



Zero Standing Privileges oder kurzlebige Konten

Ein besserer Ansatz für PAM



Dirk Schrader
VP Security Research,
Netwrix

Evolution des Privileged Access Managements



**Die Zukunft
von PAM**

Die Angriffsfläche für Lateralbewegungen verringern

- Keine Angriffsfläche für Angreifer, die es auszunutzen gilt
- Privilegien nach Bedarf schaffen / bei Nichtgebrauch entfernen

Komplexität reduzieren

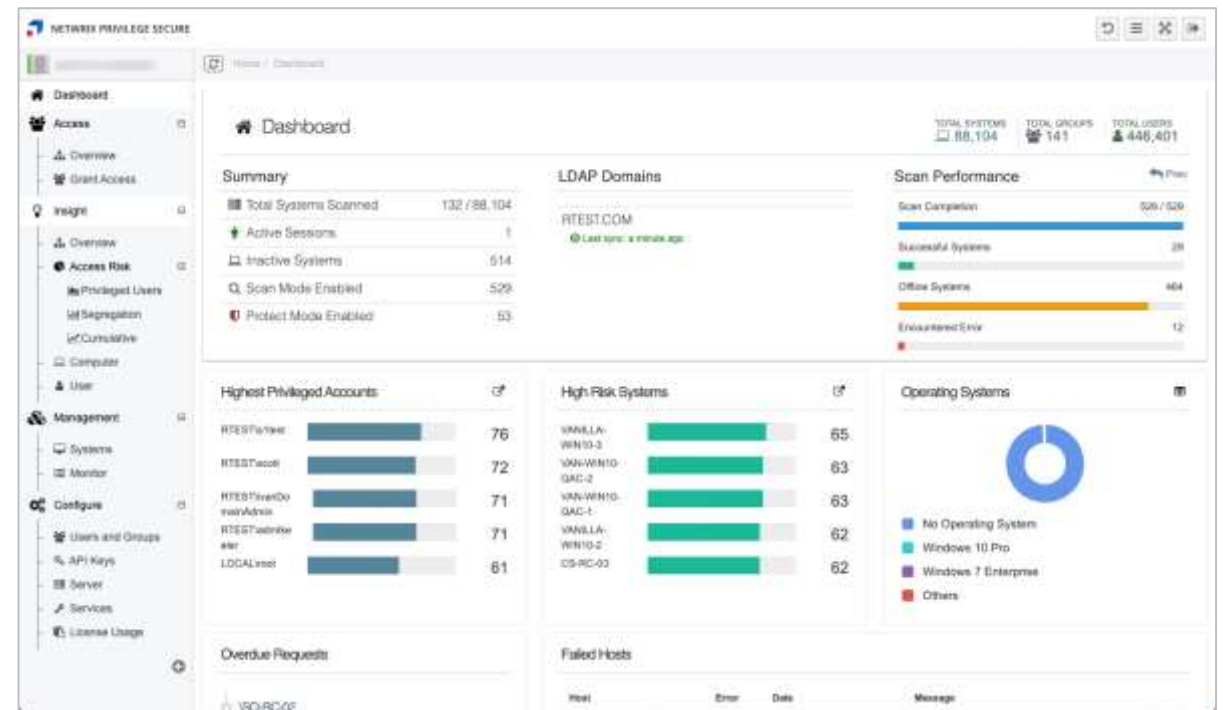
- Vereinfachen - das Leben muss nicht kompliziert sein!

Starten mit NPS for Discovery

Ja, sogar Sie haben auch eine Angriffsfläche...

Quantifizieren und überwachen

- Kontinuierliche Erkennung von Privilegien
- Benötigt keine speziellen Ports zum Scannen
- Überprüfen und berichten Sie über die Sicherheitslage im Laufe der Zeit



Um es unter Kontrolle zu halten

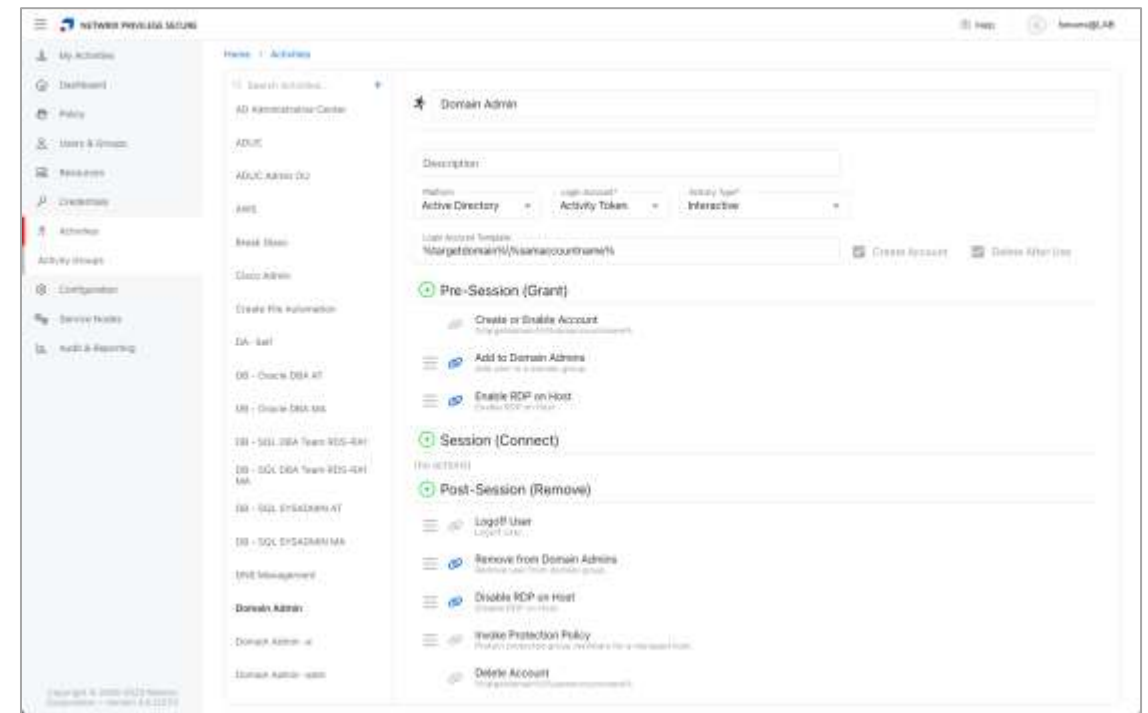
Orchestrieren Sie es...

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 Endpoint Privilege Orchestration Orchestration

- Create / Enable Accounts
- Add / Remove Permissions
- Enable/Disable RDP
- Purge Kerberos Tickets
- Group Protection
- Pre/Post File Comparison
- Dynamic SMB Shares
- Custom PowerShell
- Dynamic sudoers



Zufriedene Anwender & entlastete Admins

Local Admin Privilege, der richtige Weg

Least Privilege für Benutzer und Anwendungen - ohne Einbußen bei der Produktivität.

Durchsetzung des Prinzips der geringsten Rechte überall dort, wo Benutzer arbeiten

Delegieren Sie privilegierten Zugriff auf Einstellungen, die normalerweise lokale Administratorrechte erfordern

Least Privilege überall dort durchsetzen, wo die Benutzer arbeiten

#	setting	Policy Type	Scope	Condition	Action
	SecureRun™ policy		User Processes	File Untrusted	Block
1	Elevate Device Manager with Control Panel Rule	New Executable Policy	User Processes	Device Manager	Elevate
2	PowerPointViewer Elevated with Hash rule	New Windows Installer Policy	User Processes	Hash	Elevate
3	MSI for Microsoft Teams Elevated with Signature and Pro	New SecureRun™ Policy	User Processes	Signature, Product info	Elevate
4	CamPlay Allowed with HASH rule	New Admin Approval Policy	User Processes	Hash	Allow

#	setting	Policy Type	Scope	Condition	Action
	SecureRun™ policy	New Collection	User Processes	File Untrusted	Block
1	Elevate Device Manager with Control Panel Rule	New Executable Policy	User Processes	Device Manager	Elevate
2	PowerPointViewer Elevated with Hash rule	New Control Panel Applet Policy	User Processes	Device Manager	Elevate
2	PowerPointViewer Elevated with Hash rule	New Windows Installer Policy	User Processes	Hash	Elevate
		New Global DLL Policy			
3	MSI for Microsoft Teams Elevated with Signature and Pro	New SecureRun™ Policy	User Processes	Signature, Product info	Elevate
		New SecureCopy™ Policy			
4	CamPlay Allowed with HASH rule	New Admin Approval Policy	User Processes	Hash	Allow
		New Self Elevation Policy			
		New Global Settings Policy			
		New Policy from Audit Event			
		New Script Policy			
		New Java (JAR) Policy			
		New UWP Policy			
		New COM Class Policy			
		New ActiveX Policy			

#	setting	Policy Type	Scope	Condition	Action
	SecureRun™ policy		User Processes	File Untrusted	Block
1	Elevate Device Manager with Control Panel Rule		User Processes	Device Manager	Elevate
2	PowerPointViewer Elevated with Hash rule		User Processes	Hash	Elevate
3	MSI for Microsoft Teams Elevated with Signature and Pro		User Processes	Signature, Product info	Elevate
4	CamPlay Allowed with HASH rule		User Processes	Hash	Allow

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

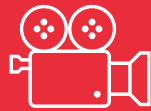


You can advance to
Zero Standing Privilege
step-by-step

Was noch? Mehr am Stand 7A-320



**Credential
Management**



**Session
Recording**



**Cloud
Workloads**



**Application
Management**



**Ecosystem
Integrations**



**Access
Certification**

Netwrix Data Security Made Easy

Vielen Dank