

# Privileged Access Management WALLIX Bastion

## Zentralisierte Kontrolle und Überwachung des privilegierten Zugriffs auf sensible Assets

Hacker nutzen privilegierte Konten, um Unternehmen zu infiltrieren und sich auszubreiten. Privileged Access Management (PAM) ist ein fundamentales Instrument zur Eindämmung von Cyberangriffen. **WALLIX Bastion** ist eine führende PAM-Lösung, die eine robuste Sicherheit und einen Überblick über privilegierte Zugriffe auf eine kritische IT-Infrastruktur bietet. Durch Ihre digitale Transformation kann **WALLIX Bastion** nahtlos eingesetzt werden, von lokalen bis hin zu Private- und Public-Cloud-Infrastrukturen.

## Merkmale & Funktionen

### Verkleinern Sie die Angriffsfläche

- Erkennen Sie Assets automatisch und eliminieren Sie alle lokalen privilegierten Konten
- Legen Sie Autorisierungsregeln fest, um den Zugriff auf kritische Systeme zu kontrollieren
- Verwenden Sie zur Durchführung von Aufgaben das geringste erforderliche Privileg
- Vergeben Sie Privilegien für autorisierte Nutzer genau zur rechten Zeit

### Schützen Sie geheime Daten

- Speichern Sie geheime Informationen von menschlichen und nicht-menschlichen Nutzern auf sichere Weise
- Aktualisieren Sie Passwörter mithilfe automatisierter Rotation zeit- und/oder nutzungsbasiert
- Löschen Sie Passwörter von Speicherlaufwerken

### Kontrollieren Sie Sitzungen

- Überwachen Sie Sitzungen in Echtzeit mit Session Sharing
- Zeichnen Sie alle Sitzungen auf und extrahieren Sie zugehörige Metadaten zwecks Analyse
- Aktivieren Sie Alarmer nach Erkennung gefährlicher Aktivitäten und beenden Sie Sitzungen

### Prüfen Sie Aktivitäten

- Managen Sie KPIs mit Berichten und Dashboards
- Korrelieren Sie verdächtiges Verhalten mit SIEM-Integration
- Profitieren Sie von einem schnellen Deployment ohne Unterbrechung der täglichen Workflows

## Technische Merkmale

- > **Verschlüsselungs-algorithmen**
  - AES-256, SHA2,
  - ECC p256, p381 und p515
  - Highend-Schlüssel für Proxys
- > **Hochverfügbarkeit**
  - Unterstützung von Clustering
  - Disaster Recovery
  - Integration von Unternehmens-Backup-Systemen
- > **Access- und Workflow-Management**
  - AD- und LDAP-Verzeichnisse
  - Identität und Zugriff
  - Ticket- und Workflow-Systeme
  - AD-Silos
- > **Authentifizierungsmethoden**
  - Benutzername und Passwort, Kerberos, LDAP, NLA, Web SSO, RADIUS, PKI, SAML...
- > **Überwachung**
  - SIEM-Integration, SNMP, E-Mail-Benachrichtigungen
- > **Public-Cloud-Umgebungen**
  - Amazon Web Services (AWS)
  - Microsoft Azure
  - Google Cloud Platform (GCP)

## Was unsere Kunden sagen

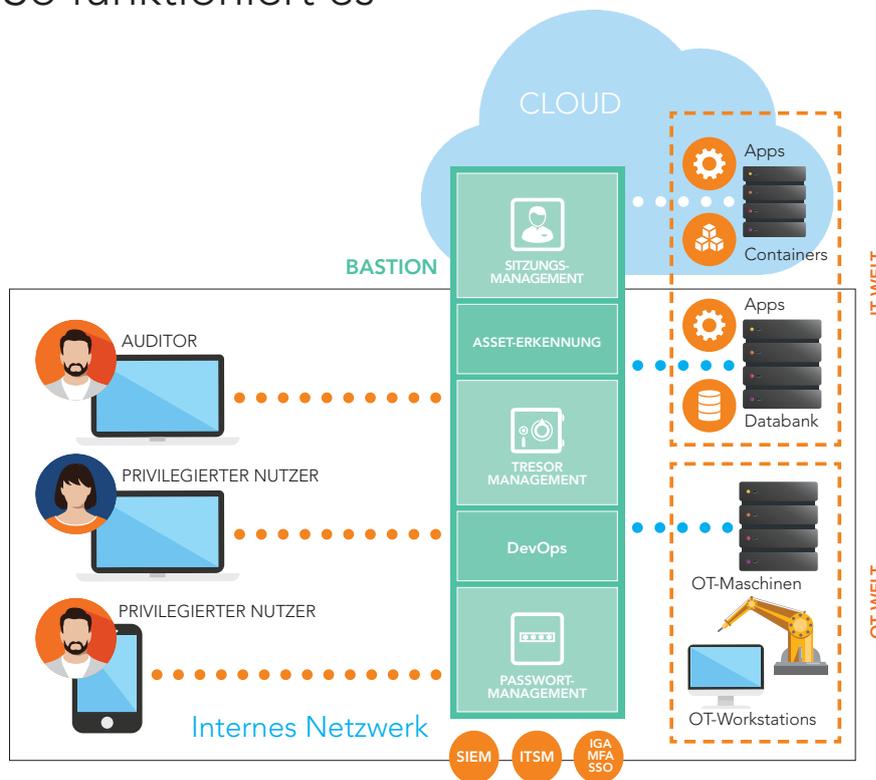
**„Das Produkt lässt sich sehr einfach installieren, nach einem Tag können wir bereits die Lösung für den Zugriff auf unsere kritischen Server bieten.“**

Infrastructure and Operations Manager, Fertigung

**„Übersichtliche Architektur, einfache und schnelle erste Implementierung.“**

Security Infrastructure Manager, Gesundheitswesen

## So funktioniert es



## Über WALLIX

WALLIX schützt Identitäten und den Zugriff auf IT-Infrastrukturen, Anwendungen und Daten. Die auf Privileged Access Management spezialisierten WALLIX Lösungen gewährleisten Konformität mit den neuesten IT-Sicherheitsstandards und schützen vor Cyberangriffen, Diebstahl und Datenlecks, die mit gestohlenen Zugangsinformationen und erweiterten Zugriffsrechten für sensible Unternehmensdaten in Verbindung stehen.

[www.wallix.com](http://www.wallix.com)

## Vorteile



### Verringerung interner und externer Bedrohungen

Zentralisieren Sie das sichere Management privilegierter Nutzer und kritischer Systeme



### Einsatz in allen Umgebungen

Stellen Sie eine nahtlose Integration in lokale, hybride und cloud-native Infrastrukturen sicher



### Sicheres Wachstum

Skalieren Sie Ihre Infrastruktur ohne jegliches Risiko



### Gewährleistung von Richtlinien-konformität

Vermeiden Sie Strafen, indem Sie kritischen Datenzugriff verfolgen und schützen



### Reduzieren Sie Ihre Kosten

Kontrollieren Sie Ihre TCO durch vereinfachte Implementierung und Bedienung