

# Privileged Access Management PEDM

wallix pam

## Erweitern Sie WALLIX PAM mit einer Least-Privilege-Strategie

Die Ausweitung von Benutzerprivilegien ist häufig der Ursprung von Cyberangriffen und Schwachstellen in Systemen. Diese Risiken lassen sich jedoch effektiv durch das Prinzip der geringsten Rechte (Least Privilege) minimieren. WALLIX PEDM (Privileged Elevation and Delegation Management) arbeitet mit lokalen Agenten auf verwalteten Systemen, um Nutzern gezielt die erforderlichen Rechte für spezifische Aufgaben zuzuweisen. Dadurch wird Sicherheit auf Prozessebene gewährleistet, während gleichzeitig die Nutzung von **allgemeinen Administratorkonten überflüssig wird**. Zusätzlich ermöglicht die Lösung eine detaillierte Kontrolle von Anwendungen und eine Überwachung von Dateien, wodurch Sicherheitslücken reduziert werden. Dies geschieht, ohne die Produktivität zu beeinträchtigen, und stellt zugleich die Einhaltung von gesetzlichen Anforderungen sicher.

## Funktionen

### Prinzip der geringsten Privilegien

- Bedarfsgerechte Eliminierung privilegierter Konten innerhalb Ihrer Organisation
- Zuweisung von Privilegien nur zur richtigen Zeit und im richtigen Kontext

### Fein abgestufte Rechteverwaltung (Least Privilege)

- Erhöhung der Rechte für Standardbenutzer auf Windows- und Linux-Systemen
- Steuerung von Prozessen durch präzise, fein granulいた Richtlinien
- Lokale Agenten setzen die Richtlinien um, ohne die Systemleistung zu beeinträchtigen

### Zentralisierte Verwaltung

- Verwaltung der Sicherheitsrichtlinien von einer zentralen Konsole aus
- Vollständige Integration mit Active Directory zur Speicherung von Regeln und Konfigurationen
- Der Agent aktualisiert seine Richtlinien regelmäßig, um sie offline anzuwenden

### Erhöhte Sicherheit

- Erstellung von Ordnerregeln, um wichtige Daten vor unbefugten Änderungen zu schützen
- Überwachung von Aktionen mit erhöhten Berechtigungen
- Bedarfsgerechte Rechteerhöhung für Prozesse

## Technische Merkmale

### > Prozesssteuerung

- Privilegien für Prozesse erhöhen, reduzieren oder blockieren
- Regelbasierte Gruppenmitgliedschaften

### > Unterstützte Betriebssysteme

- Windows Server 2003 und höher
- Windows XP SP3 und höher
- Linux Ubuntu (Versionen 18–22) und Linux Debian (Versionen 9–12)
- RedHat (Versionen 8–9)

### > Verwaltung

- Integration in Active Directory
- Verwaltung über MMC-Snap-In

### > Überwachung

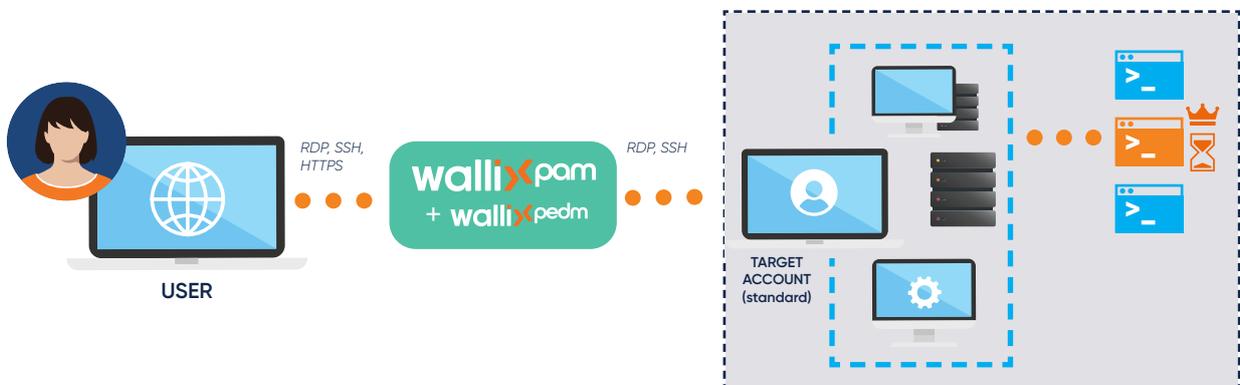
- Ereignisbasiert
- Integration in SIEM-Systeme

wallix

# Wie funktioniert unsere Lösung?

WALLIX PEDM verwendet eine exklusive, patentierte Technologie, die jedem Prozess oder jeder Anwendung den erforderlichen Sicherheitskontext zuzuweisen – unabhängig von den Benutzeranmeldedaten, mit denen sie ausgeführt werden. Mit WALLIX PEDM werden Privilegien an Prozesse und Anwendungen vergeben und nicht an Benutzer, anders als bei herkömmlichen Tools auf dem Markt.

- **Kontrollieren Sie den Zugriff auf IT-Ressourcen**, indem Sie Berechtigungen für die Anmeldung über ein Standardkonto erteilen.
- **Erteilen Sie Privilegien** nur für die Prozesse, die wirklich in der benötigten Zeit gebraucht werden.
- **Überwachen Sie jede Aktion**, die während einer Sitzung stattfindet.
- **Keine Administratorkonten mehr** in der Infrastruktur – noch nicht einmal für die IT



## Vorteile



### SCHNELLE IMPLEMENTIERUNG

Richten Sie WALLIX PEDM in Ihrer Umgebung in nur wenigen Stunden ein.



### UNMITTELBARER SCHUTZ

Kontrollieren Sie privilegierte Aktionen und verhindern Sie von Beginn an die Ausführung von nicht autorisierten Prozessen.



### 100% SKALIERBAR

Durch die Verwendung eines Client-Server-Ansatzes ist WALLIX PEDM genauso skalierbar wie Ihr Unternehmen selbst.



### TRANSPARENT FÜR ENDANWENDER

WALLIX PEDM nutzt die Mechanismen des Betriebssystems, um Sicherheit zu gewährleisten.

## Über WALLIX

WALLIX schützt digitale Identitäten sowie den Zugriff auf IT-Infrastrukturen, Anwendungen und Daten. Die spezialisierten Lösungen im Bereich Privileged Access Management sorgen für die Einhaltung moderner IT-Sicherheitsstandards und bieten umfassenden Schutz vor Cyberangriffen, Datendiebstahl und Sicherheitsverletzungen, die durch gestohlene Anmeldedaten oder missbräuchlich genutzte Zugriffsrechte verursacht werden.

[WWW.WALLIX.COM](http://WWW.WALLIX.COM)



wallix