

WALLIX BestSafe

Endpoint Privilege Management

Eliminate the risks associated with overprivileged users and avoiding the spread of malware, crypto-viruses and ransomware attacks.



LEAST PRIVILEGE TO PROTECT ENDPOINTS FROM ATTACKS

- > Remove user privileges from endpoints
 - > Monitor and block the most critical processes in the endpoint
 - > Avoid the spread of malware attempting to run from the endpoint
-



ENSURE BUSINESS USER PRODUCTIVITY

- > Users can run all the applications they need, even those requiring privileges
 - > IT controls and blocks installation of unwanted applications
 - > Seamless user experience, zero impact on productivity
-



SIMPLIFIED SECURITY MANAGEMENT

- > Simple black- and white-listing of applications
 - > Global and easy-to-deploy endpoint security policy
 - > Enable users to install a set of applications without IT support
-



BestSafe is a modular endpoint protection solution based on simple rules that are easy to implement

- Prevent attacks and their consequences while fighting effectively against malware.
- Easy-to-implement, innovative technology.
- No specific infrastructure required for installation and operation.
- Effectively reduces the risk of security breaches on Windows systems.

About WALLIX

WALLIX solutions protect against cyber threats, theft and data leaks linked to stolen credentials and misappropriated privileges. They are distributed by a network of more than 170 resellers and integrators worldwide. Listed on Euronext, WALLIX supports more than 1,000 organizations in securing their digital future.

www.wallix.com   

WALLIX
CYBERSECURITY SIMPLIFIED

WALLIX BESTSAFE

TECHNICAL CHARACTERISTICS:

> Privilege levels for users and processes

Granular blocking and permissions to execute tasks and run applications:

- White lists
- Black lists
- Ransomware

> Privilege management

- At the application level
- At the user level

> Personalized rules and parameters

- Establish permissions and privileges by user, application, and group
- Usual applications can be executed but the most dangerous API calls are blocked

> Password management

- Rotate passwords daily and vary by device

> Centralized management

- Access the closest Domain Controller

> Analytics and reports

- Integration with SIEM systems
- Creation of alerts and alarms

> Monitoring and control of execution and use of the most critical processes

- Oversight of computers, processes and applications