WALLIX
BASTION

LEAST-PRIVILEGE-PRINZIP

PEDM
PRIVILEGED ELEVATION AND DELEGATION MANAGEMENT

Umfassender Schutz für Ihre kritischen Systeme

Administratorrechte erzeugen kritische Schwachstellen in Ihrem IT-Netzwerk. Stellen Sie sicher, dass privilegierte Berechtigungen nur für die richtigen Konten und zur richtigen Zeit wirken - ohne die Produktivität zu beeinträchtigen.

LEAST-PRIVILEGE-MANAGEMENT-PRINZIP

- **Beseitigen Sie das Risiko überprivilegierter Nutzer,** die in Ihrem IT-Netz auf Knopfdruck Unheil anrichten können.
- **Keine lokalen Administratoren:** Gewähren Sie Berechtigungen auf granularer Ebene mit der Möglichkeit, einem Nutzer Sonderrechte für spezielle Aktionen zuzuweisen
- **Rechtetrennung** durch Erstellen eines Sicherheitskontextes auf Anwendungs- und Prozessebene, und weniger auf Nutzerebene
- **Produktivität steigern:** Nutzer ohne Administratorrechte können weiterhin Aufgaben mit angepassten Rechten durchführen, ohne die Produktivität zu beeinflussen

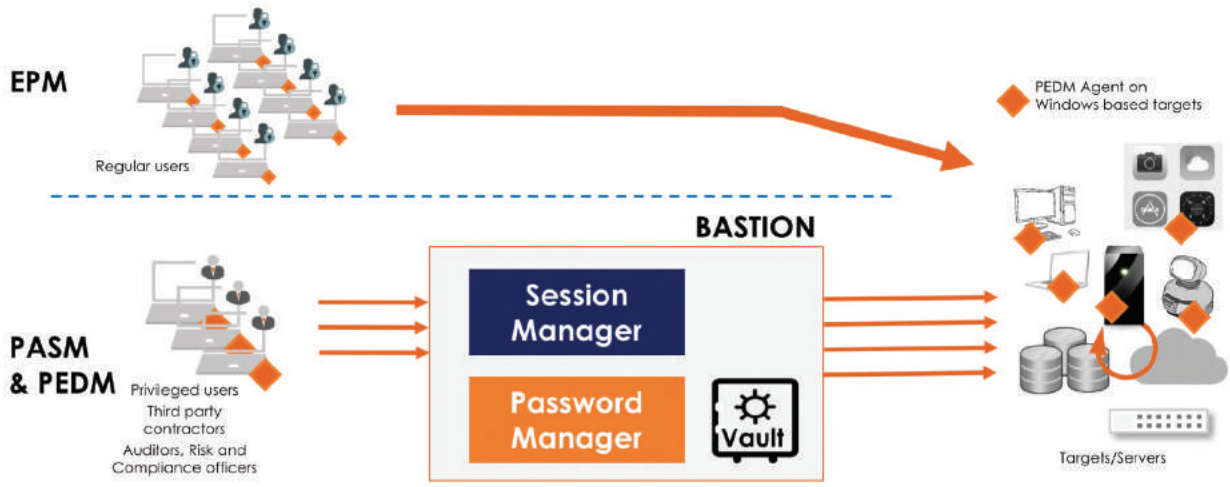
PRIVILEGED ACCESS MANAGEMENT FÜR KRITISCHE SYSTEME

- **Schützen Sie Ihre Vermögenswerte** mit Zugangs-Workflows, Passwortrotation und lokaler Rechtebeschränkung
- **Sichern Sie Ihre kritischen Systeme** durch Sitzungskontrolle und lokalem Applikations- und Prozessmanagement
- **Nachverfolgung und Überwachung von Aktivitäten** mit vollständiger Sitzungsaufzeichnung, Metadaten und Protokollen für lokale Geräte

ENDPOINT PROTECTION

- **Passen Sie Berechtigungen für Applikationen granular an,** damit diese nur genutzt werden können, um autorisierte Aktionen von autorisierten Nutzern durchzuführen
- **Verhindern Sie bekannte und unbekannte Angriffe** durch Blockieren aller nicht autorisierten Aktionen, die das System verändern wollen
- **Neutralisieren Sie Ransomware:** Verschlüsselungsaktionen werden erkannt, bevor sie ausgeführt werden

- **Integration mit der Lösung Bastion PAM** zum besseren Schutz vor Identitätsdiebstahl und des Zugangs zu kritischen Systemen
- **White/Grey/Blacklisting von Applikationen,** um lokale Administratoren zu vermeiden oder Nutzungsrechte einzuschränken
- **Vollständige Verfügbarkeit** auf allen Windows-Plattformen
- **Zentrale und vereinfachte Verwaltung** durch Integration mit Microsoft Active
- **Exklusiv patentierte Technologie,** die Prozessen und Anwendungen Sicherheitskontexte zuweist
- **Sicherheit auf Applikationsebene** zur Vermeidung von Administratorkonten auf Endpoints
- **Erkennen von verdächtigen Systemaktivitäten in Echtzeit,** z. B. Verschlüsselungen, zur Abwehr von Ransomware
- **Dateischutz** gegen Manipulation auf NTFS-Ebene
- **Vermeidung lokaler Administrator-Passwörter,** die für mehrere Systeme verwendet werden
- **Integration mit SIEM** zur Zentralisierung von Protokollinformationen für eine bessere Gefahrenerkennung



WALLIX Bastion PASM + PEDM Lösung: Völliger Schutz ohne Beeinträchtigung der Produktivität

- **Umfassender Schutz Ihrer kritischen Assets** mit Best-in-Class Passwort-Tresor- und Sitzungskontrollfunktionen, erweitert um Privilegien-Schutz für Endpoints
- **Proaktive Sicherheit auf System- und Prozessebene,** die an die neuesten Bedrohungen angepasst ist
- **Vereinfachte Verwaltung von Sicherheitsregeln mit dem Least-Privilege-Prinzip für Endpoints,** leicht umzusetzen und mit feiner Granularität
- **Keine Beeinträchtigung der Systemleistung** dank der tiefen Integration in das Betriebssystem
- **Maßgeschneiderte Ad-hoc-Lösung** durch White-/Grey- und Blacklisting, angepasst an die IT-Betriebsabläufe

BASTION

WALLIX ADMIN CENTER

ACCESS MANAGER	SESSION MANAGER	PASSWORD MANAGER	PEDM
MFA	DISCOVERY	AAPM	API

DEVOPS

WALLIX
CYBERSECURITY SIMPLIFIED