always on" 24x7x365 privileged access. On average, at a large enterprise, we find 480 users with admin access to the average employee workstation (at companies with >15K devices).

480

Average number of admins with 24x7 access to each workstation[1]

1,291

Admins with access to more than 2,000 systems

31,814

Systems with **more than 800 privileged access users**

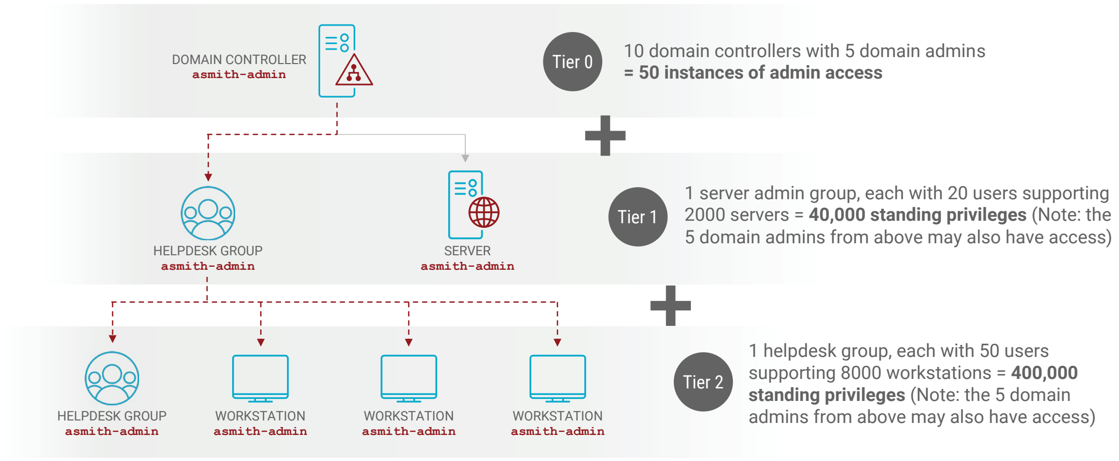
[1] For organizations with 15,000+ endpoints

Figure 1. The state of standing privilege in the average enterprise environment today (as seen by Remediant)

HOW DOES THIS OCCUR?

These privileges are typically in the form of privileged group memberships or device level permissions that allow the execution of privileged commands. So, even if a user is not explicitly given access to a specific server or workstation, their domain or group level permissions would allow them access to that server or workstation whenever they need it.

Privileged access spreads and is "standing" and an easy target



10 domain controllers with 5 domain admins
= 50 instances of admin access

1 server admin group, each with 20 users supporting 2000 servers = **40,000 standing privileges** (Note: the 5 domain admins from above may also have access)

1 helpdesk group, each with 50 users supporting 8000 workstations = **400,000 standing privileges** (Note: the 5 domain admins from above may also have access)

Figure 2. How administrator privileges spread

For more information about how standing privilege manifests itself and proliferates across a network, Dr. Shane Shook from ForgePoint Capital provides a great overview here: *https://www.remediant.com/blog/standing-privilege-is-an-apt-factor.*

WHY DOES THIS OCCUR?

There are three key reasons why standing privilege is prevalent:

1 **Access is given through groups to IT Helpdesk and Server Admins to resolve issues quickly:** In most cases, organizations provide this level of 24x7x365 access to enable administrators to do their jobs effectively. The two personas we at Remediant see with this type of access are IT Helpdesk users and systems administrators.

2 **Managing groups at a granular level becomes very complex very quickly,** so admins always have more access than they need.

3 **Administrator rights change over time very regularly, and this is something that a lot of attackers know, and a lot of security teams don't know,** which is that admin rights can change for many different reasons. New members are always added as Helpdesks and Administrator teams grow. However, old members who leave their teams or the company, aren't always removed in a timely fashion. Group membership changes, so if an active directory group confers some amount of privileged access and the membership of that group changes, then the amount of privileged access in the ecosystem correspondingly changes. Local accounts might be added or removed, conferring or removing levels of privileged access, and GPOs can change, which can confer privileged access across the entire enterprise for a set of accounts or a set of groups.

What this ultimately results in is an invisible sprawl of administrator access across the enterprise that is available 24x7x365 and more importantly, available to an attacker from the average employee workstation. If an attacker is able to phish their way into an average employee's workstation, they now have the proverbial "keys to the kingdom."

WHY DOES THIS MATTER?

This standing access increases an organization's attack surface and can impact the network as follows:

- One compromised password exposes the entire network
- Standing credentials are the primary mode of ransomware spread - Each standing privileged account is an opening to move laterally
- Standing access violates principle of least privilege – even with a Privileged Access Management solution in place that touts "zero trust"

This is why 74% of breached organizations admit that their breach involved a compromised privileged credential.

ADDRESSING THE PROBLEM

The reason we as an industry have failed miserably at addressing standing privilege is because we struggle to answer two simple questions:

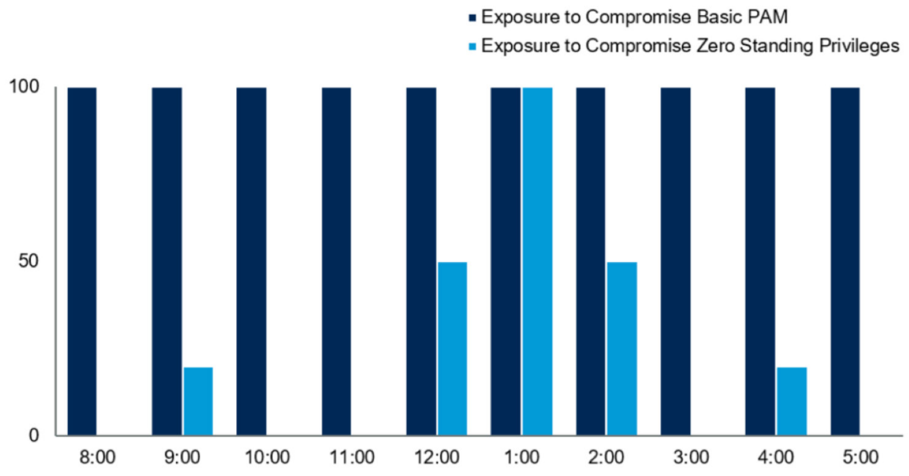
1. *What admin credentials exist and have standing access? (You cannot protect what you do not know exists.)*
2. *How do you protect them?*

Zero standing privilege is an emerging, reframed approach to privileged access management (PAM) that addresses both questions.

INTRODUCING ZERO STANDING PRIVILEGE

If we agree that standing privilege is defined as that accounts have persistent privilege access for all time on some set of systems. Zero standing privilege is the exact opposite. It is the purest form of just-in-time administrator access, ensuring that the principle of least privilege is enforced by granting, to authorized users, the privileged access they need for the minimum time and only the minimum rights that they need. This elimination of standing privilege through zero standing privilege is really a key inflection point in the understanding of privileged access today. The figure below outlines the risk exposure of an account with standing privileges versus an account in a Zero Standing Privilege environment:

A Normal Day for a Windows Administrator



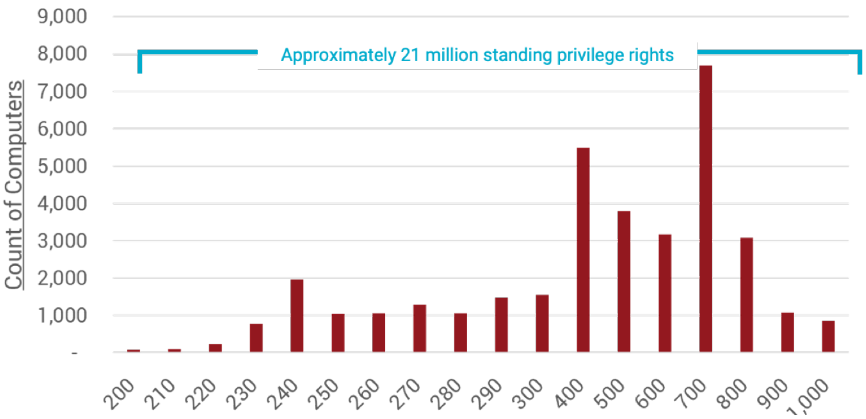
Source: Gartner
ID: 389807

Figure 3. Risk exposure of an account with standing privileges versus an account with zero standing privilege

ACHIEVING ZERO STANDING PRIVILEGE

1 MEASURE STANDING PRIVILEGE

As mentioned above, the first step to addressing standing privilege is understanding what administrator credentials exist. There are two key components to measuring standing privilege successfully. The first component is the ability to discover and identify persistent accounts across workstations and servers and map out admin access on a system by system basis:

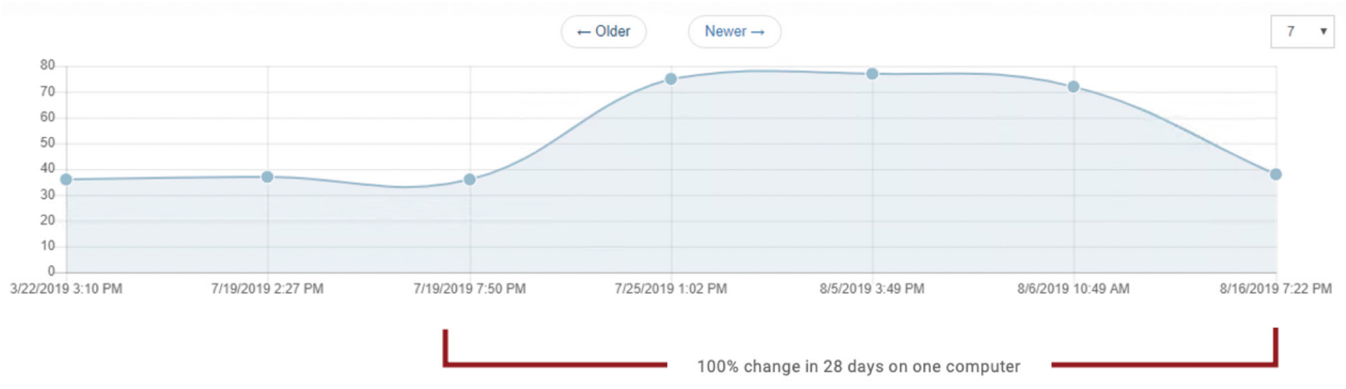


Approximately 21 million standing privilege rights

Figure 4. Example chart describing the number of admin credentials in an enterprise environment – 21M admin rights across ~50K systems

The second component is the ability to measure changes to access over time. As mentioned in previous sections, admin rights can change for many different reasons. New members are always added as Helpdesks and Administrator teams grow. However, old members who leave their teams or the company, aren't always removed in a timely fashion.

What Admin Credentials Exist Today?



100% change in 28 days on one computer

Figure 5. Example - the number of admin credentials in an enterprise environment – 21M admin rights across ~50K systems

Once standing privilege is measured, it can be managed. This brings us to the second question – how do you protect and ultimately achieve Zero Standing Privilege?

The next three steps outline a phased approach to protecting an enterprise environment and achieving Zero Standing Privilege:

2 FREEZE ACCESS TO SYSTEMS TO PREVENT NET NEW ADMIN ACCESS FROM BEING CREATED

The first step to remediating standing privilege is to "stop the bleeding" by preventing the creation of new rogue administrator accounts are not created or bifurcated. It is critical that firms have the ability to do this across all types of systems (Windows, Mac, Linux) and all types of access (local, group, domain).

3 REVIEW ACCESS AND REMOVE UNAUTHORIZED ACCOUNTS

Once the "bleeding" has stopped, the next step is to review the access identified in step 1 and determine which accounts are authorized and which accounts are not (and to what system(s)). Unauthorized access should then be revoked, ideally in bulk, to quickly mitigate one of the accounts being compromised.

4 SHIFT APPROVED ADMINISTRATORS TO JUST-IN-TIME ACCESS

The last step to achieving Zero Standing Privilege is shift administrators into a just-in-time mode that allows them to gain access to the system they need to perform required tasks, but only for the right time frame and only to the right system(s). Access should be revoked once the work is complete and only provisioned back (limited to the right system for the right time frame) when needed again.

CONCLUSION

"Effective PAM practice embraces the entire concept of least privilege,
granting only the right privileges to only the right system and to only
the right person for only the right reason at only the right time."

MICHAEL KELLEY GARTNER - REMOVE STANDING PRIVILEGES THROUGH A JUST-IN-TIME PAM APPROACH

Zero Standing Privilege is an inflection point in privilege management. It is encouraging to see the market has started to recognize standing privilege as a key risk that needs to be addressed and that vaulting secrets and rotating local admin passwords on critical servers are not sufficient. Attackers are targeting workstations as the low hanging fruit and using the admin access available from those workstations to spread across networks.

The credential has become a commodity that will be breached. So, focus and spend needs to start shifting towards the access the credentials provide. As an industry, if we do not take a Zero Standing Privilege stance in our environments, stolen credentials will continue as attacker low hanging fruit and continue to contribute to 80% of data breaches.

Remediant
Two Embarcadero Center, 8th Floor
San Francisco, CA 94111
(415) 854-8771 www.remediant.com

Remediant leads with innovation, delivering enterprise-class cybersecurity solutions that enable real-time monitoring, zero trust protection of privileged accounts and Just-In-Time Administration (JITA) across IT/Security ecosystems. We protect organizations from stolen credentials being used to take their data, which is the #1 attack vector across all breaches.