TECH BRIEF

BeyondTrust™

VISIBILITY. KNOWLEDGE. ACTION.

A Technical Solutions Guide for Privileged Password & Session Management Use Cases

Table of Contents

Introduction 3
Accountability and Control 3
Caching 10
Aliasing 11
Least Privilege 12
Policy Enforcement and Ongoing Administration 17
Integration and Extensibility 22
Final Thoughts on Privileged Password & Session Management 24
Capabilities Checklist 25
About the PowerBroker Privileged Access Management Platform 27
Free Tool: Privilege Discovery and Reporting Tool 28
About BeyondTrust 28

Introduction

Despite the number of data breach stories in the news, many IT organizations fall into the easy trap of using shared accounts for users, administrators, or applications. While this practice means that, when access is needed, everyone can easily pitch in to get the work done, it comes with massive, unjustifiable security and compliance tradeoffs.

In even the smallest of environments, the practice of sharing credentials poses outsized risks. And, even for small teams, the default process of manually managing passwords quickly becomes untenable when you consider:

- Various systems have embedded or hard-coded passwords (opening up opportunities for misuse)
- Passwords are needed for application-to-application (A2A) and application-to-database (A2DB) access
- Credential management for cloud apps is not as stringent as for on-premise systems
- Manual password rotation is unreliable and does not scale
- Monitoring, auditing, and reporting on access is complex and time-consuming.

So, how do organizations ensure oversight of shared privileged accounts to meet compliance and security requirements – without adversely impacting administrator productivity? For simplicity, let's group common use case themes into four categories: accountability and control, least privilege, access policy enforcement and ongoing administration, and integration and extensibility.

Accountability and Control

THE CHALLENGE - Discovering *All* Accounts & Assigning Ownership

The first step in gaining control of privileged access is to identify all of the accounts within your managed environment. People typically think of operating systems, but make sure you keep in mind routers, firewalls, servers, desktops, databases, and those Internet of Things (IoT) devices! Accounts exist on most workstations as well as on servers.

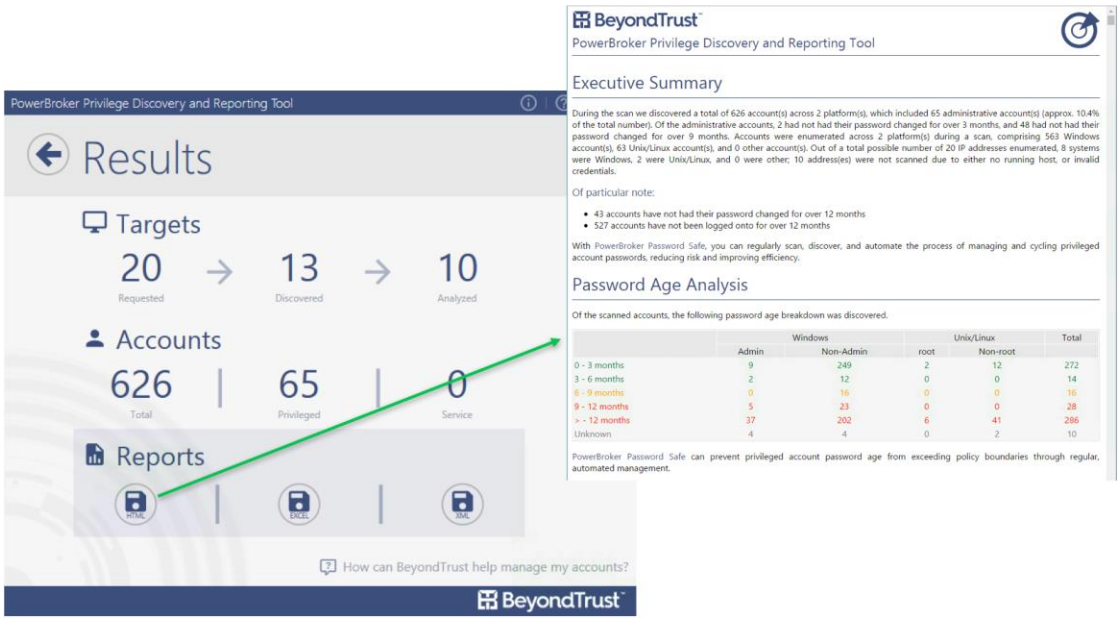


Figure 1: The free [PowerBroker Privilege Discovery and Reporting Tool] helps you quickly and easily reveal privileged accounts, users, and assets across Windows, Unix, and Linux environments.

THE SOLUTION

The PowerBroker Discovery and Reporting Tool (included free with PowerBroker Password Safe) goes a step further by uncovering hidden devices and assets, illuminating for IT the most complete picture of its privileged account landscape. For every account, you need to identify its purpose, location, and assign a business owner who can take accountability for its existence.

Once you've found all of your accounts, you can use Password Safe's smart groups feature to group them logically and apply policies efficiently to reduce overhead. After eliminating all accounts that are no longer needed, you can rely on Password Safe to store, issue, and rotate critical passwords for the legitimate accounts that remain.

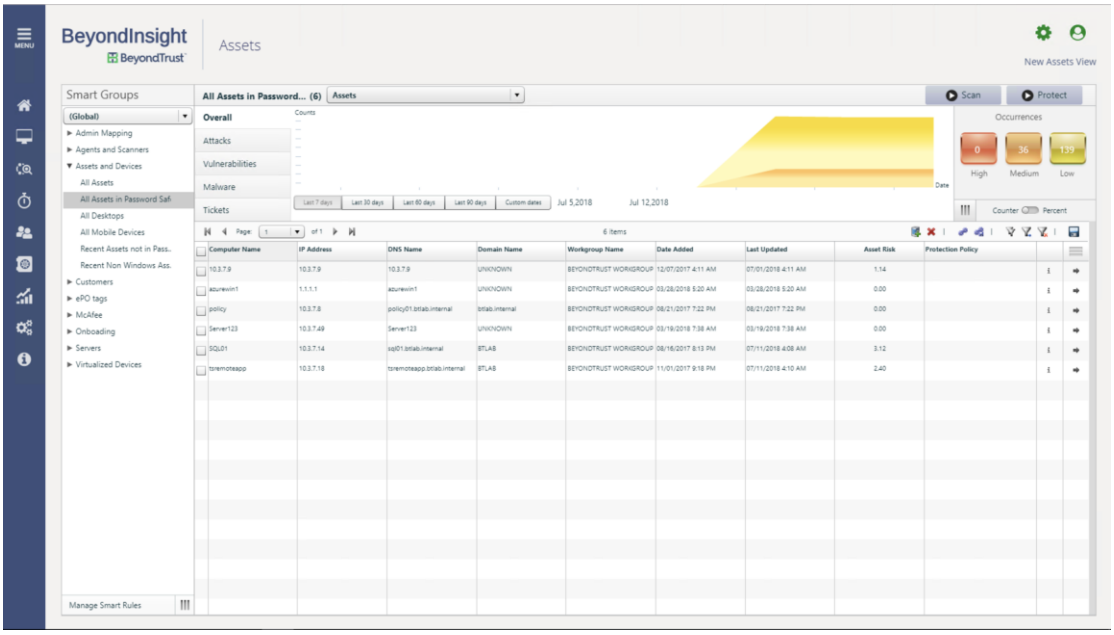


Figure 2: Available with PowerBroker, this grid allows easy segregation of assets according to any asset attribute. Attributes may be auto-populated via discovery, or manually assigned.

THE CHALLENGE - Controlling Third-Party Access to Internal Systems

Any connection into your network from or by a vendor increases the risk of a breach. In recent years, a number of high-profile breaches such as the Equifax breach, have resulted from attacks by malicious outsiders, or via third-party systems. Access controls, network separation, and activity monitoring are essential controls to implement around remote access by vendors and contractors to limit the potential scope of any threat originating from privilege misuse.

THE SOLUTION

To dramatically reduce the risk of third-party password theft and misuse, we recommend deploying Password Safe to provide a secure connection gateway through which RDP, SSH, and Windows applications can pass. Instead of issuing/revealing passwords to your third party, external users simply connect to Password Safe, activate a session, and the connection is made automatically to the target system(s). In this use case for Password Safe, the password is never revealed to the third party, and, for an extra layer of accountability, the session is recorded and logged for inappropriate behavior.

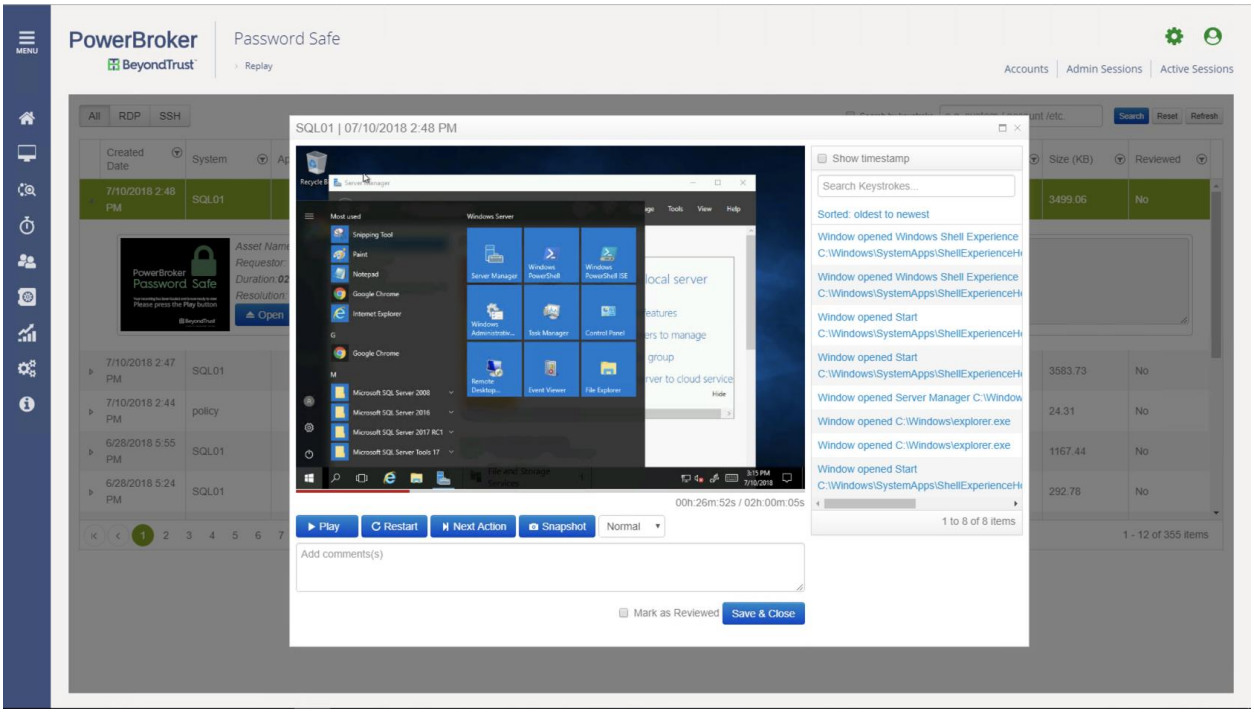


Figure 3: Third-party activity may be reviewed and signed off through the PowerBroker Password Safe session replay tool.

THE CHALLENGE - Controlling DevOps User Activity in SSH Sessions

In some circumstances, particularly in Unix and Linux systems, you may want to directly control the exact commands that can be run against a host. To improve the security of critical systems and sensitive data, one best practice abided by many organizations is implementation of host-based controls that limit which commands can be executed once a privileged session has initiated. Password Safe extends this control by automating specific commands when an SSH proxy session is opened. This reduces risk stemming from batch operators or programmatic automation jobs.

THE SOLUTION

With Password Safe, administrators can leverage a Unix or Linux jumphost to run a specific command or script after the session connects. Use cases include: menus, backup scripts, command delegation, and remote command execution (when used in conjunction with PowerBroker for Unix & Linux).

DevOps methodologies often require the pushing of code, compilation, and integration of post-compile workflows. You want developers to safely and easily execute critical workflows—but without having direct access to the systems themselves. Password Safe makes this possible by controlling the secure connection into your continuous integration/continuous deployment environment by administrators, automation jobs, or developers.

THE CHALLENGE – Updating passwords on Unix and Linux Hosts

Many password management solutions use known passwords for the accounts they manage on target systems in order to change the password after account use. When those accounts are changed out-of-band (intentionally or accidently), it stops the password manager from being able to update the account password. Most vendors address this for their customers by implementing a second, highly privileged account (sometimes called a backup or functional account). However, the drawback to this approach is that a new and privileged account is now required on every system controlled by the password management tool.

THE SOLUTION

BeyondTrust PowerBroker Password Safe, in conjunction with PowerBroker for Unix & Linux, offers the capability to change passwords on Unix and Linux hosts without the need for a functional account on each host. Leveraging remote command execution, PowerBroker for Unix & Linux will change managed account passwords on any remote system under its control.

A different option is provided when using PowerBroker Password Safe along with PowerBroker for Unix & Linux Essentials. A single system can be specified as the jump host or password proxy, leveraging a single non-privileged account in conjunction with a small piece of privilege control policy code to enable the deployed clients to update the password on managed systems. This greatly reduces the administrative overhead as well as the potential attack surface by removing the need to deploy so many privileged accounts for the sole purpose of password updates.

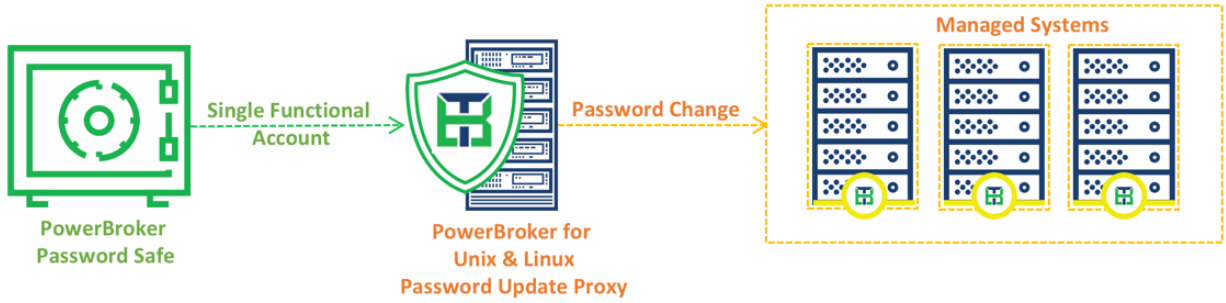


Figure 4: Setup is simple – just use the system elevation feature to point all requests to the Password Update Proxy (pbrun jumphost).

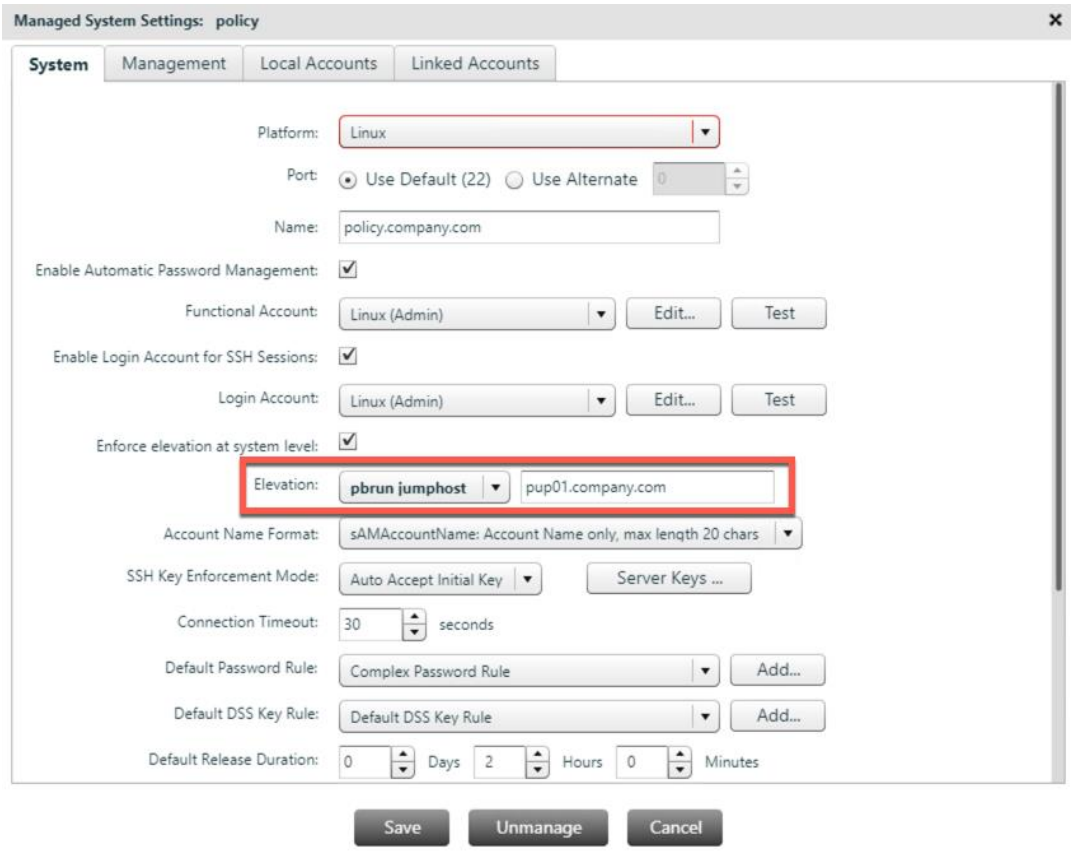


Figure 5: Policy Rules in PowerBroker for Unix and Linux allow password updates to be securely passed to managed end points.

THE CHALLENGE - Rotating Passwords on Remote or Intermittently-Connected Systems

In today's dynamic work environment, laptops travel around the world and cloud machines start and stop, as they are needed. If you attempt to manage the local passwords on most of these machines, you will likely end up with a high failure rate due to connectivity issues or

machines being offline. Organizations MUST ensure that these credentials for local (non-domain) accounts are properly cycled and checked for compliance, and that the introduction of defaults, or non-safe credentials, are brought back into compliance.

THE SOLUTION

PowerBroker Password Safe, when used with PowerBroker for Windows, can periodically check that any outstanding password-related tasks are not missed, and if they were, complete the process when the original change event fails. This integration ensures reliability in managing local credentials even in highly separated environments, or when machines are commonly offline during the scheduled password change.

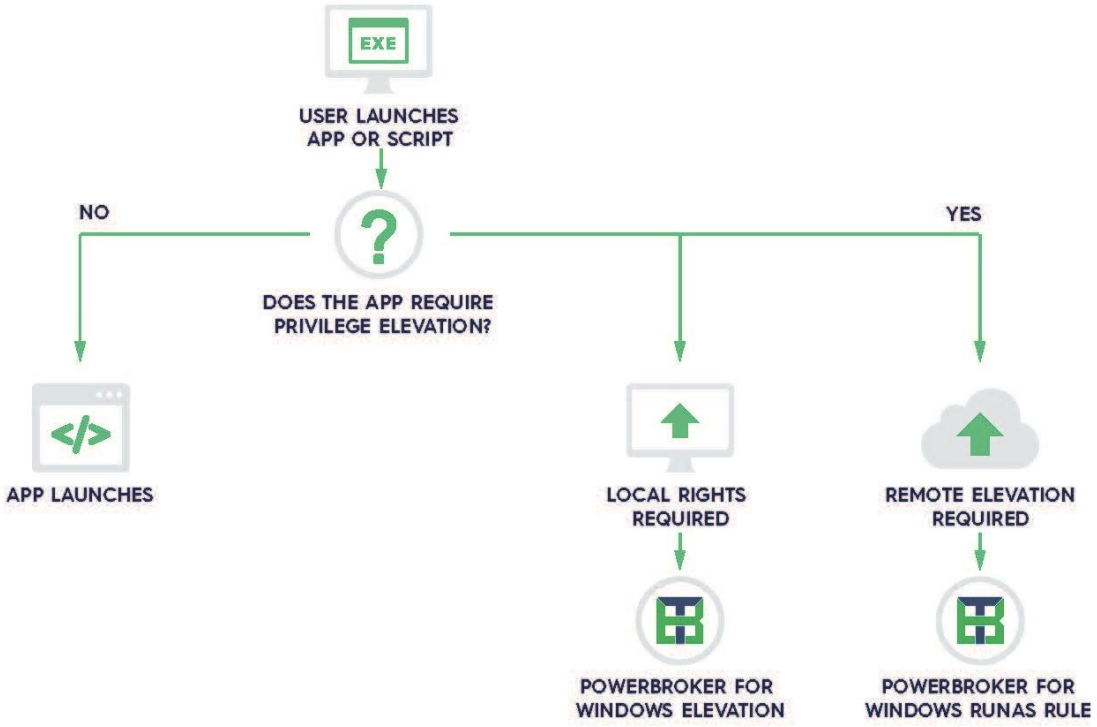


Figure 6: Privileged password management solutions can allow applications to be launched as a RemoteApp.

In a dynamic cloud environment, you can ensure that Windows computers return to compliance upon restart/re-introduction into your environment.

No doubt, you want your customers and employees to be able to access business resources and systems continually, and you cringe at the thought of any service disruption or downtime and all the headaches it entails. The automation or security tools you implement should deliver "always available" services. There are a number of features in Password Safe that can be implemented to enable this "always available" design.

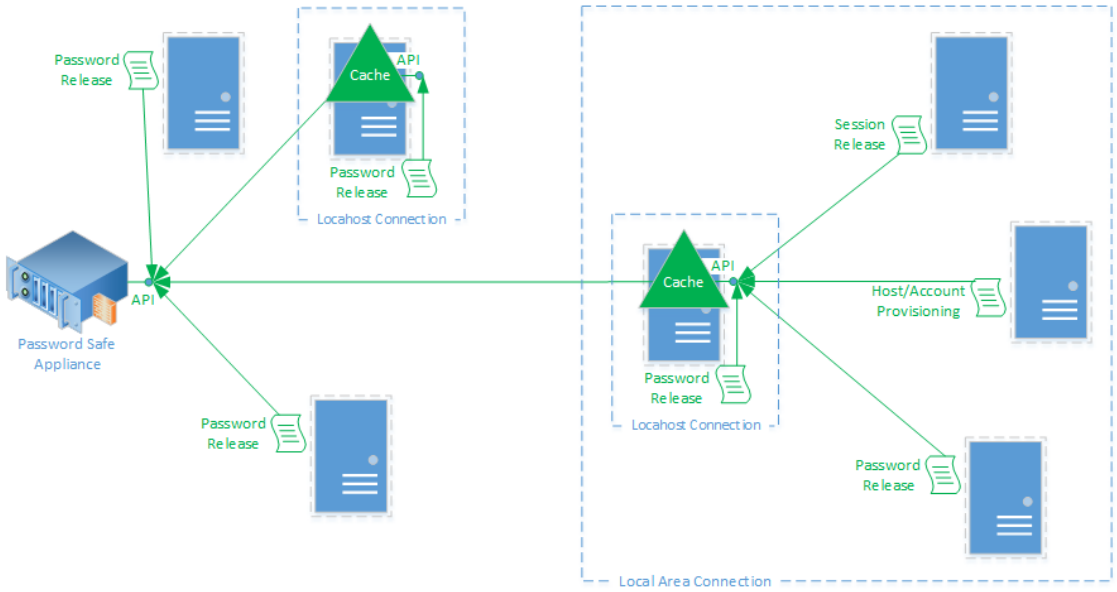


Figure 7: An unlimited number of Caches may be deployed in an environment to provide redundancy and low latency connection.

Caching

For high volume API requests, Password Safe's Password Cache utility allows credentials to be accessed directly on a local host (for close to zero latency), or from a local subnet. Using Password Safe, deploy an unlimited number of caches to distribute access to managed credentials to meet your scalability and redundancy needs.

In the event of a catastrophic system or network failure, these persistent caches will provide a failsafe mechanism to ensure that critical operations (including automated batch jobs) may continue.

Aliasing

When APIs are normally accessed in extremely high-volume applications, there is always a risk that a credential may be stale due to latency inherent in standard password change operations. Password Safe addresses this issue by creating aliases for API usage. Setup simply requires creating an account alias, which is then mapped to one or more managed accounts. In use, the 'alias API' will return both the currently active account name and password. When a password change is needed for the actively mapped account, the alias will automatically map to the next account in the list before a password change occurs. This ensures that credentials will only be returned for stable accounts that are not in the midst of a password change.

THE CHALLENGE - Managing Remote Applications

Passwords embedded within applications pose an oft-overlooked and undermanaged risk. Password Safe lets you bring these application passwords under complete management. Applications might have a database, a custom interface, or they might be a unique piece of technology that is custom to your organization.

Some password solutions require that you build a custom connector each time you want one of your applications to be managed, However, Password Safe leverages advanced technology within Microsoft Remote Desktop Services, which reduces complexity and improves availability.

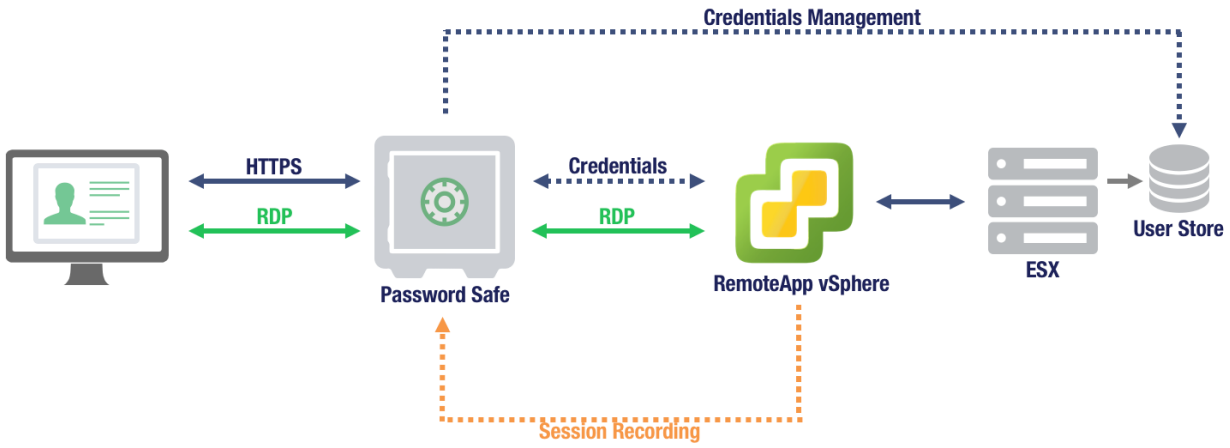


Figure 8: Privileged password management solutions can allow applications to be launched as a RemoteApp.

THE SOLUTION

From simple DBMS applications, such as SQL Server Management Studio, PL/SQL Dev or TOAD, to complicated web interfaces that require AutoIt scripts to play credentials in, Password Safe makes the process simple. Even file utilities such as FileZilla can be automatically launched. PowerBroker Password Safe allows any Windows application to be launched as a RemoteApp and delivered via the proxy with no password exposure to the end user. All activity is recorded and can be monitored in real-time with the ability to lock and terminate sessions.

Least Privilege

THE CHALLENGE - Leveraging Identity and Access Management Data for Privileged Access Decisions

As a best practice, organizations should ensure ongoing attestation of access to validate that those who have access to your critical infrastructure still need this access – as validated by an appropriate party. A comprehensive review should include both privileged and non-privileged access.

THE SOLUTION

PowerBroker Password Safe includes a dynamic, bi-directional certified integration with SailPoint IdentityIQ, allowing organizations to effectively manage user access for both privileged and non-privileged accounts.

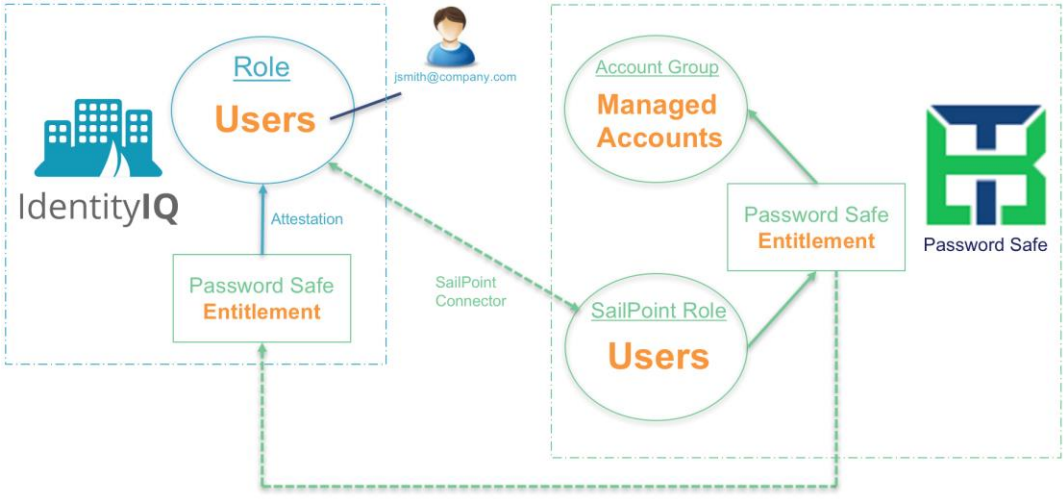


Figure 9: Direct API-based integration provides immediate provisioning of, and visibility into, all privileged access. Users may be granted immediate runtime access to Password Safe to request passwords or sessions for managed privileged accounts.

THE CHALLENGE – Granting Just-in-Time Privileges to Improve Workflow

While granting privileged access typically focuses on the ‘what’, many organizations also need a solution that addresses the ‘where,’ ‘when,’ and ‘how’.

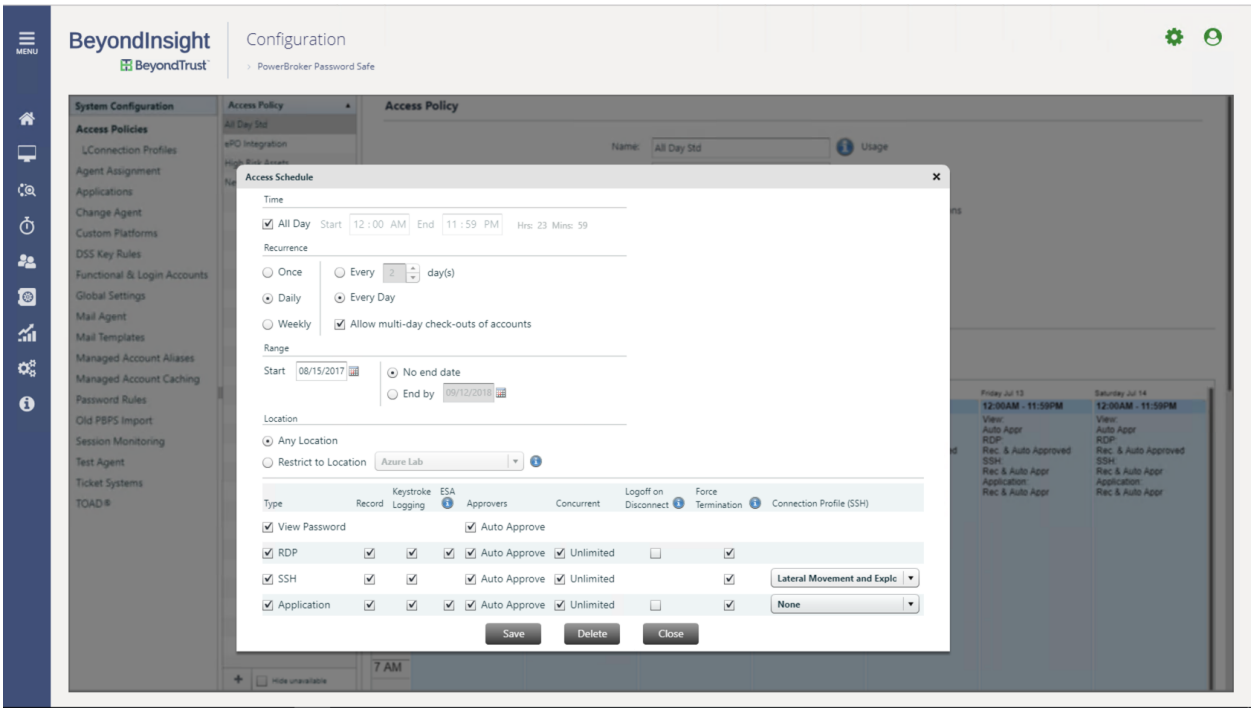


Figure 10: PowerBroker Password Safe utilizes adaptive workflow controls to help IT security teams manage access based on myriad criteria, such as location, date, and time.

THE SOLUTION

Adaptive workflow control in Password Safe allows you to control access based on context within multiple criteria. The workflow analyzes the day, the date, the time, who, what, and where at that particular session. PowerBroker Password Safe can also look at a particular date range and even a network address, allowing you to ask and act on questions such as, "Is this user authorized to come in and actually run this specific command, and from that location?"

THE CHALLENGE - Mitigating Privileged Access Risk in Cloud Environments

When assessing privileged access controls within your cloud environment, you should consider hosted applications (Software-as-a-Service), infrastructure deployments (Infrastructure-as-a-Service), and the management of users within these environments (Single Sign-On, Cloud Access Security Brokers).

Few organizations have migrated fully to non-local datacenter deployments; therefore, whenever you consider solutions to manage your environment, you should consider hybrid on-prem/cloud deployments that can easily manage credentials within your data center, as well as across your cloud deployments.

Some password solutions manage users directly, some manage entitlements of users within applications, and other solutions allow management of the administrative accounts that control the underlying foundation of your cloud products.

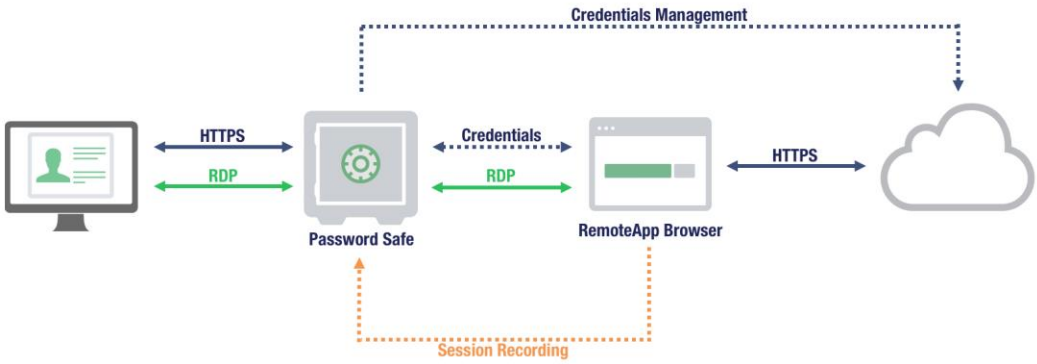


Figure 11: Store web credentials and auto-launch websites with zero password exposure to the end-user.

THE SOLUTION

PowerBroker Password safe can help you address a wide spectrum of use cases, allowing you to utilize a standard methodology across even the most sophisticated and heterogeneous cloud deployments. With Password Safe:

- Manage API Keys to access cloud-based automation services
- Control the SaaS credentials of administrative users
- Handle the SSH, API, and password credentials of users of machines deployed on private cloud or public cloud “virtual private clouds”
- Control access to the CASB Console (CASB Admin credentials)
- Manage passwords of automation accounts that are used for dynamic DevOps provisioning for solutions such as Puppet, Chef, and Ansible

- Utilize hybrid provisioning – manage the accounts over private VPN or any standard network connection to the server or service
- Control access passwords for use in CI/CD workflows
- Contain deployment workflow secrets with solutions such as Docker

THE CHALLENGE - Integrating Identity and Access Management with Privileged Access Management

Most organizations that implement Privileged Access Management (PAM) and Identity and Access Management (IAM) have done so independently, so they are likely missing out on some key values that could come from IAM-PAM integration. IAM adoption tends to get driven by the need to gain control over user access, permissions, and rights to address a security, compliance, or IT efficiency challenge. But IAM solutions only go so far. PAM solutions take security and compliance a step further by helping IT teams control privileged users and accounts, while also providing granular visibility into how identities are actually being used.

One common use case for an IAM solution is to provision identities into Active Directory (AD). The typical provisioning process includes, but is not limited to, populating attributes and adding provisioned accounts to AD group policy or security groups.

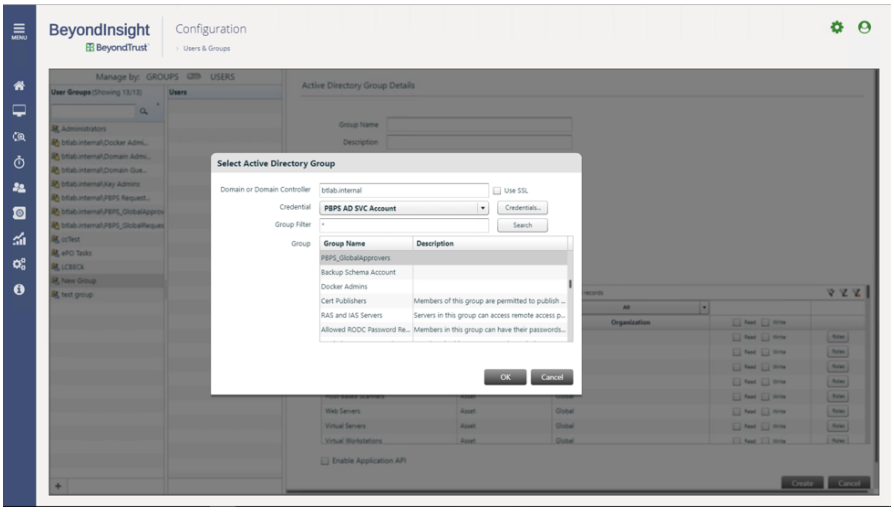


Figure 12. Active Directory / LDAP groups may be leveraged to apply granular entitlements to users

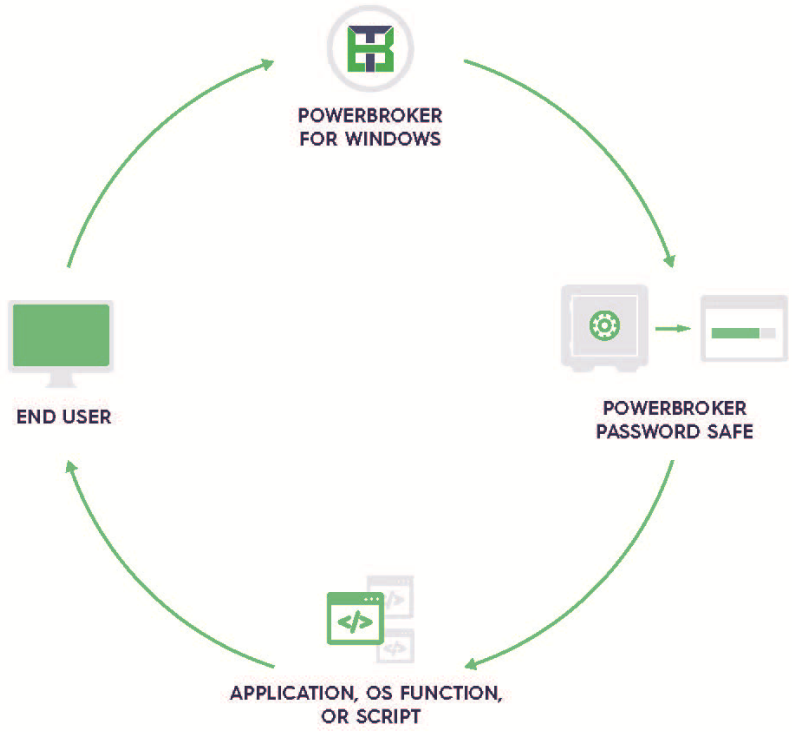
THE SOLUTION

Once an identity is provisioned based on an IAM policy, PowerBroker Password Safe seamlessly leverages those identities for privileged password and session access, while also enforcing least privileged controls. Password Safe provides granular insight into privileged account and entitlement access. When fed into an IAM solution, you get a holistic view of any individual's privileged and non-privileged access.

Policy Enforcement and Ongoing Administration

THE CHALLENGE - Improving Efficiency in Run-As Access to Applications

When using real credentials for an application (in an environment that has a password management solution), multiple user interfaces and mouse-clicks are often required to obtain the proper credentials, which is a less than optimal environment for end users.



How it works:

1. PowerBroker for Windows automatically calls PowerBroker Password Safe using a dedicated rule action.
2. Rules automatically match an application, OS function, or script to the proper credentials and execute them without the end user ever seeing the hostname, username, or password.

Benefits of this approach:

- Enhances security by using only credentials for targeted application
- Never exposes credentials to end user

Figure 13: With PowerBroker Password Safe and PowerBroker for Windows, the Network Administrators never need to see the credentials used to access network resources.

THE SOLUTION

PowerBroker Password Safe, when used with PowerBroker for Windows, can run applications using alternate credentials with minimal clicks and without exposing credentials to the user. This integration eliminates user frustration and maintains a high level of security for the company.

THE CHALLENGE - Utilizing Advanced Threat Analytics to Make Better Privileged Access Decisions

Traditional security analytics solutions struggle to correlate diverse data to discern hidden risks amidst all the noise. Seemingly isolated events are written off as exceptions, filtered out, or lost altogether in a sea of data, while an intruder continues to traverse the network, and damage mounts up.

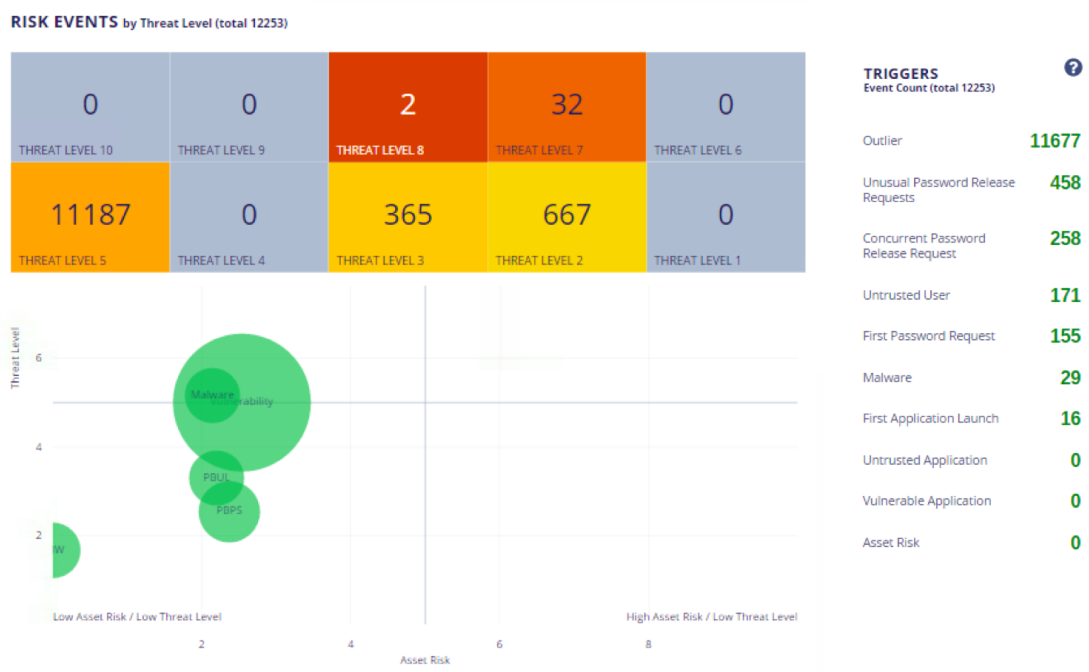


Figure 14: BeyondTrust Privileged Threat Analytics, available to PowerBroker Password Safe users, provides a clear view of security events from integrated BeyondTrust solutions, as well as external data feeds

THE SOLUTION

BeyondTrust provides the groundbreaking ability to apply risk and vulnerability intelligence to automatically halt access for high-risk privileged accounts, automatically rotate passwords that are considered compromised, and more.

Privileged Threat Analytics, a standard capability that comes with Password Safe, can pinpoint specific, high-risk users and assets by correlating low-level privilege, vulnerability, and threat data. It collects, correlates and analyzes user and asset activity data from several BeyondTrust and third-party solutions, including:

- PowerBroker Password Safe: privileged password and session activity
- PowerBroker for Windows: privileged user and account activity data from desktops and servers
- PowerBroker for Unix & Linux: privileged user and account activity from servers
- PowerBroker Endpoint Protection Platform: IPS, IDS, anti-virus, and firewall log data
- Retina CS Enterprise Vulnerability Management: vulnerability data
- Third-Party Vulnerability Scanners: imported data from Qualys, Tenable, and Rapid7

THE CHALLENGE - Promoting Transparency Using Agentless Privileged Session Monitoring

Who is watching the watchers? Monitoring of privileged sessions helps promote organizational transparency and provides IT administrators with the ability to view and, if necessary, interrupt a privileged session. Limiting access to servers by leveraging firewall rules, or by restricting "Log on Locally" rights through Windows, helps minimize password usage on servers.

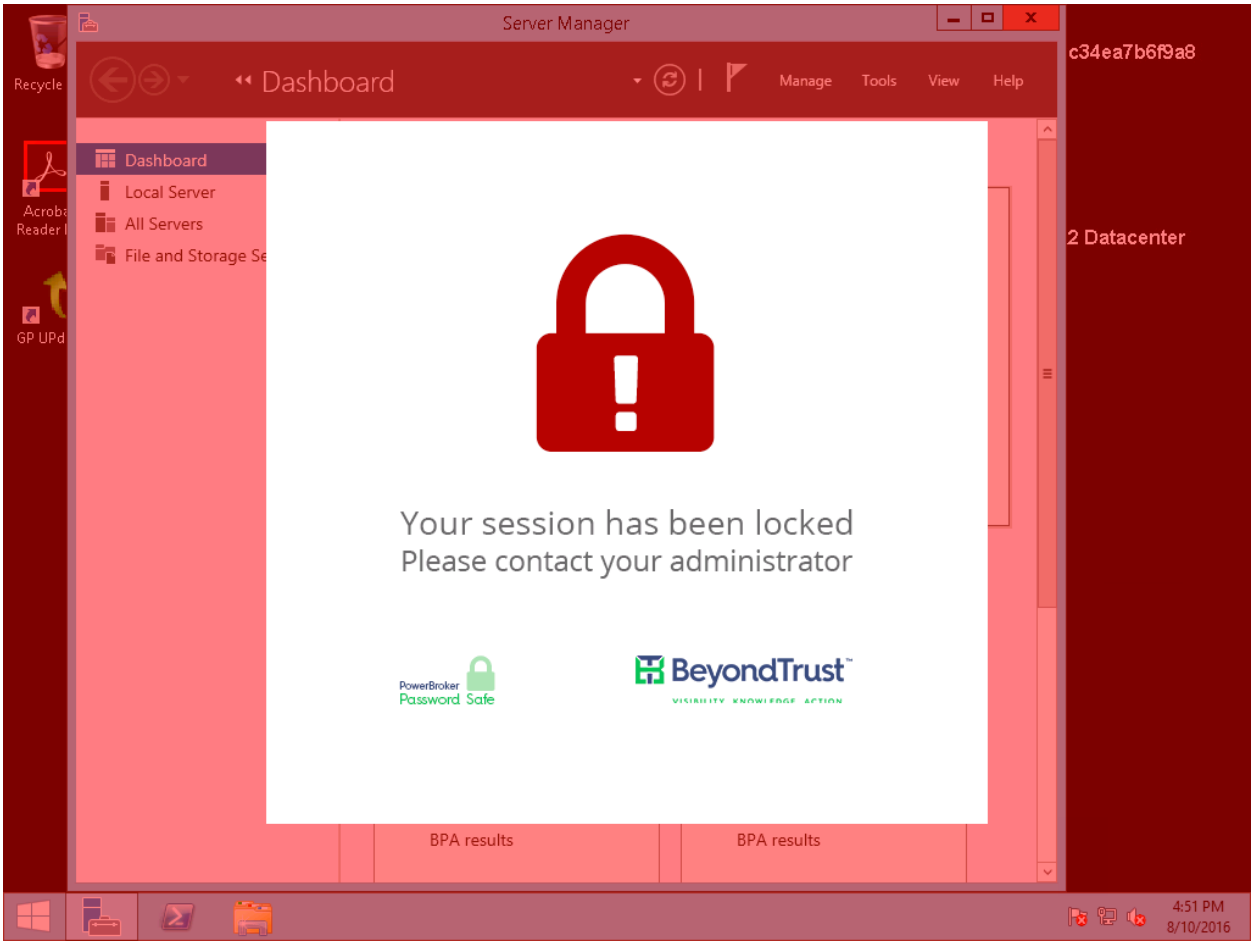


Figure 15: PowerBroker Password Safe includes live session management, enabling true dual control that, allows admins to investigate suspicious behavior without killing sessions – or productivity.

THE SOLUTION

PowerBroker Password Safe uses standard desktop tools, such as PuTTY and Microsoft Terminal Services Client, ensuring administrators can leverage common management tools - without the need for Java.

Recording privileged sessions is an important capability for IT to ensure the security and integrity of its sensitive information. Capturing this activity and referring back to it during audits, or in the event of a data breach, is absolutely critical. However, as you may be painfully aware, combing through hundreds of logs to pinpoint suspicious user activity is time-consuming and impractical. PowerBroker Password Safe helps make your job easier here with an enhanced session viewer that provides keystroke indexing with full text search capability.

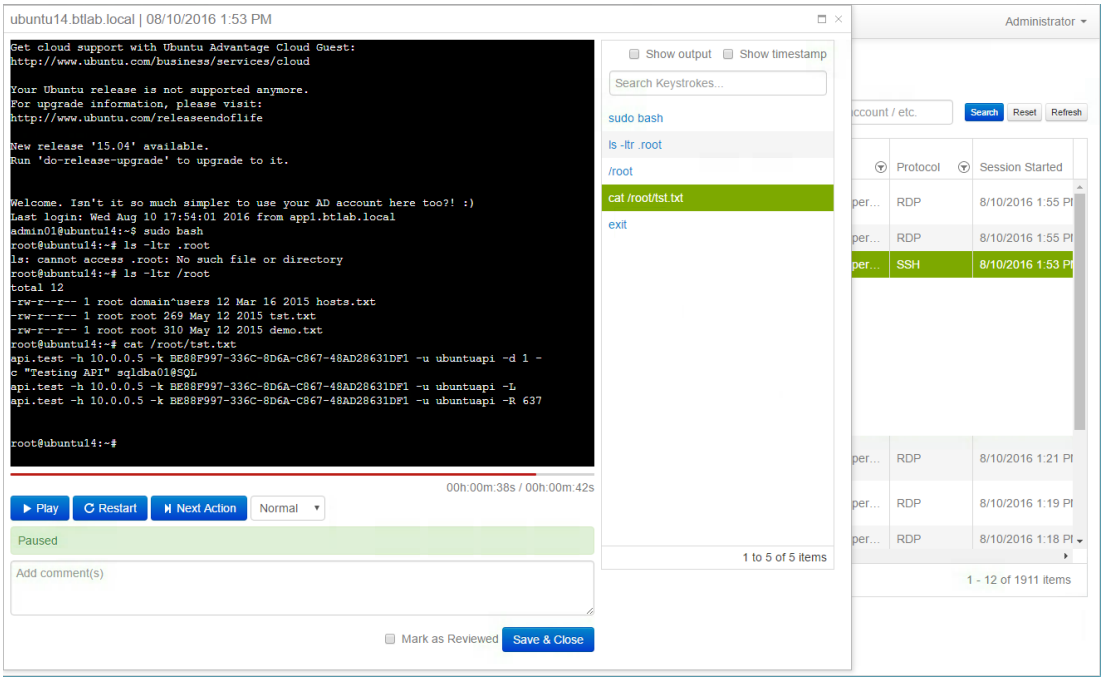


Figure 16: All user activity, whether it is command line-based, or GUI based, is presented in an easy to use replay tool.

Any RDP and SSH activity is automatically captured and displayed. For SSH sessions, both the input and output are indexed and searchable. When an index is clicked, the session immediately jumps to that section and starts playback. You can also instantly search for words that may have been typed, or text that has been displayed.

THE CHALLENGE – Managing assets and accounts without granting excessive privileged access

Most IT organizations do not have a systematic approach to managing assets or granting access to accounts. Without a method of grouping assets, they run the risk of missing accounts, or worse – granting too much access to certain users.

THE SOLUTION

With PowerBroker Password Safe, you can avoid that time-consuming work using Smart Rules. Using collected system details from the discovery process to automatically categorize assets, Smart Rules can be triggered to generate alerts or auto-provision managed assets (and even accounts) based on system categorization.

With Smart Rules, you can quickly identify assets with common traits and automatically place them under Password Safe management. This simpler, more automated approach saves time and helps prevent missed accounts.

Integration and Extensibility

THE CHALLENGE – Connecting to SSH Sessions Quickly and Efficiently

Connecting to a webpage to request access to an SSH session can be seen as an unnecessary step for administrators that primarily work within command line environments, especially when those sessions are generally auto-approved.

PowerBroker Password Safe version lets you automatically launch an SSH session by simply passing a connection string to the proxy. In this manner, you can choose to bookmark and store favorites directly in your SSH clients such as PuTTY, MobaXterm, Reflection etc.

For example: btlab\user@root@systemx@passwordsafeproxy

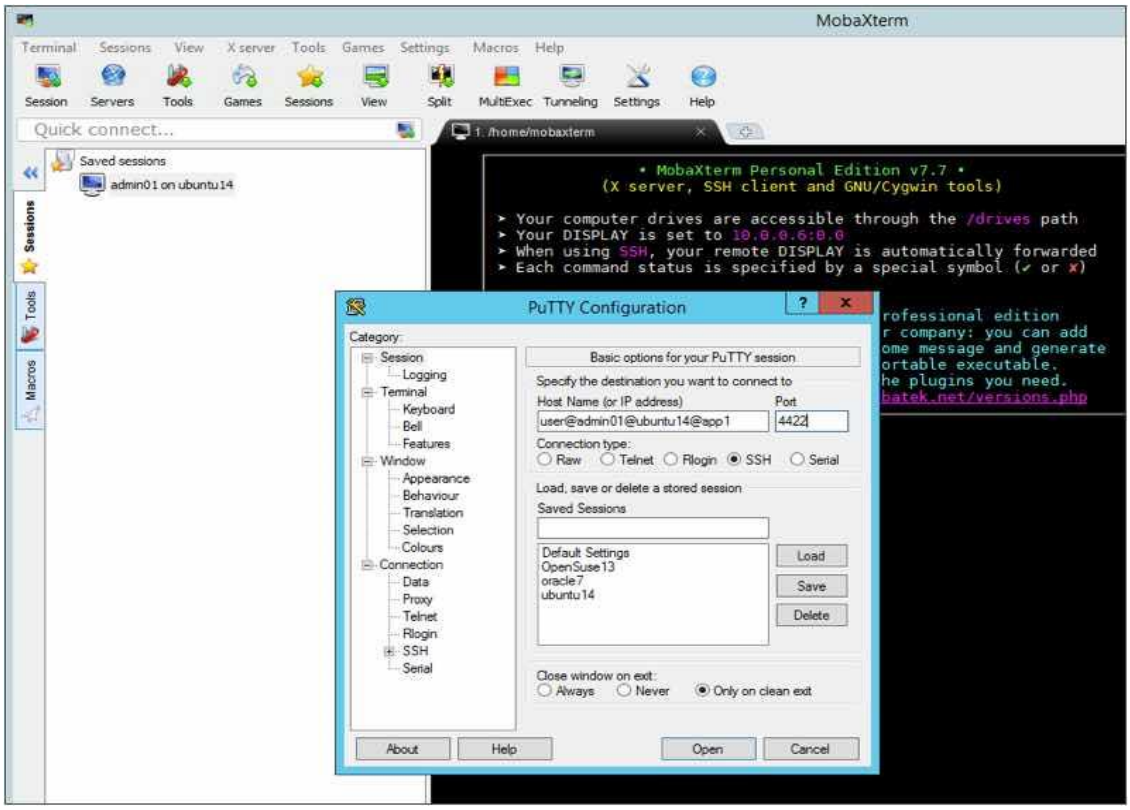


Figure 17: In this example, when passing the connection string to the Password Safe proxy, the user will be prompted for the password of their own account (btlab\user), then directly logged onto an SSH session running as root on systemx.

THE SOLUTION

PowerBroker Password Safe lets you automatically launch an SSH session by simply passing a connection string to the proxy. No agents need to be installed on the hosts, and connection to any SSH system is supported, including Unix/Linux hosts, and network devices such as routers or firewalls. Password Safe SSH DirectConnect allows sessions to be easily established via your existing desktop tools without having to initiate via a web interface.

THE CHALLENGE – Managing privileged passwords and privileged sessions through a single security console

When a data breach happens as a result of the misuse or abuse of excessive user privileges, the natural reaction for IT is to restrict the use of shared accounts, enhance endpoint protection, and remove administrator rights. But this approach often requires multiple tools that don't talk to one another.

THE SOLUTION

Integrating PowerBroker Password Safe with McAfee ePO will help overcome the complexity involved with making these changes and will enable cohesion within a single user interface to manage endpoint and privileged risks.

The integration helps McAfee ePO customers:

- Selectively rotate privileged passwords on assets directly from ePO.
- Launch an interactive session or retrieve privileged credentials for SSH or RDP as an ePO Action using native client tools
- Gain lifecycle management of privileged accounts from discovery through management, within ePO
- Identify whether a system is provisioned into PowerBroker and whether it is under Password Safe management
- Automatically push tags from ePO into Password Safe, enabling dynamic access control for managed accounts

Final Thoughts on Privileged Password & Session Management

With PowerBroker Password Safe, all of the privileged password management and privileged session management capabilities are included – no extra fees or extensive customization is needed. With Password safe, you can:

- Secure and automate the process for discovering, managing, and cycling privileged account passwords and SSH keys
- Control how people, services, applications, and scripts access credentials
- Auto-logon users onto RDP and SSH sessions, without revealing the passwords
- Record all user and administrator activity in a comprehensive audit trail
- Alert in real-time as passwords are released and privileged session activity is started

With PowerBroker Password Safe, IT organizations get a solution which is easy to use, quick to deploy, and offers a broad range of capabilities to address privileged password and privileged session management challenges.

Capabilities Checklist

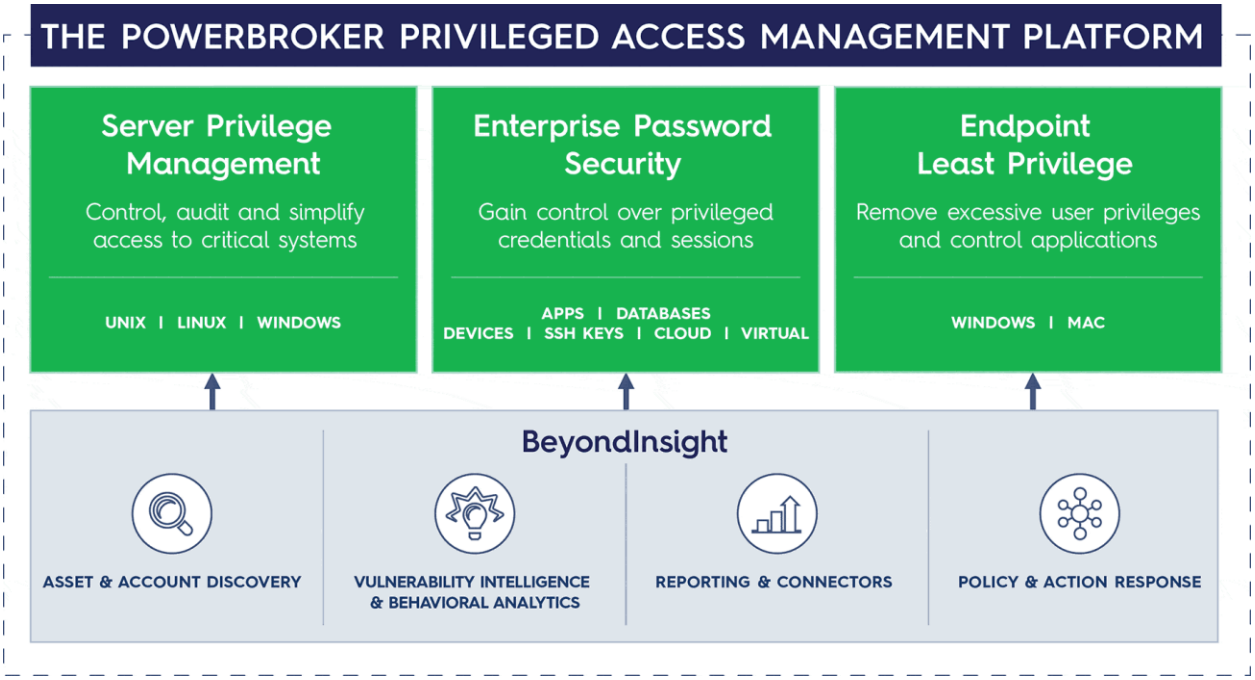
As you evaluate your organization's needs, it's important to ensure that the capabilities you need are included in your privileged password management solutions. Here's a checklist of capabilities included with PowerBroker Password Safe. Request a free trial.

PowerBroker Password Safe Key Capabilities	
Automated discovery and enforcement of privileges over new accounts, users, and assets	♦
Automated password management, including rotation of passwords	♦
Automated service account management	♦
Application to application (A2A) password management	♦
Adaptive workflow to control access based on any date, time, or location	♦
Simplified SSH Key management	♦
Privileged session management and recording	♦
Lock, terminate, or cancel sessions in real-time	♦
Agentless session management	♦
Support across on-premise, cloud, and hybrid environments	♦
On-premise, cloud, and hosted deployments	♦
Hundreds of reports out-of-the-box for usage analytics and compliance	♦
Scalable to millions of accounts and endpoints	♦
Helpdesk integration	♦

Centralized policy management	
Intelligent, vulnerability-based privileged access decision-making	
Supports industry-standard encryption algorithms	
Agentless, Web-based, with no reliance on Java	
Helps support password protection and audit regulations	
Break-glass support	
Password Caching and Account Aliasing	
Leverages role-based access controls	

About the PowerBroker Privileged Access Management Platform

PowerBroker Password Safe is part of BeyondTrust's solution for Enterprise Password Security and integrates seamlessly with other privileged access management solutions in the PowerBroker Privileged Access Management Platform. Analysts and users recognize PowerBroker as the most comprehensive, highly integrated solution for privilege access management. By uniting capabilities that many alternative providers offer as disjointed tools, PowerBroker simplifies deployments, reduces costs, improves system security and closes gaps to reduce privileged risks.



Free Tool: Privilege Discovery and Reporting Tool

Want to take the next step in assessing the state of your organizations privileged credentials? PowerBroker Privilege DART (Discovery and Reporting Tool is a free tool you may download to instantly assess the state of your organization's privileged accounts, users, and assets. It's a standalone executable that can be set up and run on any box in minutes, with no install required.

Use Privilege DART to:

- Uncover and profile all user and local accounts; SSH keys; and Windows and Linux groups
- Identify privileged passwords, including default and hard-coded passwords
- Assess password strength, age, and other key risk indicators
- Analyze credential, account, and asset metrics in a graphical dashboard
- Generate customizable reports on accounts, keys, and systems exposed to risk

About BeyondTrust

BeyondTrust® is a global cyber security company that believes preventing data breaches requires the right visibility to enable control over internal and external risks.

We give you the visibility to confidently reduce risks and the control to take proactive, informed action against data breach threats. And because threats can come from anywhere, we built a platform that unifies the most effective technologies for addressing both internal and external risk: Privileged Access Management and Vulnerability Management. Our solutions grow with your needs, making sure you maintain control no matter where your organization goes.

BeyondTrust's security solutions are trusted by over 4,000 customers worldwide, including over half of the Fortune 100. To learn more about BeyondTrust, please visit www.beyondtrust.com.