PowerBroker Password Safe

Privileged Password Management and Privileged Session Management

BeyondTrust
VISIBILITY. KNOWLEDGE. ACTION.

Many organizations use shared accounts to maintain limited sets of credentials for groups of users, administrators and/or applications. However, if managed incorrectly, this practice presents significant security risks stemming from intentional, accidental or indirect misuse of shared privileges — with little to no accountability or serious consequences — when something goes wrong.

These are just a few among the litany of challenges and risks to consider:

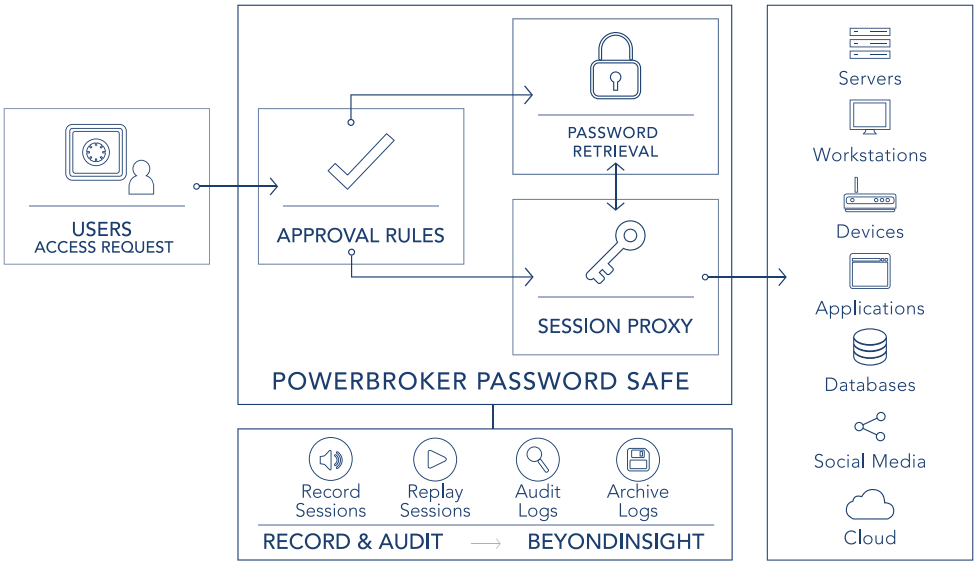
- Certain systems have embedded or hard-coded passwords
- Passwords are needed for app-to-app and application-to-database access
- Passwords are generally static, meaning they could be leaving the organization
- Password rotation is unreliable and manual
- Credentials for cloud apps are often not managed as well as those on-prem
- Monitoring, auditing and reporting on access is complex and time consuming

How do organizations ensure accountability of shared privileged accounts to meet compliance and security requirements without impacting administrator productivity?

Improve Accountability and Control Over Privileged Passwords

BeyondTrust PowerBroker® Password Safe is an automated password and session management solution that provides secure access control, auditing, alerting and recording for any privileged account — such as a local or domain shared administrator account; a user's personal admin account; service, operating system, network device, database (A2DB) and application (A2A) accounts; and even SSH keys, cloud and social media. By improving the accountability and control over privileged passwords, IT organizations can reduce security risks and achieve compliance objectives.

> "PowerBroker Password Safe is a solid tool for the secure procurement and dissemination of passwords."
>
> — Frost & Sullivan, Product Review



Password Safe automates password and session management enterprise-wide.

Key Differentiators

COMPREHENSIVE PASSWORD MANAGEMENT

Secure and automate privileged password discovery, management and rotation.

ENHANCED PRIVILEGED SESSION MANAGEMENT

Record, lock and document suspicious behavior with dual control capabilities that minimize disruptions in sessions and productivity.

SECURE SSH KEY MANAGEMENT

Automatically rotate keys on a schedule, and enforce granular access control and workflow. Leverage stored private keys for secure, proxied, and recorded access to Unix and Linux systems, without exposing keys to users.

APPLICATION-TO-APPLICATION PASSWORD MANAGEMENT (AAPM)

Eliminate hard-coded or embedded application credentials through an API interface with unlimited Password Caches for scalability and redundancy.

DISCOVERY-DRIVEN DYNAMIC POLICY

Scan, identify and profile all assets with a distributed discovery engine. Automated onboarding capabilities include dynamic categorization and policies that self-adjust to environmental changes.

ADAPTIVE ACCESS CONTROL

Grant access based on the context of each request, such as day, date, time and location.

ADVANCED THREAT ANALYTICS

Correlate data, connect evidence, and reveal user and asset risk. Receive alerts based on the scope and speed of changes in asset characteristics and user behaviors.

The PowerBroker Privileged Access Management Platform

PowerBroker Password Safe is part of the BeyondTrust PowerBroker Privileged Access Management Platform, which delivers visibility and control over all privileged accounts, users, and assets. The platform integrates a comprehensive set of PAM capabilities to simplify deployments, reduce costs, improve system security, and reduce privilege-related risks. PowerBroker solutions include:

- **Enterprise Password Security:** Provide accountability and control over privileged credentials and sessions.
- **Server Privilege Management:** Control, audit, and simplify access to business critical systems.
- **Endpoint Least Privilege:** Remove excessive user privileges and control applications on endpoints.

CONTACT

North America
info@beyondtrust.com

EMEA
emeainfo@beyondtrust.com

APAC
apacinfo@beyondtrust.com

LATAM
latam@beyondtrust.com

CONNECT

Twitter: @beyondtrust
Facebook.com/beyondtrust
Linkedin.com/company/beyondtrust
www.beyondtrust.com

Key Features

DISCOVERY AND PROFILING

- Discover all known and unknown assets, and shared user and service accounts
- Automatically discover all SSH keys on host systems
- Identify and manage assets with common traits via Smart Rules

PASSWORD PROTECTION AND SSH KEY MANAGEMENT

- Selectively process password change, password test, and account notification queue items for designated workgroups
- Support industry-standard encryption algorithms, such as AES 256 and Triple DES
- Rotate SSH keys automatically and enforce granular access control and workflow
- Get control over scripts; eliminate application credentials, files, code and embedded keys

PRIVILEGED SESSION MANAGEMENT

- Use keyword search to give admins the ability to watch, record, lock, terminate or cancel live sessions
- Record privileged sessions in real time via a proxy service for SSH, RDP, and TOAD
- Meet regulations listed in SOX, HIPAA, GLBA, PCI DSS, FDCC, FISMA, and more
- Utilize 'log off on disconnect' feature to ensure sensitive data is not exposed in subsequent RDP sessions
- Allow any Windows application to have login credentials played in automatically

WORKFLOW AND USABILITY

- Use DirectConnect to launch an SSH or RDP session by passing a string to the proxy
- Leverage Role-Based Access Controls with AD and LDAP integration for assigning roles and rights to users
- Single interface with localization for Spanish, Japanese, Korean, and Brazilian Portuguese
- Manage checkout workflow with connectivity to RDP and SSH via native desktop tools such as PuTTY and MSTSC
- Accommodate fire-call requests after hours or in other emergency situations
- Leverage a Unix/Linux Jumphost to run a command or script after the session connects
- Use "OneClick" to expedite checkout passwords, sessions and applications

DEPLOYMENT

- Benefit from a single solution for both password and session management
- Integrates with McAfee ePolicy Orchestrator to deliver complete lifecycle management of privileged account
- Deploy as hardware appliances, virtual appliances, or software
- Employ out-of-the-box connectors, plus a custom connector builder for all systems that support Telnet or SSH

SECURITY AND UPTIME

- Rely on hardened appliances with FIPS 1402-validated components, AES256 encryption & HTTPS/SSLv3 communications
- Analyze privileged password, user, and account behavior with threat analytics capabilities
- Allow an unlimited number of Password Safe appliances to be connected to an external SQL AlwaysOn Availability Group for unparalleled high-availability and scalability