

# BASTION

PRIVILEGED ACCESS MANAGEMENT PLATFORM

DEDICATED  
TO PROTECTING  
STRATEGIC DATA  
AND ASSETS



## WALLIX Bastion: Secure Privileged User Access

The WALLIX Bastion is a centralized solution that secures privileged access and monitors privileged sessions. It provides unalterable audit trails and behavioral analysis reports on privileged user activity. These resources can be useful when making security decisions and can help prevent the spread of malicious software to other systems.

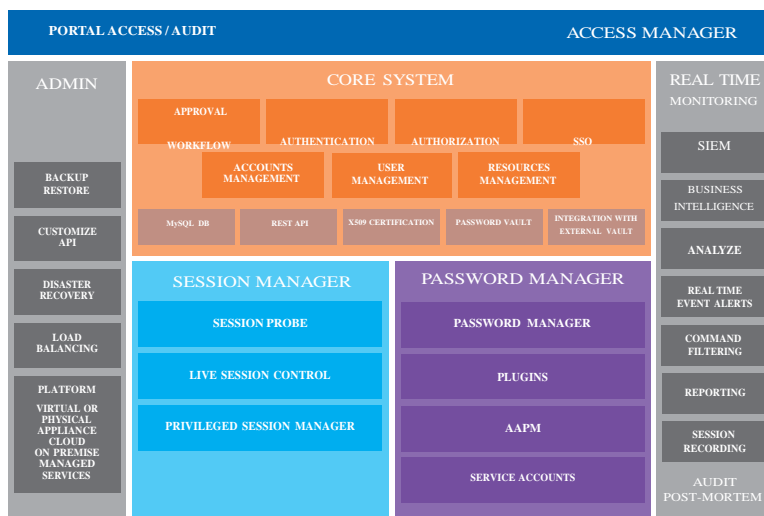
### WALLIX BASTION CORE

The core of the WALLIX Bastion allows you to secure your privileged accounts and support your teams regulatory compliance efforts. It includes the following capabilities:

- **Administration:**
  - HA/load balancing
  - Disaster recovery
  - Backup and restore
  - Management APIs
- **Audit/Real-time monitoring:**
  - Real-time monitoring of all privilege user activities through alerts, reporting and remote session
  - Automatic session termination based on actions interception: blacklist, widget event reports, process sequences, keyboard traffic ("4-Eyes", OCR) or the use of bounce servers)
  - Users accountability and trace actions for statistical reports on monitored activity using:
    - Video and text recordings for all videos
    - Complete audit logs and advanced searches to isolate incidents
- **Password Vault:**
  - Password and SSH keys safekeeping in the WALLIX certified vault
  - Open architecture to enable integration with third party vaults
- **Reporting:**
  - Basic reports accessible from the user interface and downloadable as .csv file
  - Bi-directional SIEM integration for advanced reporting and real-time processing of malicious behavior detection

## FEATURES & BENEFITS

- n Seamless integration with existing environments, capitalizing on previous investments into previous security solutions thanks to universal connectors and plugins
- n The platform provides a single point of access that can adapt to meet your organizations unique needs using a scalable and interoperable architecture
- n Easy and efficient deployment toward quickly attainable milestones resulting in better control over implementation and cost, while also optimizing the Total Cost of Ownership (TCO)
- n Enforce regulatory requirements through traceable audit trails and separation of operational tasks from administrative perimeter
- n Identify accounts at risk and map your privileged accounts using the WALLIX Discovery



The WALLIX Bastion includes session, password, and portal access management features on a unified and scalable platform for optimal security.

## 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 (SAML2.0)
- Multi-tenant architecture compatible with service providers' environments, with a complete isolation of instances
- Customizable web interface
- No VPN required for remote access

## 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.

FOR MORE INFORMATION

[info@dkbsolutions.com](mailto:info@dkbsolutions.com)