

Zero Standing Privilege: Wie Nutzer- Berechtigungen vergänglich werden



PRIVILEGED ACCESS MANAGEMENT

Privilegierte Konten stehen im Mittelpunkt praktisch jedes Sicherheitsverletzungsereignisses.

Um ihr Gefährdungsrisiko zu mindern, müssen Unternehmen nicht nur die Nutzung privilegierter Konten sichern, kontrollieren, verwalten und überwachen, sondern privilegierte Konten und ihren Zugriff vollständig entfernen, indem sie einen Just-in-Time-Ansatz mit Just-Enough Berechtigungen verwenden.

PRIVILEGED ACCESS MANAGEMENT- PROBLEME

FORRESTER®

„Forrester schätzt, dass 80 % der Sicherheitsverletzungen privilegierte Zugangsdaten beinhalten. Es ist verständlich: Nachdem sich ein Eindringling Zugang zu den Geräten der Mitarbeiter verschafft hat, versucht er, das Netzwerk auszuschnüffeln und Keylogger zu installieren, um Zugangsdaten mit höheren Berechtigungen (wie Root oder Administrator) zu erhalten. Privilegierte Zugangsdaten bieten mehr Möglichkeiten, Daten massenhaft zu stehlen als einzelne Konten..“





Zero Standing Privilege mit Netwrix



Secure

Verringern Sie das Risiko eines Missbrauchs privilegierter Zugangsdaten, und verkleinern Sie diese Angriffsfläche, indem Sie Konten mit dauerhaften Berechtigungen aufspüren und entfernen.



Comply

Vermeiden Sie nachteilige Audit-Ergebnisse und beweisen Sie, dass privilegierte Aktivitäten keine Sicherheitsbedrohungen darstellen; automatisieren Sie den Audit-Prozess automatisieren.



Enable & Control

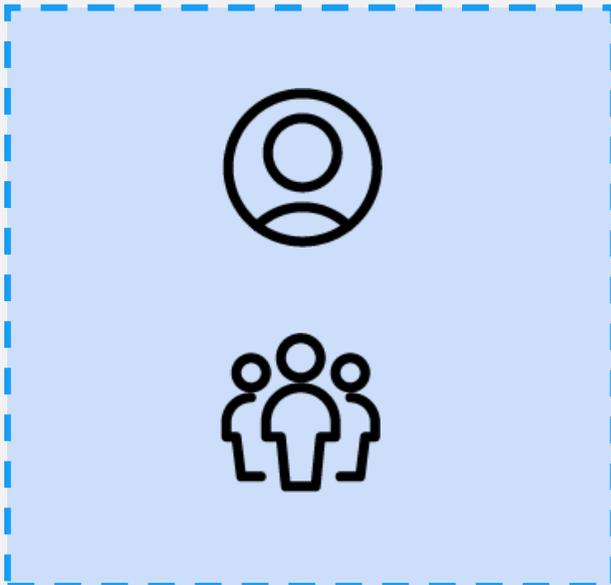
Verbessern Sie die Sicherheit und gleichzeitig die IT-Produktivität, kontrollieren Sie privilegierte Aktivitäten, erkennen und reagieren Sie schneller auf verdächtiges Verhalten.



PAM bringt Administratoren sicher von A nach B

ACCESS POLICY

BENUTZER & GRUPPEN

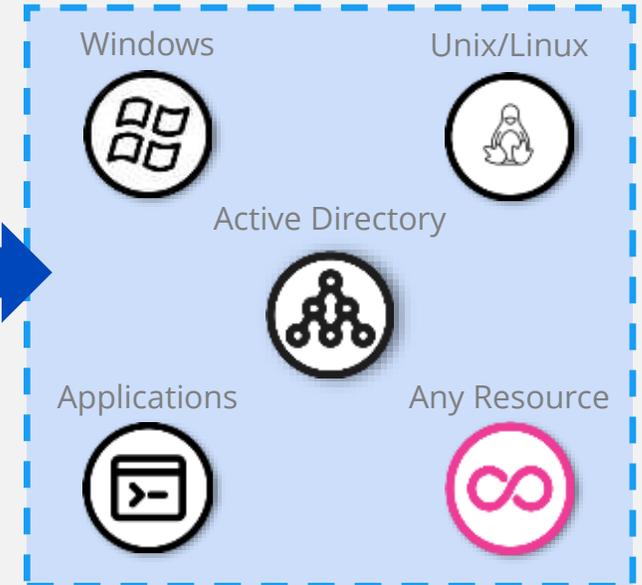


AKTIVITÄTEN

- Domain Admin Access
- Password Reset
- Hyper-V Management
- Enterprise Admin Access
- Exchange Administration
- DNS Change
- Local Admin Access
- DHCP Management
- Unlock Account
- Group Policy Management
- Database Management
- ETC...



RESSOURCEN



PLATFORM SERVICES

Discovery

Proxy

Live Session
Monitoring &
Recording

Credential &
Service Account
Management

LAPS & Vault
Integration
(BYOV)

Auditing

Approval
Workflows



PRIVILEGED ACCESS MANAGEMENT – WIE?

01 DISCOVER



Entdecken Sie privilegierte Konten mit ständigem Zugriff auf das System, die Anwendung und die Dateninfrastruktur

02 ONBOARD



Integrieren Sie Konten für die Verwaltung und entfernen Sie permanente Berechtigungen, um die Angriffsfläche zu reduzieren

03 GRANT



Erteilen Sie dem Benutzer genau die erforderliche Berechtigungsstufe, um die gewünschte Verwaltungsfunktion auszuführen

04 CONNECT



Verbinden Sie den Benutzer direkt oder über einen Proxy für eine erweiterte Sitzungsüberwachung

05 REMOVE



Entfernen Sie den Zugriff des Benutzers vollständig und bereinigen Sie das System, um den gewünschten Zustand zu erreichen, um fortgeschrittene Techniken zum Diebstahl von Anmeldeinformationen zu vermeiden



Zero Standing Privilege mit Netwrix

Secure

Das Risiko des Missbrauchs privilegierter Zugangsdaten verringern.

Comply

Nachteilige Audit-Ergebnisse vermeiden und beweisen, dass privilegierte Aktivitäten keine Sicherheitsbedrohungen darstellen.

Enable & Control

IT-Sicherheit und IT-Produktivität verbessern, privilegierte Aktivitäten kontrollieren.



Privilegierte Konten finden und deren Anzahl auf ein absolutes Minimum bringen.



Privilegierten Zugang nur bei Bedarf gewähren und nur so lange wie nötig.



Bessere Dokumentation, da Sie jede Sitzung genehmigen, protokollieren und aufzeichnen.



Zero Standing Privilege mit Netwrix

Secure

Das Risiko des Missbrauchs privilegierter Zugangsdaten verringern.

Comply

Nachteilige Audit-Ergebnisse vermeiden und beweisen, dass privilegierte Aktivitäten keine Sicherheitsbedrohungen darstellen.

Enable & Control

IT-Sicherheit und IT-Produktivität verbessern, privilegierte Aktivitäten kontrollieren.



Identifizierung und Entfernung nicht benötigter privilegierter Konten.



Auditierbare Prüfpfade für alle Aktivitäten.



Zuverlässigen Nachweise durch Aufzeichnung und Wiedergabe.



Zero Standing Privilege mit Netwrix

Secure

Das Risiko des Missbrauchs privilegierter Zugangsdaten verringern.

Comply

Nachteilige Audit-Ergebnisse vermeiden und beweisen, dass privilegierte Aktivitäten keine Sicherheitsbedrohungen darstellen.

Enable & Control

IT-Sicherheit und IT-Produktivität verbessern, privilegierte Aktivitäten kontrollieren.



Effizient privilegierte Aktivitäten systemübergreifend zentral verwalten.



Serviceausfälle während Passwortrotationen minimieren, Änderungen anhalten und zurücknehmen.



Einführungsaufwände verringern, damit Ihr Team die bevorzugten Tools SICHER nutzen kann.

**PAM mit
Zero Standing Privilege:
Mehr dazu bei Netwrix
Halle 7A – Stand 320**

