



Security is nothing without Control.

**WALLIX BASTION,
DEDICATED
TO PROTECTING
STRATEGIC DATA
AND ASSETS**

PAM'S TRUE PURPOSE

The core objective of privileged access management is to ensure that only the right person can access the right system at any given time, **but you need more.**

A comprehensive PAM solution addresses not just who has access, but offers in-depth monitoring and audit of what users do in your most critical systems.

Who Has Access To What, When & What Do They Do?

Identifying what users do requires more than a vault. WALLIX's PAM solution is recognized for its best-in-class Session Manager that guarantees full control, monitoring and auditing of privileged session activity.

■ **All-in-one solution:** The Bastion features powerful *Session* and *Password* solution, secure web access with the all-new *Access Manager*, and run reports on all user accounts in your network (for free!) with *Discovery*.

■ **Enhanced security:** WALLIX doesn't just stack AES-256. We offer full CA management and generation, Elliptic Curve Cryptography, and CHACHA20.

■ **Low Total Cost of Ownership:** No need to install multiple servers. Take advantage of full capabilities through a single point of entry (compared to many servers with other solutions).

WHY WALLIX

The WALLIX Bastion is an all-in-one solution. What's more, WALLIX offers unique agentless Session Probe technology: no need to deploy and maintain a fleet of agents across your infrastructure.

WALLIX is Cybersecurity Simplified: easy to use, easy to integrate with existing solutions, and easy user adoption. And it takes just 15 minutes in-lab and mere hours on-premises to deploy.

Learn more about the WALLIX Bastion at www.wallix.com or [get in touch!](#)



● STRONG ● GOOD ● POOR

WALLIX THYCOTIC

	WALLIX	THYCOTIC
Unified Discovery: Discover Unix/Windows/AD accounts	●	●
Discovery reporting	●	●
Session & application remote access	●	●
Audit and monitoring	●	●
Workflows	●	●
Behavior analytics bidirectional integration with SIEMS	●	●
Reporting	●	●
HA/DRA	●	●
Professional Password vault and clustering	●	●
Encryption capabilities*	●	●
Least privileges capabilities & application control	●	●
Ease of deployment	●	●
Pricing	●	●
TCO	●	●
Support/Formation	●	?

*Encryption is key for PAM a solution. If everyone advertise the support of AES 256, the WALLIX Bastion offers more: it can be a Certificate Authority, it supports CHACHA20 and implements Elliptic Curve Cryptography!

**The WALLIX Bastion is an all-in-one solution. Access all desired capabilities without deploying separate systems for each of them.

WALLIX SESSION MANAGER

This module enables administrators to manage privileged user sessions in real-time for enhanced risk prevention:

- Manage and govern privileged accounts through:
 - Unix or Windows operating systems, network devices, databases, mainframes, virtual infrastructures, or SU/SUDO injection
 - Consoles, business web applications, and fat clients (e.g.: firewall management, Salesforce, or Sage)
 - Direct access to resources using native clients (PuTTY, WinSCP, MSTC, OpenSSH, etc.) with connection rules embedded directly into the Bastion
 - Workflows designed with context-relevant access configurations
- Gather metadata (session probe) to supply dashboards with detailed and context-relevant information
- Remote APP management

WALLIX PASSWORD MANAGER

This module allows administrators to manage passwords and enforce password policies. The security is enhanced by ensuring that users only have permissions to access the resources they need to complete their job duties. This helps guarantee that passwords and SSH keys will not be disclosed or misused:

- Enforce periodic change and rotation of passwords
- Includes dedicated plugin library for target password management
- Support SSH certificates
- Application-to-Application to Password Management and Services accounts management

WALLIX ACCESS MANAGER

WALLIX Access Manager provides a web portal for users and administrators. Administrators can track operations more efficiently and in real-time:

- Global search across your entire Bastion infrastructure
- Single sign-on (SSO) integrates across all deployed Bastions using RDP and SSH architecture
- Protect assets and systems through set rules that can automatically authorize or revoke user access
- Delegation to third-party systems for user authentication and identification (SAML 2.0)
- Multi-tenant architecture compatible with service providers' environments, with a complete isolation of instances
- Customizable web interface
- No VPN required for remote access

FOR MORE INFORMATION

Email: info@wallix.com

www.wallix.com

TECHNICAL SPECIFICATIONS

Encryption Algorithm

AES 256.

Authentication method

Identifier, LDAP, Active Directory, Radius, TACAS+, Kerberos, X509, OTP, Web SSO,

Authentication technologies utilized by WALLIX ALLIANCE PARTNERS-WAP.

Protocols

HTTP/HTTPS, RDP/TSE, SSH, VNC, Telnet, SFTP.

Monitoring

SNMP & e-mail monitoring tools ticketing and workflows for administrator notifications.

Architecture

3 layers for scalability (WALLIX Bastion farm, Bastion cluster, bounce server cluster).

Integration/Deployment

Bastion running as a proxy or in a transparent mode.

- Available as On Premise or On Demand
- Accessible through AWS & Azure marketplaces
- Available as a hardware appliance for virtual machine, or as a software

Easy provisioning and synchronization with central Identity Access Management solutions within the REST API.

Plugins to integrate with all business partners environments, supported by WALLIX ALLIANCE PARTNERS-WAP.

High availability and Load Balancing

Bastion clusters.
F5 BIG IP, A10 Thunder.