Securing VMware Infrastructure with PowerBroker Password Safe

Privileged Password Management and Privileged Session Management

BeyondTrust™
VISIBILITY. KNOWLEDGE. ACTION.

While the vast majority of VMware® administrators change default passwords, most credentials can be still guessed via brute-force attacks. Even strong, complex passwords may not be enough to prevent breaches. For instance, VMware environments are often put at risk when the same usernames and passwords are used across the infrastructure — or when passwords are infrequently changed. Once credentials are compromised, attackers can siphon sensitive data from the organization via custom malware and other malicious techniques.

FIVE COMMON SIGNS OF VMWARE ACCOUNT SECURITY RISKS

1. Default or common passwords are not configured correctly
2. Credentials are shared across multiple devices
3. Passwords remain unchanged for excessive periods of time
4. Privileged sessions are unmonitored
5. No accountability controls exist for outsourced VMware devices and infrastructure

Any of these scenarios can set your organization up for a serious data breach. Fortunately, there is a simple and effective way to secure your VMware infrastructure against account-based risks: privileged password management with PowerBroker® Password Safe.

AUTOMATED PRIVILEGED PASSWORD MANAGEMENT FOR VMWARE

PowerBroker Password Safe is an automated password and privileged session management solution offering secure access control, auditing, alerting and recording for any privileged account. Password Safe strengthens VMware security by:

- Ensuring no device has a default password for administrative accounts
- Guaranteeing each device has a unique complex password
- Automatically rotating passwords based on age and usage
- Limiting administrative access and communications to authorized individuals

Password Safe can secure privileged accounts across your enterprise environment, including:

- Local or domain shared administrator accounts
- Personal admin accounts (in the case of dual accounts)
- Service, operating system, network device, database (A2DB), & application (A2A) accounts
- SSH keys, cloud and social media accounts

Key Differentiators

NETWORK-BASED ASSET DISCOVERY

Scan, identify and profile all users and services; automatically onboard systems and accounts under management, speeding time to value.

DYNAMIC RULES & ASSET GROUPINGS

Build Smart Rules to trigger alerts or auto provision based on system categorization, speeding time to resolution.

SIMPLIFIED SSH KEY MANAGEMENT

Schedule SSH key rotation and enforce granular access control and workflow.

UNIFIED PASSWORD AND SESSION MANAGEMENT

Use a single solution for both password management and session management, lowering cost and complexity.

AGENTLESS SESSION MANAGEMENT

Utilize native tools including Microsoft® Remote Desktop and PuTTY to connect to systems without the need for Java.

APPLICATION PASSWORD MANAGEMENT

Get control over scripts, files, code and embedded keys by eliminating hard-coded or embedded credentials automatically.

ADVANCED WORKFLOW CONTROL

Add context to workflow requests by considering the day, date, time and location when a user accesses resources.

THREAT ANALYTICS & REPORTING

Leverage a central data warehouse to collect, correlate, trend and analyze key threat metrics; customize reports to meet specific needs.

The BeyondInsight platform for unified asset and user risk intelligence

PowerBroker Password Safe is part of the BeyondInsight™ IT Risk Management Platform, which unifies PowerBroker privileged account management solutions with Retina CS Enterprise Vulnerability Management. Capabilities include:

- Centralized solution management and control via common dashboards
- Asset discovery, profiling and grouping
- Reporting and analytics
- Workflow and ticketing
- Data sharing between Retina and PowerBroker solutions

The result is a fusion of user and asset intelligence that allows IT and security teams to collectively reduce risk across complex environments.

CONTACT

North America
Tel: 800.234.9072 or 480.405.9131
info@beyondtrust.com

EMEA
Tel: +44 (0)1133 970445
emeainfo@beyondtrust.com

APAC
Tel: +65 6701 8267
apacinfo@beyondtrust.com

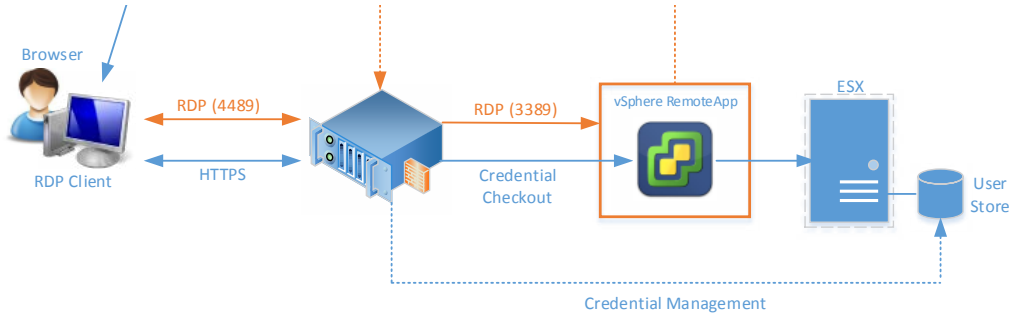
CONNECT

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

Securing VMware accounts with PowerBroker Password Safe

PowerBroker Password Safe enables you to secure VMware infrastructure with complete control and audit all privileged account access.

- Discover all VMware vCenter® and ESXi® devices, including on and offline images
- Verify that no default passwords exist on any hyper-visor or managed device
- Manage all VMware ESXi devices automatically using PowerBroker Smart Rules, and store a unique password for each device
- Automatically rotate each device's password based on age or after each administrator login
- Provide a complete workflow for device access, including an approval process for admin access
- Enable administrators to SSH to VMware ESXi without ever seeing the admin password
- Record and playback all privileged sessions to document and review device changes
- Record user activity in VMware vSphere® (video and keystrokes – October 2015)
- Report on all privileged credentials requested and used
- Detect abnormal device and credential access, and receive alerts, via patent-pending BeyondInsight® Clarity threat analytics



Extend VMware security with BeyondTrust least privilege solutions

BeyondTrust least privilege solutions, including PowerBroker for Unix & Linux and PowerBroker for Windows, enable you to further harden your VMware infrastructure. These solutions reduce the risk of privilege misuse, especially when third-party tools and other applications are required to manage VMware infrastructure. With PowerBroker, you can eliminate local admin privileges, enforce least-privilege policy, maintain application access control, and log privileged activities.

For more information on how BeyondTrust can help you meet your security and compliance requirements, please refer to these VMware Partner Addendum Guides:

PCI:
www.beyondtrust.com/Resources/Whitepaper/BeyondTrust-Coalfire-PCI-Solutions-Guide

HIPAA:
www.beyondtrust.com/Resources/Whitepaper/BeyondTrust-Coalfire-HIPAA-Solutions-Guide