WALLIX
BASTION

LE PRINCIPE DU MOINDRE PRIVILÈGE AU SERVICE DE LA SÉCURITÉ

PEDM
PRIVILEGED ELEVATION AND DELEGATION MANAGEMENT

Un périmètre de sécurité pour vos systèmes critiques

Les droits administrateurs introduisent des vulnérabilités dans vos systèmes critiques. Assurez-vous que seul le privilège adéquat est accordé au compte adéquat, au moment opportun, sans compromettre la productivité.

APPLICATION DU PRINCIPE DU MOINDRE PRIVILÈGE

- **Éliminez les risques liés aux utilisateurs surprivilégiés** pouvant compromettre vos données,
- **Politique de zéro administrateur local :** accordez des privilèges très finement et octroyez des droits spécifiques à chaque utilisateur,
- **Répartition des privilèges en établissant un contexte de sécurité pour les applications et processus** plutôt que pour les utilisateurs,
- **Favorisez la productivité :** les utilisateurs non-administrateurs peuvent toujours exécuter des tâches requérant des privilèges.

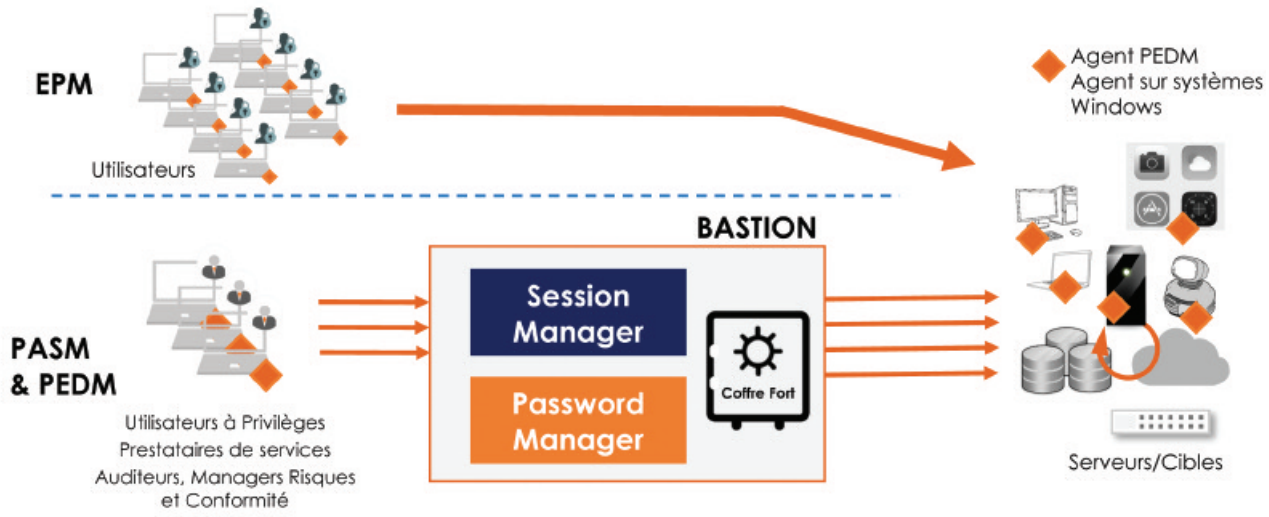
GESTION DES ACCÈS À PRIVILÈGES POUR LES SYSTÈMES CRITIQUES

- **Protégez les ressources** avec des contrôles d'accès utilisateur, la rotation des mots de passe et la limitation des droits locaux,
- **Sécurisez les systèmes critiques** grâce au contrôle des sessions et à la gestion locale des applications et des processus système,
- **Tracez et surveillez l'activité** avec l'enregistrement complet des sessions, des métadonnées et des journaux.

PROTECTION DES INFRASTRUCTURES

- **Affinez les droits applicatifs** pour que les utilisateurs autorisés ne puissent exécuter que les actions autorisées,
- **Prévenez les attaques connues et inconnues** en bloquant toutes les actions non autorisées tentant de modifier le système,
- **Neutralisez les logiciels de rançon :** les opérations de chiffrement sont détectées avant leur exécution.

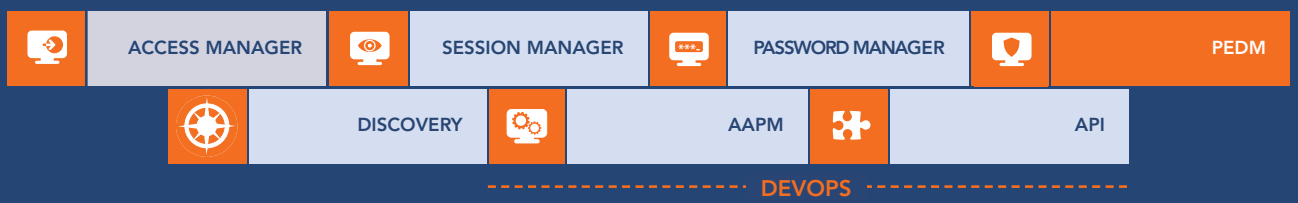
- **Intégré avec le Bastion** pour renforcer la sécurité et protéger l'accès aux ressources critiques contre l'usurpation d'identité
- **Listes blanche/grise/noire d'applications** pour éliminer les administrateurs locaux ou limiter les droits d'utilisateurs
- **Supporté par toutes les plateformes** Windows, Desktop ou Windows Server
- **Gestion centralisée et simplifiée** grâce à l'intégration avec Microsoft Active Directory et sa base de données
- **Technologie brevetée :** Affectation d'un contexte de sécurité aux processus et applications
- **Sécurité au niveau applicatif** pour éliminer les comptes administrateurs sur les systèmes
- **Blocage des ransomwares** grâce à la détection en temps réel des fonctions système telles que l'exécution d'opérations de chiffrement
- **Protection des fichiers contre la falsification** au niveau NTFS
- **Élimination des mots de passe d'administrateur local** partagés sur le réseau
- **Intégration avec les SIEMs** pour centraliser les journaux systèmes et permettre de détecter les potentielles menaces



Solution WALLIX Bastion PASM + PEDM : une protection totale sans impact sur la productivité

- **Protection holistique des ressources** grâce à un coffre-fort pour les identifiants, au contrôle des sessions et à la sécurité locale des équipements
- **Sécurité proactive au niveau du système et des processus,** adaptée aux menaces en évolution constante
- **Gestion simplifiée des règles de moindre privilège**, facile à mettre en œuvre et avec une granularité très fine
- **Aucun impact sur les performances des systèmes d'information** grâce à l'intégration avec le système d'exploitation
- **Solution *ad hoc* utilisant des listes blanches, grises et noires** adaptées à l'expérience des utilisateurs

BASTION



WALLIX
CYBERSECURITY SIMPLIFIED

WWW.WALLIX.COM