WALLIX BASTION

LEAST PRIVILEGE IN ACTION

PEDM
PRIVILEGED ELEVATION AND DELEGATION MANAGEMENT

A security perimeter for your critical systems

Administration rights introduce critical vulnerabilities to your vital assets. Ensure that only the right privilege is granted to the right account, at the right time, without compromising productivity.

ENFORCED LEAST PRIVILEGE MANAGEMENT PRINCIPLE

- **Eliminate the risk of overprivileged users** who can wreak havoc in your IT network at the click of a button
- **Zero local administrator policy:** grant privileges at a granular level with the ability to assign specific rights to a user to execute a specific action
- **Privilege segregation** by establishing a security context for applications & processes rather than by user
- **Facilitate productivity:** non-administrator users can still run tasks with adapted privileges with no impact on productivity

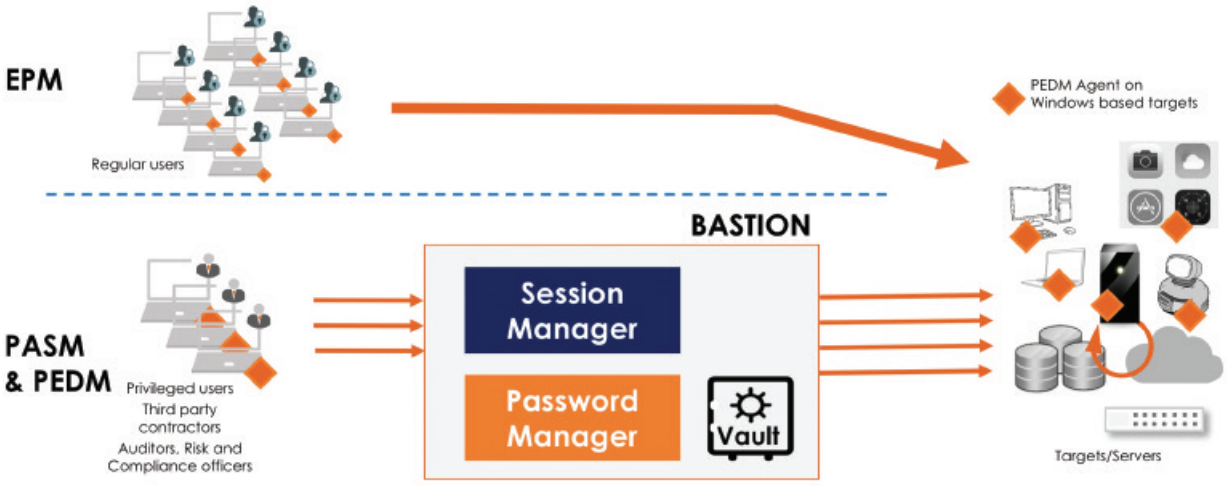
PRIVILEGED ACCESS MANAGEMENT FOR CRITICAL SYSTEMS

- **Protect assets** with combined user access workflows, credential rotation, and local rights limitation
- **Secure critical systems** through session control and local system application and process management
- **Trace and monitor activity** with complete session recording, metadata, and logs for local devices

ENDPOINT SYSTEM PROTECTION

- **Fine-tune application rights** so that they can only be used to perform authorized actions by authorized users
- **Prevent known and unknown attacks** by blocking all unauthorized actions intending to modify the system
- **Neutralize ransomware:** encryption operations are detected before being carried out

- **Integrated with Bastion PAM solution** to increase security for identity theft protection and access to critical assets
- **Application white/grey/black-listing** to eliminate local administrators or limit user rights
- **Fully supported** on all Windows platforms, desktop or Windows Server
- **Centralize and simplify management** through integration with Microsoft Active Directory and its database
- **Exclusive patented technology** that assign security context for processes and applications
- **Application-level security** to eliminate administrator accounts on endpoints
- **Real-time detection of system functions** such as performing encryption operations to block ransomware
- **File protection** against tampering at NTFS level
- **Eliminate local administrator passwords** shared across systems
- **Integrate with SIEM** to centralize log information for advanced threat detection



WALLIX Bastion PASM + PEDM solution: total protection with no impact on productivity

- **Holistic protection of assets** with best-in class credentials vaulting and session control, enhanced with privilege protection for the endpoint
- **Proactive security at the system and process** level adapted to always evolving threats
- **Simplified management of generic rules with endpoint least privilege principle,** easy to implement and with fine level of granularity
- **No impact on systems performances** thanks to deep integration with the Operating System
- **Tailor made ad-hoc solution** using white, grey and black listing, adapted to IT operations practices

BASTION

WALLIX
CYBERSECURITY SIMPLIFIED

WWW.WALLIX.COM