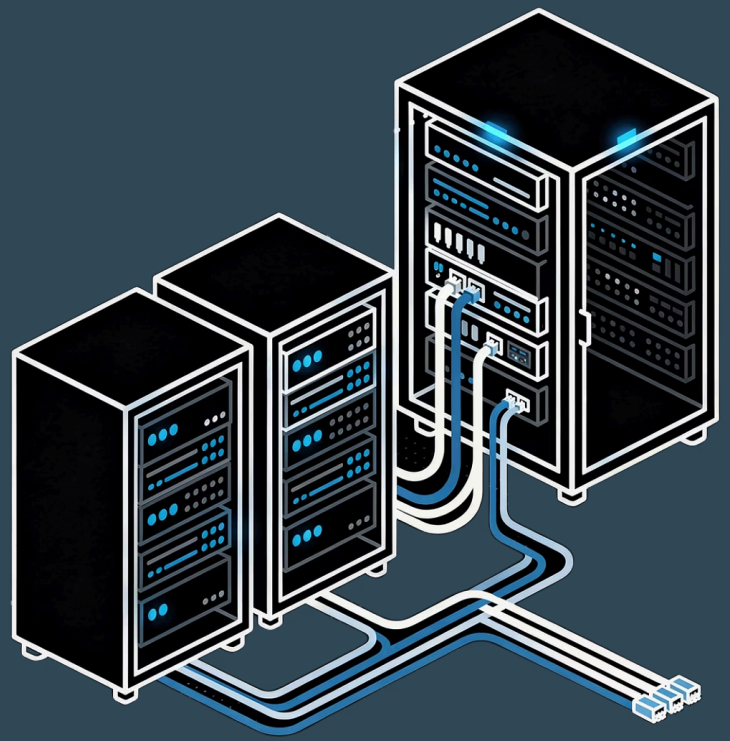

🔐 Pourquoi mettre en place un bastion d'administration comme WALLIX ?

À destination des CISO/RSSI et professionnels de la cybersécurité

Les comptes administrateurs : cibles privilégiées

Les comptes administrateurs sont des cibles privilégiées pour les cyberattaquants. Une simple compromission peut donner accès aux serveurs Windows, Linux, équipements réseau et données sensibles de l'entreprise.

Serveurs Windows & Linux

Accès root ou admin compromis = contrôle total du système

Équipements réseau

Firewalls, switches, routeurs exposés en cas de fuite d'identifiants

Données sensibles

Bases de données, secrets métiers, propriété intellectuelle à risque

Conséquences directes d'une absence de bastion

L'absence d'un bastion d'administration expose les organisations à des risques majeurs, transformant chaque compte à privilèges en une porte d'entrée potentielle pour les attaquants. Les statistiques sont alarmantes et soulignent l'urgence d'une protection renforcée.

80%

Violations par identifiants

des violations de données impliquent des identifiants compromis.

4.1M€

Coût moyen d'une violation

coût moyen global d'une violation de données en 2023.

204

Jours pour détecter

nombre moyen de jours pour détecter une violation.

Ces chiffres démontrent que les identifiants privilégiés sont la clé de voûte des cyberattaques réussies, entraînant des pertes financières considérables, des interruptions d'activité et des dommages réputationnels à long terme. La capacité à détecter rapidement une intrusion est également critique pour minimiser l'impact.

WALLIX Bastion : centraliser, contrôler et tracer

Avec WALLIX Bastion, les accès privilégiés RDP et SSH sont centralisés, contrôlés et tracés :

Authentification & Coffre-fort

- Authentification nominative et MFA
- Coffre-fort des mots de passe administrateurs

Contrôle des accès

- Principe du moindre privilège
- Accès temporaire sécurisé pour les prestataires
- Suppression des connexions administratives directes

Traçabilité & Conformité

- Enregistrement et traçabilité des sessions
- Transmission des événements vers le SIEM
- Contribution aux exigences ISO 27001, TISAX et NIS2

Cas d'usage concrets du bastion WALLIX

Le bastion WALLIX n'est pas qu'un outil de conformité ; c'est une solution flexible qui répond à des besoins de sécurité critiques dans divers contextes opérationnels. Il s'adapte aux architectures les plus complexes pour protéger les accès privilégiés, du datacenter aux infrastructures industrielles.

Prestataires externes

Gérez et tracez les accès temporaires des tiers à vos infrastructures, avec un contrôle granulaire et une révocation instantanée, essentiel pour la maintenance ou les audits.

Télétravail sécurisé

Offrez à vos collaborateurs distants un accès sécurisé et audité aux ressources internes, sans exposer votre réseau via un VPN direct ou des postes non maîtrisés.

Environnements Cloud

Sécurisez et centralisez la gestion des accès privilégiés aux consoles et ressources IaaS/PaaS (AWS, Azure, GCP) pour une gouvernance unifiée.

Intégration DevOps

Sécurisez l'injection de secrets et la rotation des identifiants dans vos pipelines CI/CD, garantissant que les outils d'automatisation opèrent avec le moindre privilège.

Infrastructures OT/SCADA

Isolez et contrôlez les accès aux systèmes industriels (PLCs, HMIs) pour prévenir les cyberattaques sur les environnements critiques de production.

🎯 L'objectif : visibilité totale sur les accès

Savoir qui accède à quoi, quand, pourquoi et quelles actions sont réalisées.

Qui ?

Identification nominative de chaque administrateur ou prestataire

Quoi & Quand ?

Ressource accédée, horodatage précis de chaque session

Pourquoi & Comment ?

Justification de l'accès et enregistrement complet des actions réalisées

Conformité réglementaire : un allié stratégique

Face à l'évolution constante des menaces et l'accroissement des exigences légales, le bastion WALLIX devient un levier essentiel pour les organisations cherchant à garantir leur conformité. Il apporte une réponse concrète aux défis posés par des réglementations clés telles que NIS2, ISO 27001, TISAX, RGPD et DORA, en sécurisant et en traçant l'ensemble des accès à privilèges.

NIS2 : Renforcement de la cyber-résilience

- Garantit la **sécurité des accès aux systèmes critiques** (articles 20, 21).
- Facilite la **gestion des incidents** grâce à la traçabilité complète des sessions (article 23).
- Sécurise la **chaîne d'approvisionnement** numérique en contrôlant les accès des tiers (article 21).

ISO 27001 : Maîtrise de la sécurité de l'information

- Assure la **gestion des accès** (A.5.15, A.5.16, A.5.18).
- Permet la **journalisation et la surveillance** des activités des utilisateurs (A.8.16).
- Contribue à la protection des **informations sensibles** et à la conformité (A.5.23).

TISAX : Sécurité pour l'industrie automobile

- Répond aux exigences spécifiques de **protection des prototypes** et données de R&D.
- Facilite les **audits** en fournissant des preuves de contrôle d'accès et de traçabilité.
- Gère de manière sécurisée les **accès des partenaires** et fournisseurs de la chaîne automobile.

RGPD : Protection des données personnelles

- Contrôle l'**accès aux systèmes contenant des données personnelles** (article 32).
- Fournit une **preuve de l'intégrité et de la confidentialité** des données (article 5).
- Soutient l'**obligation de rendre compte** en traçant les opérations sur les données (article 5).

DORA : Résilience opérationnelle numérique financière

- Renforce la **gestion des risques liés aux TIC** pour les entités financières.
- Sécurise les **accès aux infrastructures critiques** et aux données financières.
- Améliore la **résilience face aux cyberattaques** et aux interruptions de service.

En offrant une solution unifiée de gestion des accès à privilèges, WALLIX simplifie la démonstration de la conformité et réduit significativement les risques de non-conformité, protégeant ainsi l'organisation des sanctions et des dommages réputationnels.

Bastion ≠ MFA : une complémentarité essentielle

Le MFA seul ne suffit pas

Le MFA vérifie l'identité à l'entrée — mais ne contrôle pas ce que fait l'administrateur une fois connecté, ni avec quels droits.

Le Bastion complète le MFA

WALLIX applique une véritable politique de **Privileged Access Management (PAM)** : contrôle granulaire des droits, enregistrement des sessions et révocation immédiate des accès.

Pour un CISO/RSSI, WALLIX constitue une brique essentielle pour **réduire le risque lié aux comptes à privilèges** et renforcer la traçabilité du système d'information.

1

MFA

Vérifie l'identité

2

Bastion PAM

Contrôle les accès

3

Traçabilité

Enregistre les actions

4

Conformité

ISO 27001, NIS2, TISAX

Comment déployer WALLIX Bastion : les étapes clés d'un projet PAM réussi

La mise en œuvre d'une solution de gestion des accès à privilèges (PAM) est un projet stratégique qui nécessite une approche méthodique. Pour un CISO ou un RSSI, il est crucial de suivre un cheminement clair pour garantir l'efficacité du déploiement de WALLIX Bastion et maximiser le retour sur investissement, en minimisant les risques et en assurant une adoption réussie.

Audit des Comptes Privilégiés

Identification exhaustive de tous les comptes, utilisateurs et applications disposant d'accès privilégiés, y compris les comptes de service et génériques, sur l'ensemble de votre infrastructure IT et OT.

Définition des Politiques d'Accès

Élaboration de règles d'accès granulaires basées sur le principe du moindre privilège, incluant les workflows de demande/approbation, les durées d'accès limitées et les contrôles de session spécifiques à chaque ressource.

Déploiement Technique et Intégration

Installation et configuration du bastion, intégration transparente avec vos annuaires d'entreprise (Active Directory, LDAP) et vos systèmes de gestion des informations et événements de sécurité (SIEM).

Formation et Accompagnement des Équipes

Accompagnement ciblé et formation des administrateurs, des équipes de sécurité, des équipes opérationnelles et des utilisateurs finaux pour une adoption fluide et une utilisation optimale de la solution au quotidien.

Amélioration Continue et Évolution

Mise en place de revues régulières, adaptation des politiques aux nouveaux cas d'usage, suivi des indicateurs de performance et ajustements nécessaires pour maintenir un niveau de sécurité optimal.

Un projet PAM réussi est un processus itératif qui s'aligne sur les besoins évolutifs de votre organisation, garantissant une protection pérenne contre les menaces internes et externes.

🔎 Un accès administrateur ne devrait jamais être direct, permanent ou impossible à auditer.

Prenez le contrôle de vos accès à privilèges. Passez à l'action avec WALLIX Bastion.

Réduire la surface d'attaque

Éliminez les accès directs et non contrôlés

Renforcer la traçabilité

Chaque session enregistrée, chaque action auditée

Assurer la conformité

ISO 27001 · TISAX · NIS2