

# PRIVILEGE MANAGEMENT FOR UNIX & LINUX

PROTECTION DES COMPTES À PRIVILÈGES ET MISE EN CONFORMITÉ



## Limitation des accès root

Etablissez des règles granulaires d'élévation de privilèges pour l'exécution de tâches ou commandes spécifiques.

## Audit de toute l'activité des utilisateurs

Protégez-vous des changements non autorisés sur les fichiers, scripts et annuaires.

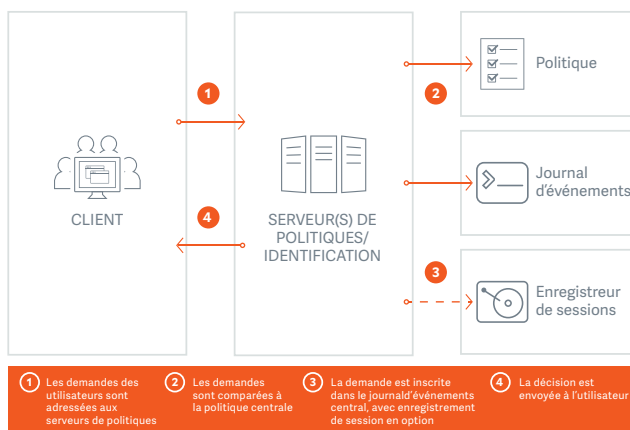
## Surveillance des logs et sessions

Détectez les utilisateurs, comptes et activités suspects en temps réel.

BeyondTrust Privilege Management for Unix & Linux est une solution inégalée de gestion des privilèges qui vous offre visibilité et contrôle sur des environnements de serveurs complexes.

## Fonctionnalités

- **Audit et gouvernance** : analysez le comportement des utilisateurs en collectant, en sauvegardant et en indexant de manière sécurisée les frappes clavier, les enregistrements de session et autres événements lors de sessions privilégiées.
- **Moindre privilège granulaire** : élevez les privilèges des utilisateurs standard sur systèmes Unix et Linux via des contrôles de règles granulaires.
- **Politique d'accès dynamique** : utilisez des facteurs tels que l'horaire, le jour, l'emplacement et la vulnérabilité de l'application/asset pour attribuer et prendre les décisions d'élévation de privilège.
- **Contrôle à distance des systèmes et des applications** : les utilisateurs peuvent exécuter des commandes spécifiques et établir des sessions à distance selon les règles en place sans devoir utiliser un compte de type root ou admin.
- **Contrôle de l'intégrité des fichiers et des règles** : auditez et générez des rapports sur les changements apportés aux fichiers critiques de règles, systèmes, applications et données.
- **Analyse des menaces** : corréllez le comportement des utilisateurs aux données de vulnérabilités des assets et aux renseignements de sécurité fournies par les solutions de sécurité.



# Plateformes supportées

Privilege Management for Unix & Linux supporte plus de 100 plateformes dont Debian GNU, HP-UX, HP Tru 64, Red Hat Enterprise Linux, Sun Solaris, SuSE Linux Enterprise, VMware ESX, IBM AIX, etc.

« Le déploiement de Privilege Management for Unix and Linux est une réussite. Tous les accès aux serveurs sont limités, y compris par SSH. Les auditeurs voient aisément que les procédures sont suivies et nos salariés IT demeurent productifs. »

**SVP SYSTEMS / RECOVERY,  
CTO, DCI**

## BÉNÉFICES

### Conformité et respect des réglementations

- Création d'un rapport d'audit exhaustif de l'activité de tous les utilisateurs.
- Conformité réglementaire grâce aux cloisonnement des tâches IT nécessitant des comptes privilégiés.
- Garantie que les fichiers et politiques critiques n'ont pas été altérés.

### Protection des systèmes et fichiers critiques

- Réduction de la surface d'attaque : fournissez juste l'accès nécessaire pour effectuer une tâche.
- Empêche l'utilisation des comptes root.
- Exécution uniquement des applications/commandes approuvées.
- Elimination des contournements ou failles
- Prise de décisions concernant les privilèges basée sur le contexte et le risque.
- Protection des fichiers critiques contre les malwares et utilisations abusives.

### Efficacité

- Simplification des processus complexes avec sudo.
- Gestion et déploiement simplifiés via une console d'administration centrale.

BeyondTrust est le leader mondial du Privileged Access Management, offrant l'approche la plus complète du marché afin de réduire les risques de failles liées à l'exploitation des privilèges. Flexible, notre plateforme permet aux organisations de sécuriser les privilèges sur les endpoints, serveurs, réseaux et environnements cloud, DevOps etc. de façon évolutive pour faire face aux menaces en constante mutation et évolution. Plus de 20 000 clients dans le monde nous font confiance.

[beyondtrust.com/fr](https://beyondtrust.com/fr)