Privileged Access Management
PEDM

wallix pam

Enhance WALLIX PAM with Least Privilege Strategy

Privilege escalation is at the heart of most cyber-attacks and system vulnerabilities. Yet, many of these risks can be effectively mitigated by enforcing the Principle of Least Privilege. WALLIX PEDM employs local agents on managed systems to grant specific privileges to logged-in users, providing process-level security that enables organizations to eliminate administrator accounts. It also delivers application-level control and file monitoring, reducing the likelihood of security breaches without compromising productivity and ensuring compliance with regulatory standards.

Capabilities

Principle of Least Privilege

- Eliminate the need for privileged accounts within your organization
- Assign privileges only at the right time and context

Centralized Management

- Manage security policies from a centralized console
- Leverage full integration with Active Directory to store rules and configurations
- The agent periodically updates its policies to apply them offline

Fine-Grained Least Privilege

- Elevate privileges for standard users on Windows and Linux
- Control processes through fine-grained policies
- Agents apply policies without affecting performance

Increased Security

- Implement folder rules and protect important data from being modified
- Monitor elevated actions
- On-demand process elevation

wallix

Technical Characteristics

> Process control

- Elevate, reduce, or block privileges for processes
- Rule-based group membership

> Supported operating systems

- Windows Server 2003 and above
- Windows XP SP3 and above
- Linux Ubuntu 18-22 and Linux Debian 9-12
- RedHat 8-9

> Management

- Active Directory integration
- MMC snap-in

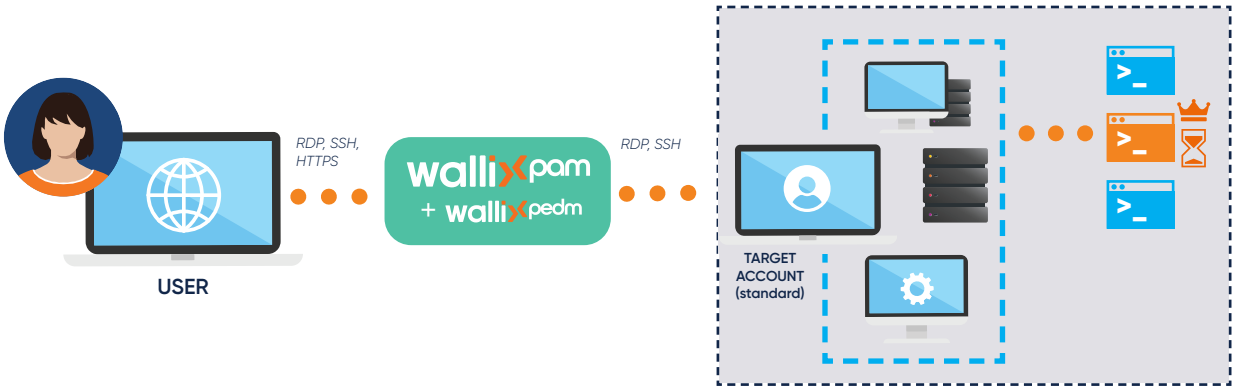
> Monitoring

- Event-based
- SIEM integration

How it Works

WALLIX PEDM uses exclusive patented technology to assign the necessary security context to each process or application, regardless of the user credentials with which it is executed. With WALLIX PEDM, privileges are granted to processes and applications instead of users, unlike trad itional tools on the market.

- **Control access to IT resources** by granting permissions to log in through a standard account.
- **Give privileges** to those processes that need them for the time needed.
- **Monitor every action** that takes place in a session.
- **No need for admin accounts** in the infrastructure – Not even for IT



Benefits

FAST IMPLEMENTATION

Implement WALLIX PEDM in your environment in just a few hours.

IMMEDIATE PROTECTION

Control privilege actions and prevent the execution of unauthorized processes from the get-go.

100% SCALABLE

Using a client-server approach allows WALLIX PEDM to be as scalable as the organization itself.

TRANSPARENT TO END USERS

WALLIX PEDM relies on the mechanism of the operating system to grant security.

About WALLIX

WALLIX protects identities and access to IT infrastructure, applications, and data. Specializing in Privileged Access Management, WALLIX solutions ensure compliance with the latest IT security standards and protect against cyber-attacks, theft, and data leaks linked to stolen credentials and elevated privileges.