

Privileged Access Management for Today's Cyber Threats

Evolution of Privileged Access Management



**PASSWORD
VAULTING**



**PROXY
SERVERS**



**DEDICATED
ACCOUNTS**

Evolution of Privileged Access Management



**STILL
RELEVANT?**

Lateral Movement Attack Surface

- Accounts retain their privilege 24x7 and are easy targets
- Artifacts often left behind that can be exploited

Complex to Manage

- Legacy PAM solutions were designed for specific use and have not evolved

Evolution of Privileged Access Management



THE FUTURE OF PAM

REMOVE Lateral Movement Attack Surface

- Zero attack surface for adversaries to exploit
- Create privilege on-demand / remove when not in use

REDUCE Complexity

- Simplify – life doesn't have to be complicated!

Keep it Under Control

Orchestrate it...

The Power of Privilege Orchestration

Before Session

jsmith-adm



Account disabled / no privileges / no attack surface

During Session

jsmith-adm



Account enabled / just-enough privilege for task

After Session

jsmith-adm



Account disabled / no privileges / no attack surface

The Power of Identity Orchestration

Before Session



Account doesn't exist / no attack surfaces

During Session

jsmith4hs9
k3h86fd



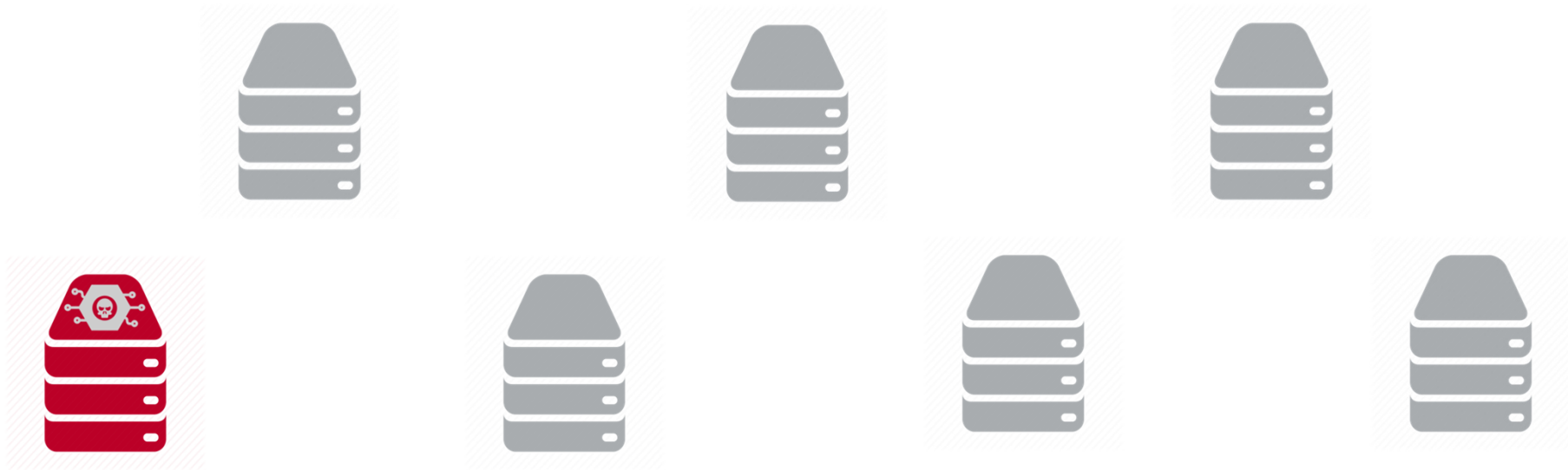
Ephemeral account created /
just-enough privilege for task

After Session



Account removed / no attack surfaces

Getting to Zero Standing Privilege



Clearing ALL Attack Surfaces

RDP

Services

Kerberos Tickets

File Shares

Just-in-Time Orchestration

Create what you need to do your specific task at the point you need it, and remove the attack surface when you are not using it

Identity Orchestration

Privilege Orchestration

- Create / Enable Accounts
- Add / Remove Permissions
- Enable/Disable RDP
- Purge Kerberos Tickets
- Group Protection

Endpoint Orchestration

- Pre/Post File Comparison
- Dynamic SMB Shares
- Custom PowerShell
- Dynamic sudoers

The screenshot displays the Netwrix Privilege Secure web interface. The left sidebar contains navigation options: My Activities, Dashboard, Policy, Users & Groups, Resources, Credentials, Activities, Activity Groups, Configuration, Service Nodes, and Audit & Reporting. The main content area is titled 'Home > Activities' and shows a search bar and a list of activities. The 'Domain Admin' activity is selected, showing its configuration details. The configuration includes a description field, platform (Active Directory), login account type (Activity Token), and activity type (Interactive). The login account template is set to '%targetdomain%\%samaccountname%'. There are checkboxes for 'Create Account' and 'Delete After Use'. The 'Pre-Session (Grant)' section includes actions like 'Create or Enable Account', 'Add to Domain Admins', and 'Enable RDP on Host'. The 'Post-Session (Remove)' section includes actions like 'Logoff User', 'Remove from Domain Admins', 'Disable RDP on Host', 'Invoke Protection Policy', and 'Delete Account'.

Demonstration

5 Key Take Aways



No standing privilege –
no attack surface



Don't just *manage*
privileges, **remove** them!



PAM does not have to be
hard to deploy, or manage



PAM can easily scale
from 3 to 30,000 users
and be performant



You can advance to
Zero Standing Privilege
step-by-step

**Soon, you'll forget all about
password vaults**

Make Admins Happy

Dealing with PAM Stress...

Privileged Access Management Stress or what?

"It's taken over 5 minutes for the UI to load this morning!"

"I can't believe how complicated it is to do simple things..."



"I just want to do my job!!"

"I have to use RDP to access my database - its so unworkable..."

Life Shouldn't be Complicated!

- Clean, simple, structured UI workflow - front-end and back-end
- Fits with your admins' standard operating procedure
- Reduces RDS overhead and use of jump hosts for applications
- Different strokes... a Linux admin works entirely differently to a Windows admin