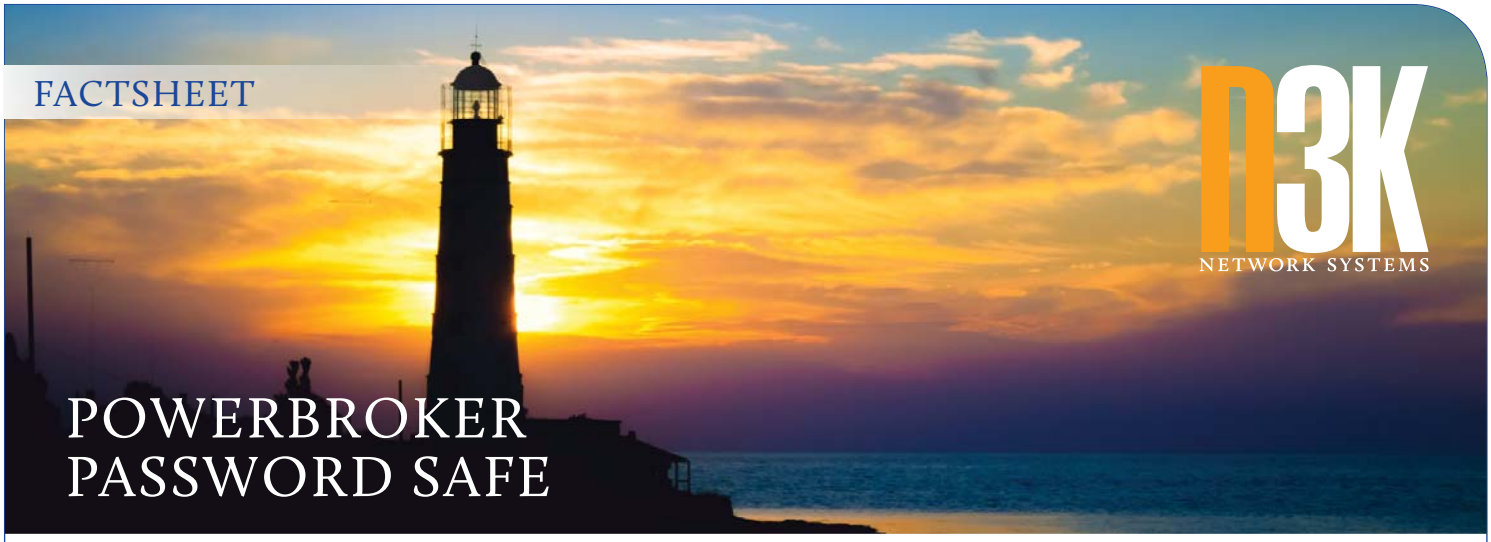


FACTSHEET

POWERBROKER PASSWORD SAFE

Privileged Password and Session Management

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

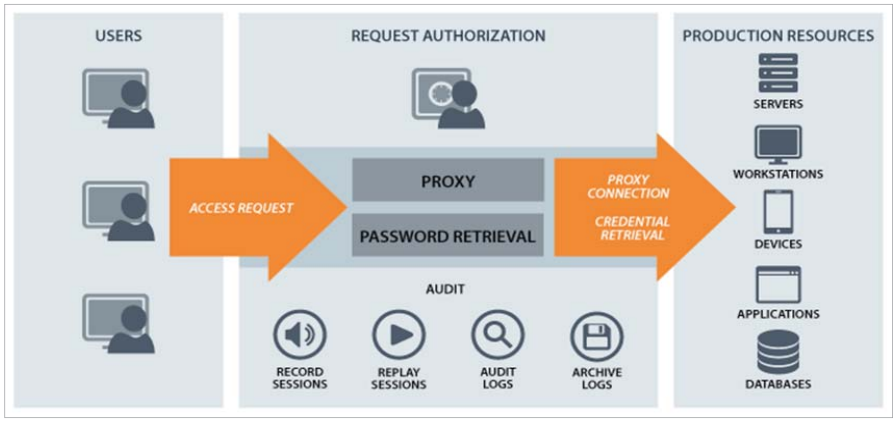
How do organizations ensure accountability of shared privileged accounts to meet compliance and security requirements without impacting administrator productivity?

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.

> „BeyondTrust PowerBroker PasswordSafe is a solid tool for the secure procurement and dissemination of passwords."
>
> - Frost & Sullivan Product Review

How it works



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.

Key Features

Discovery and Profiling

- Discover all known and unknown as sets, and shared, user and service ac counts
- Automatically discover all SSH keys on host systems
- Identify and manage assets with com mon traits via Smart Rules

Password Protection and SSH Key Management

- Selectively process password change, password test, and account notificati on queue items for designated work-groups
- Support industry-standard encrypti-on algorithms, such as AES 256 and Triple DES
- Randomize passwords on a scheduled basis or upon check-in
- Rotate SSH keys automatically and enforce granular access control and workflow
- Utilize PowerBroker for Windows to update passwords on remote and mo-bile devices
- Get control over scripts; eliminate application credentials, files, code and embedded keys

Privilegend Session Monitoring

- Manage live sessions to give admins the ability to lock, terminate or cancel sessions
- Record privileged sessions in real time via a proxy service for SSH, RDP, and any Windows applications such as TOAD – without need for Java, or a client on the desktop
- Meet regulations listed in SOX, HIPAA, GLBA, PCI DSS, FDCC, FISMA, and more
- Use keyword search to watch privile-ged sessions and log all session reviews
- Allow any Windows application to have login credentials played in auto matically with usage monitored and recorded

Workflow and Usability

- Use DirectConnect to launch an SSH or RDP session by passing a string to the proxy
- Leverage true Role-Based Access Con-trols with Active Directory and LDAP integration for assigning roles and rights to users
- Manage checkout workflow with se amless connectivity to RDP and SSH via native desktop tools such as PuTTY and MSTSC
- Accommodate fire-call requests to en-sure access to password-managed sys-tems after hours, on weekends, or in other emergency situations
- Leverage a Unix/Linux Jumphost to run a command or script after the ses-sion connects
- Use “OneClick” to expedite checkout operations for access to passwords, ses-sions and applications that would nor-mally be approved automatically

Deployment

- Benefit from a single solution for both password and session manage-ment
- 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 Pass word Safe appliances to be connected to an external SQL AlwaysOn Availa bility Group for unparalleled high high-availability and scalability

IP ADDRESS MANAGEMENT

PRIVILEGE MANAGEMENT

ACTIVE DIRECTORY MANAGEMENT

Über N3K: Schnellwachsende IP-Netzwerke erfordern professionelle Lösungen für die verschiedensten Facetten des Netzwerk-Managements. N3K Network Systems hat sich auf die Gebiete IP Address Management, Privilege Management sowie auf Active Directory Management spezialisiert. So können mit hoher Kompetenz auf die individuellen Anforderungen der Kunden zugeschnittene Lösungen entwickelt werden. N3K unterstützt die Kunden über den gesamten Projektzyklus hinweg bei Bedarfsanalyse, Konzeption, Projektplanung, Implementierung und Schulung. Hinzu kommen umfangreiche Wartungs-Services inklusive weltweitem 7x24-Support und direkter Einwahl beim Kunden. Aufbauend auf dieser einfachen und effektiven Philosophie hat sich N3K als führender Anbieter in Deutschland etabliert. Mehr als 50% der DAX-Unternehmen sind N3K-Kunden. Durch Standorte in den USA und in Singapur können die Leistungen weltweit erbracht werden.

n3k Informatik GmbH · Ferdinand-Braun-Straße 3 · 74074 Heilbronn · Telefon +49 7131 59495 0 · Telefax +49 7131 59495 100 · www.n3k.de · info@n3k.de