

# WALLIX BestSafe

## Endpoint Management

Supprimez les privilèges utilisateurs des endpoints et évitez la propagation des malwares, ransomwares et crypto-virus sans impacter votre productivité.



### LE PRINCIPE DU MOINDRE PRIVILÈGE AU SERVICE DE LA PROTECTION DES ENDPOINTS

- > Supprimez les privilèges des utilisateurs sur les endpoints
- > Surveillez et bloquez les processus les plus critiques sur les machines
- > Évitez la propagation de logiciels malveillants tentant de s'exécuter à partir du endpoint

.....



### GARANTIR LA PRODUCTIVITÉ DES UTILISATEURS

- > Les utilisateurs peuvent exécuter toutes les applications dont ils ont besoin, même celles qui nécessitent des privilèges
- > La DSI contrôle et bloque l'installation par l'utilisateur d'applications indésirables
- > Expérience utilisateur fluide

.....



### SIMPLIFIER LE MANAGEMENT DE LA SÉCURITÉ

- > Catalogue d'applications autorisées, liste noire d'applications blacklistées
- > Politique de sécurité des endpoints globale et facile à déployer
- > Permet aux utilisateurs d'installer un ensemble d'applications autorisées sans le support de la DSI

.....



---

## BestSafe est une solution de protection des endpoints modulaire, basée sur des règles simples et faciles à mettre en place

- Prévenir les attaques des ransomwares et malwares et leurs conséquences
- Technologie innovante et facile à mettre en place
- Aucune infrastructure spécifique requise pour l'installation et l'exploitation
- Réduction effective du risque de failles de sécurité sur les systèmes Windows

---

## À propos de WALLIX

Les solutions WALLIX protègent des cybermenaces, vols et fuites de données liés aux identifiants volés et aux privilèges détournés. Elles sont distribuées par un réseau de plus de 170 revendeurs et intégrateurs à travers le monde. Cotée sur Euronext, WALLIX accompagne plus de 1000 organisations dans la sécurisation de leur avenir numérique.

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

**WALLIX**  
CYBERSECURITY SIMPLIFIED

## WALLIX BESTSAFE

### CARACTÉRISTIQUES TECHNIQUES :

- > Des niveaux de privilèges pour les utilisateurs et les processus

Blocages granulaires et permissions pour exécuter des tâches et des applications :

- Listes blanches
- Listes noires
- Ransomware

- > Gestion des privilèges

- Au niveau applicatif
- Au niveau de l'utilisateur

- > Règles et paramètres personnalisés

- Etablir des permissions et des privilèges par utilisateur, par application et par groupe
- Les applications usuelles peuvent s'exécuter mais leurs appels d'API les plus dangereux sont bloqués

- > Gestion des mots de passe

- Rotation aléatoire quotidienne des mots de passe sur l'ensemble du parc

- > Management centralisé

- Console unique de gestion des règles de gouvernance des processus applicatifs

- > Analyses et rapports

- Intégration avec les systèmes de SIEM (Security Information and Event Management)
- Création d'alertes et d'alarmes

- > Surveillance et contrôle de l'exécution et de l'utilisation des process les plus critiques

- Surveillance des ordinateurs, processus et applications. Blocage si nécessaire.