netwrix

PAM Roadmap

Key Strategies for Effective Deployment and Team Engagement

- 36 years in IT
- 26 years in cybersecurity and access management
- Built #2 PAM solution on the market
- Patent awarded for JIT Orchestration

Martin Cannard

VP of Product Strategy

Martin.Cannard@netwrix.com

Poll

Agenda

01 History of PAM

02 PAM Approaches

03 Understanding Workflow Mapping

04 Deployment Best Practices

05 Strategies for Introducing PAM

06 New Methodologies for Easier Transition

Evolution of Privileged Access Management

PASSWORD VAULTING

PROXY SERVERS

DEDICATED ACCOUNTS

Evolution of Privileged Access Management

STILL RELEVANT?

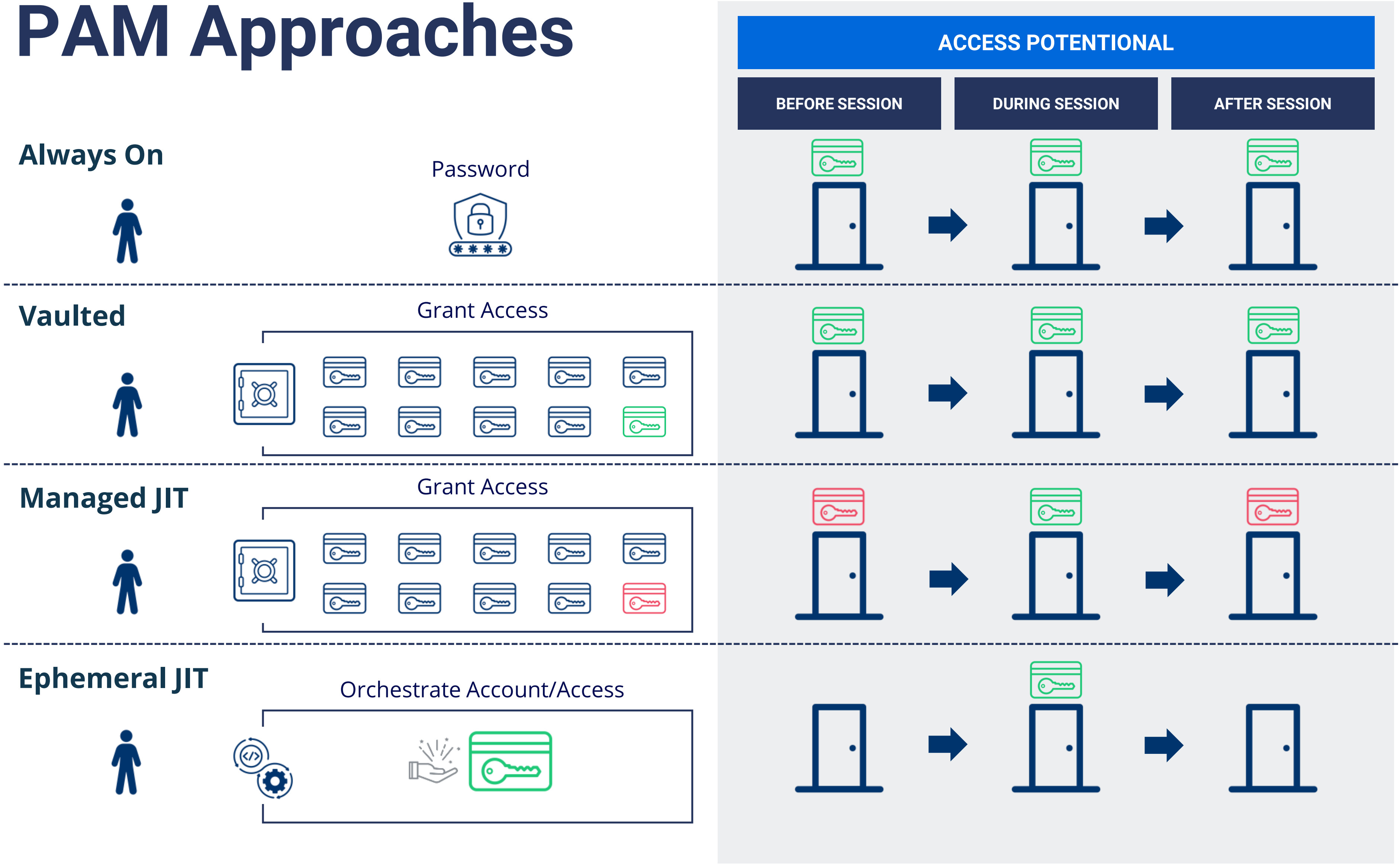
Lateral Movement Attack Surface

- 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

PAM Approaches



		ACCESS POTENTIONAL		
		BEFORE SESSION	DURING SESSION	AFTER SESSION
Always On	Password	🟩	🟩	🟩
Vaulted	Grant Access	🟩	🟩	🟩
Managed JIT	Grant Access	🟥	🟩	🟥
Ephemeral JIT	Orchestrate Account/Access		🟩	

Always On: Access is persistent and highly susceptible to compromise

Vaulted: The only difference between Vaulted and Always On is you don’t know the password

Managed JIT: Managed JIT is Vaulted, but the Account is non-privileged/disabled when not in use.

Managed JIT is in essence as good as Ephemeral JIT and overcomes the challenge of creating new accounts every time.

Ephemeral JIT: Ephemeral is ideal for the highest risk scenarios (e.g., logging into a Domain Controller with Domain Admin privileges) or when you’re doing a random task

🟩 = Available and Enabled

🟥 = Available, but Disabled

Common Use Case Examples

Use Case	Approach	Why?
Entra ID admin needs to log onto Entra ID as a Global Administrator	Managed JIT	Entra ID is making MFA mandatory for all user accounts. This will make it impractical to use an ephemeral account where MFA will have to added for every session. Instead, a managed account can be used that has pre-existing MFA configured.
AD admin needs to run Active Directory Users and Computers as Domain Admin	Ephemeral JIT	Here we do not worry so much about having a persistent user profile on the servers as most Domain Admin activities are point-in-time administrative events. An ephemeral account works well here as a new profile is created for each session.
Helpdesk admin needs to update drivers on a Windows Desktop	Ephemeral JIT Managed JIT	For tasks relating to administration of desktops connected to the network, an ephemeral account may be used. For remote devices, a managed account works best where we do not have access to the desktop.
Linux admin needs to run backup scripts on an AWS EC2 instance using AD authentication	Ephemeral JIT	For use cases where an AD bridge would normally be necessary, PAM can often authenticate the user via their AD account and dynamically create an ephemeral account on the Linux target.
Database admin needs to launch SSMS to run queries against a database	Managed JIT	Due to latency creating database accounts and launching DBMS tools, a managed account is preferable for this use case rather than ephemeral.
Network device admin needs to modify settings on a firewall	Managed JIT	Generally, access is via a managed local account or managed AD account. It is possible to use ephemeral accounts, but latency issues can crop up in distributed environments; managed is a safer option.
Social media admin needs to update Facebook page	Always On / Vaulted	In this use case we may not be able to rotate the password, but we can store it in a secret vault such that the user may be logged on but not aware of the password value.

Workflow Mapping

How and Why

Not all jobs are the same

Carolyn
DBA

Opens DBMS tools on her desktop and connects directly to database using her own account. She dislikes PAM tools that force access through RDP

Jeff
AD Admin

Typically logs onto servers via RDP, through a local RDP connection manager and runs RSAT applications for maintenance

Michael
Programmer

Creates scripts and applications but needs to have access to accounts with privilege for them to run

Leonard
Network Admin

Manages network devices. Some are able to integrate through AD with TACACS and others need direct login using native accounts

Jenna
Helpdesk

Takes calls from end users and will occasionally log on directly to the user systems to install software, update drivers etc.

Map Current to New Workflows

Carolyn
DBA

Consider using tools that allow applications to be opened from the desktop that do not require the use of RDS remoteapps

Jeff
AD Admin

Look for a workflow that allows Jeff to open his sessions directly from his connection tool. As usage is generally app-based, consider ephemeral JIT

Michael
Programmer

Look for tools with an API to make integration easy. Look for the native ability to run CLI environments under the context of privilege

Leonard
Network Admin

Launching SSH and web sessions without having to go through a PAM tool web UI would retain workflow. AD authentication for normalization

Jenna
Helpdesk

Look for tools that integrate with existing remote desktop products. If supported, use JIT access to keep local attack surface to a minimum

Deployment Fundamentals

Important things to consider

PAM Deployment Common Issues

You might never finish

- Deploying PAM is hard

Your users will push back

- Workarounds or failure to adopt leads to security gaps

Priorities can shift

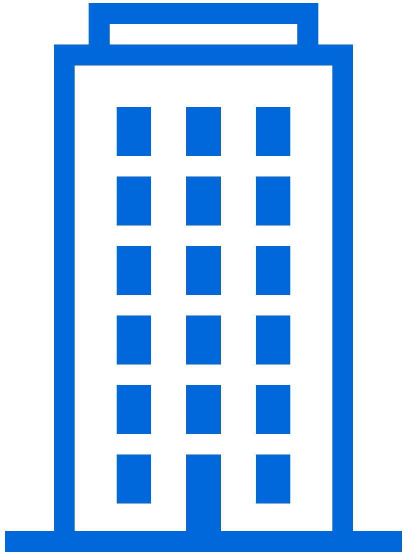
- Are you fully deployed before you are moved onto the next project?

There are many dependencies

- PAM is integral to most organizations with multiple stakeholders

Deploying the HARD way

Changing a process that is already in active use and replacing with another.
Remember: the business needs to carry on regardless of your project.



People are resistant to change

New processes introduce risk

If things don't work out, is there a fall back?

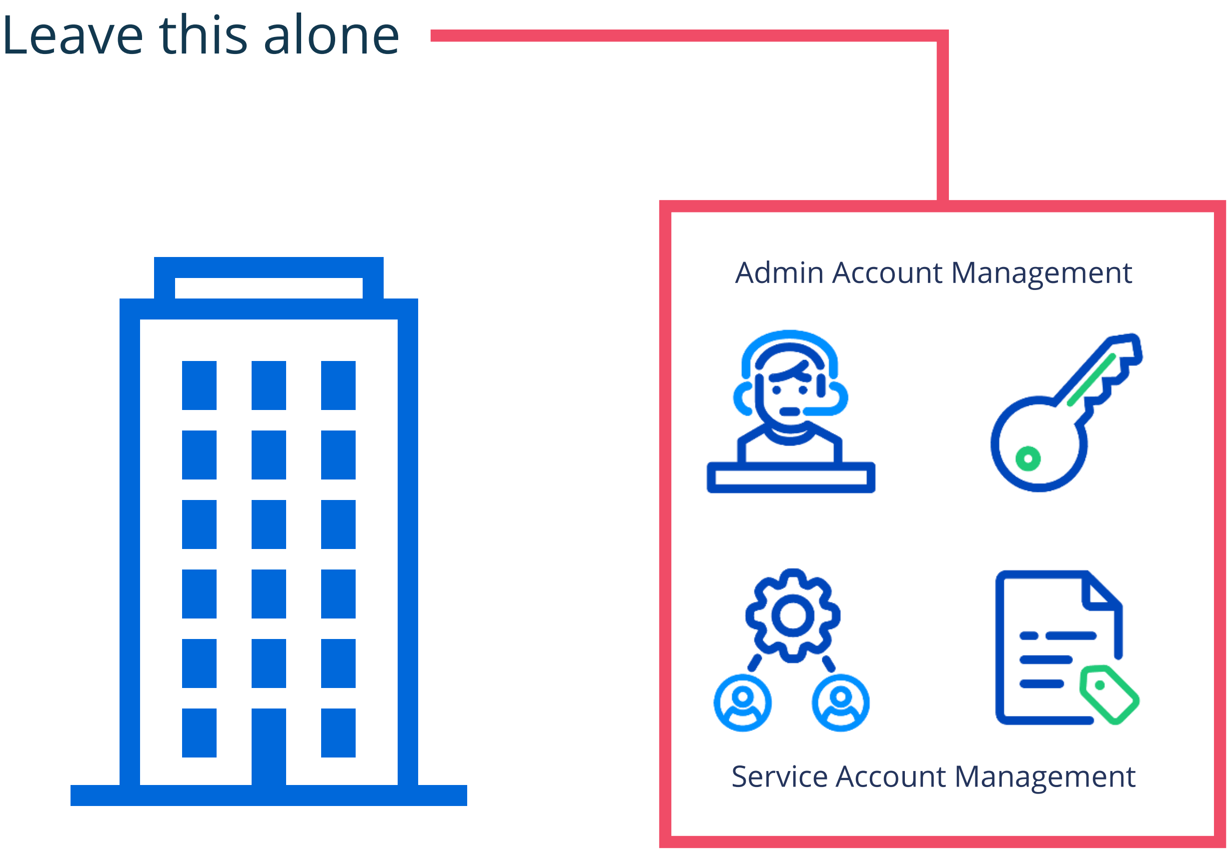
Fundamentals

- Your administrators just want to do their job – business continuity generally wins
- Remember, nobody *wants* PAM – you can make their life easier
- Don’t try to be too clever – keep it simple
- Look for ways to complement what you already have
- Look for quick wins that can show success and win over stakeholders
- Different strokes for different folks – map out your workflows!!

Strategies for introducing PAM

Lower the risk and objections

Parallel Deployment via JIT



Leave this alone

Admin Account Management

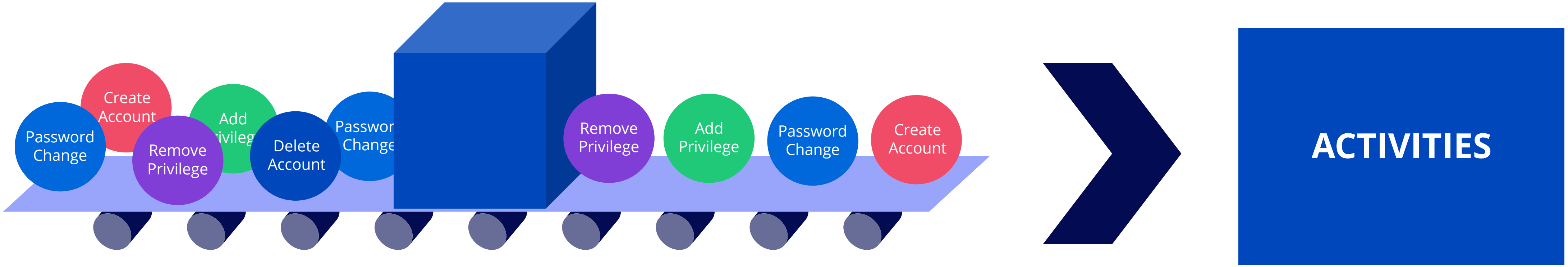
Service Account Management

Build a parallel just-in-time (JIT) process

Orchestrate what you need when you need it

Remove it when you have finished

Orchestrate it!



Traditional PAM simply **manages** privilege

Next-generation PAM **removes** privilege and is easier to deploy

Identity Orchestration

One-time accounts do not affect existing managed accounts

Before Session		🟩	Account doesn’t exist / no attack surfaces
During Session	jsmith4hs9k3h86fd	🟥	Ephemeral account created / just-enough privilege for task
After Session		🟩	Account removed / no attack surfaces

Privilege Orchestration

Managed accounts auto-onboard with option to offboard from old PAM solution

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

Environment Orchestration

Services

RDP

Kerberos Tickets

File Shares

Replication

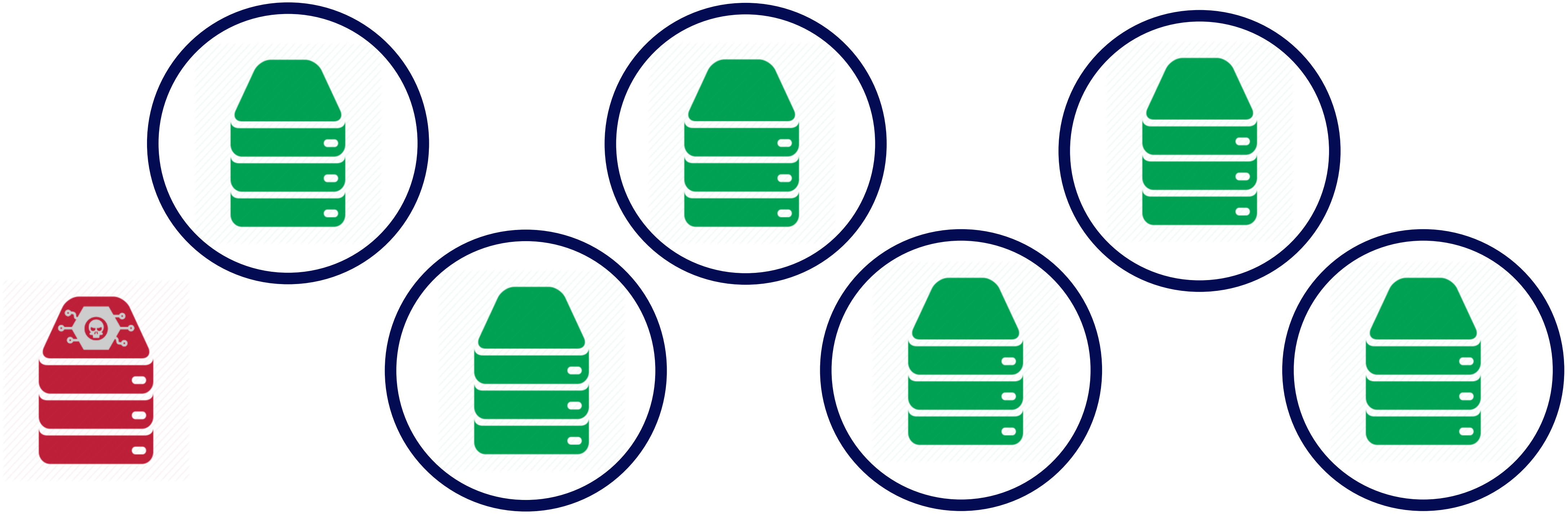
Risk Reduction

Roll out the new process without disturbing the old

When you are ready, simply turn off the old process

Another Orchestration Benefit

“Zero Standing Privileges”



Zero Standing Privileges

Operational Efficiency

Removing a problem is more efficient than managing it. Easier and risk-free deployment.

Reduced Attack Surface

Limiting the existence of privilege to when it is in legitimate use reduces the risk of malware spreading

Lower TCO

On-demand orchestration of privilege reduces complexity and FTE overhead

Forensics

Privileges exist only when authorized, facilitating cross-check of false positives

Key Points to Remember

- Use orchestration to roll out in parallel, then switch over
- Use JIT to remove Standing Privileges (Not all JIT is JIT)
- Look to embrace and enhance, don’t rip and replace
- Be mindful of different stakeholders and their needs – map workflow
- Above all… Keep it simple!!

Netwrix Privilege Secure

72% of customers deploy in less than 8 hours

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

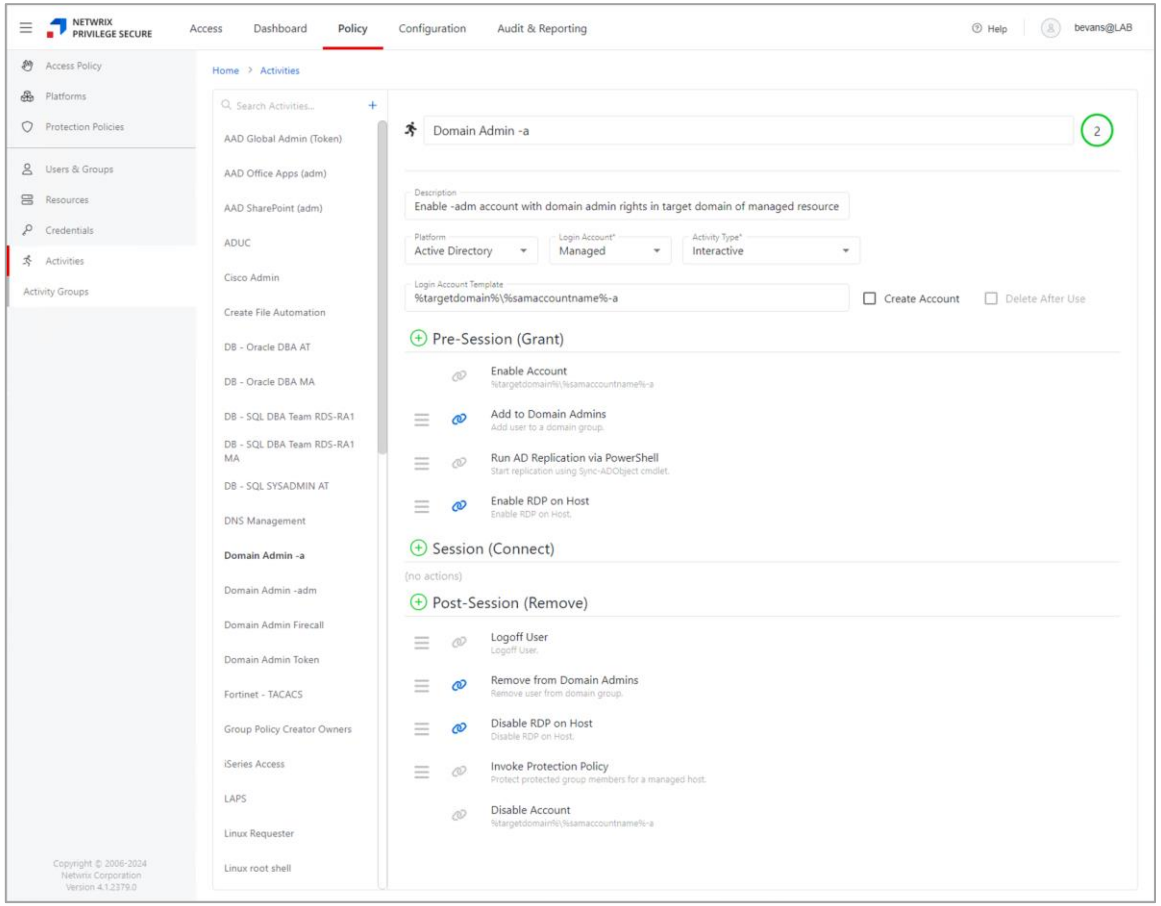
- Create / Remove Accounts
- Enable / Disable Accounts

Privilege Orchestration

- Add / Remove Permissions
- Enforce Group/Role Membership

Endpoint Orchestration

- Enable/Disable RDP
- Purge Kerberos Tickets
- Pre/Post File Comparison
- Dynamic SMB Shares
- Custom PowerShell
- Dynamic sudoers



AAD Global Admin (Token)
AAD Office Apps (adm)
AAD SharePoint (adm)
ADUC
Cisco Admin
Create File Automation
DB - Oracle DBA AT
DB - Oracle DBA MA
DB - SQL DBA Team RDS-RA1
DB - SQL DBA Team RDS-RA1 MA
DB - SQL SYSADMIN AT
DNS Management
Domain Admin -a
Domain Admin -adm
Domain Admin Firecall
Domain Admin Token
Fortinet - TACACS
Group Policy Creator Owners
iSeries Access
LAPS
Linux Requester
Linux root shell

Copyright © 2006-2024
Netwrix Corporation
Version 4.1.2379.0

Domain Admin -a

Description: Enable -adm account with domain admin rights in target domain of managed resource

Platform: Active Directory
Login Account*: Managed
Activity Type*: Interactive

Login Account Template: %targetdomain%\%samaccountname%-a
□ Create Account
□ Delete After Use

Pre-Session (Grant)

Enable Account
%targetdomain%\%samaccountname%-a

Add to Domain Admins
Add user to a domain group.

Run AD Replication via PowerShell
Start replication using Sync-ADObject cmdlet.

Enable RDP on Host
Enable RDP on Host.

Session (Connect)

(no actions)

Post-Session (Remove)

Logoff User
Logoff User.

Remove from Domain Admins
Remove user from domain group.

Disable RDP on Host
Disable RDP on Host.

Invoke Protection Policy
Protect protected group members for a managed host.

Disable Account
%targetdomain%\%samaccountname%-a

Active Directory ✷ Entra ID ✷ Windows ✷ Linux ✷ Databases ✷ Network Devices ✷ Websites ✷ Applications

Product Demo

Poll

SANS

WE WANT YOUR FEEDBACK

netwrix

SANS 2025 SURVEY:

SECURING DATA: *UNVEIL INSIGHTS ON CYBERSECURITY STRATEGIES AND BUYER PRIORITIES*

OPEN NOW – Nov 26

- Your Insights Matter!
- Enter Drawing: $250 Gift Card

www. sans.org/u/1yPD

TAKE SURVEY

Questions?

Visit us at netwrix.com

Thank you!

Visit us at netwrix.com