

# WALLIX BestSafe

## Endpoint Privilege Management

Elimine los riesgos asociados con los usuarios con excesivos privilegios y evite la propagación de malware, cripto-virus y ataques de ransomware.



### PRINCIPIO DEL MENOR PRIVILEGIO PARA PROTEGER LOS ENDPOINTS DE ATAQUES

- > Elimine admin privilegios de usuario de los endpoints
- > Monitoree y bloquee los procesos potencialmente peligrosos en el endpoint
- > Evite la propagación de malware que intenta ejecutarse desde el endpoint

.....



### GARANTICE LA PRODUCTIVIDAD DE LOS USUARIOS DEL NEGOCIO

- > Los usuarios pueden ejecutar todas las aplicaciones que necesiten, incluso aquellas que requieren privilegios elevados
- > TI controla y bloquea la instalación de aplicaciones no deseadas
- > Experiencia de usuario perfecta, sin impacto significativo en la productividad

.....



### ADMINISTRACIÓN DE SEGURIDAD SIMPLIFICADA

- > Sencillas listas blancas y negras de aplicaciones
- > Política de seguridad de endpoint global y fácil de implementar
- > Permitir a los usuarios instalar un conjunto de aplicaciones autorizadas, sin soporte de TI

.....



---

## BestSafe es una solución modular de protección de endpoint basada en reglas simples y fáciles de implementar

- Evite los ataques y sus consecuencias mientras lucha eficazmente contra el malware
- Tecnología innovadora y fácil de implementar
- No requiere infraestructura adicional para la instalación y operación
- Reduce efectivamente el riesgo de brechas de seguridad en sistemas Windows

---

## Acerca de WALLIX

Las soluciones WALLIX protegen contra las amenazas cibernéticas, el robo y la fuga de datos vinculada a credenciales robadas y privilegios malversados. Son distribuidos por una red de más de 170 revendedores e integradores en todo el mundo. Listado en Euronext, WALLIX apoya a más de 1,000 organizaciones para asegurar su futuro digital.

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

**WALLIX**  
CYBERSECURITY SIMPLIFIED

## WALLIX BESTSAFE

### CARACTERÍSTICAS TÉCNICAS:

#### > Niveles de privilegios para usuarios y procesos

Bloqueo granular y permisos para ejecutar tareas y aplicaciones:

- Listas blancas
- Listas grises
- Listas negras
- Ransomware

#### > Gestión de privilegios

- a nivel de aplicación
- a nivel de usuario

#### > Reglas y parámetros personalizados

- Establecer permisos y privilegios por usuario, aplicación y grupo
- Las aplicaciones habituales pueden ejecutarse pero las llamadas a la API más peligrosas están bloqueadas

#### > Gestión de contraseñas

- Rotación de contraseñas diario y diferente por dispositivo

#### > Gestión centralizada

- Acceda al Controlador de Dominio más cercano

#### > Análisis e informes

- Integración con sistemas SIEM
- Creación de alertas y alarmas

#### > Monitoreo y control de ejecución y uso de los procesos más críticos

- Supervisión de equipos, procesos y aplicaciones