# Bullet Proof Your Cisco Infrastructure

## Privileged Password Management and Privileged Session Management

BeyondTrust™
VISIBILITY. KNOWLEDGE. ACTION.

The most common user name and passwords for Cisco® devices are not necessarily the defaults that come with the device. Most administrators change them. Unfortunately, in most environments they can be guessed or compromised using brute force password attacks. In addition, the second most common privilege flaw is to use the same ones across the entire infrastructure and rarely, if ever, are they changed in mass even if you have outsourced the management. This problem can lead to a variety of malicious activities including recent vulnerabilities that can replace the device's bootstrap loader with a piece of custom malware.

While this vulnerability, the possible ex-filtration of data, and other flaws in privileges can lead to a compromise, there is a rather simple and effective way to secure your Cisco infrastructure from these flaws – privileged account and password management.

### THE RISKS CAN STEM FROM A SIMPLE LACK OF PRIVILEGED ACCOUNT MANAGEMENT ON CISCO DEVICES:

- Default or common passwords that are not configured correctly
- Shared credentials across multiple devices for management simplicity
- Excessive password ages due to fear of changing or lack of management capabilities
- Compromised or insider accounts making changes to allow ex filtration of data
- Outsourced devices and infrastructure where changes in personnel, contracts, and tools expose credentials to unaccountable individuals

Anyone of these could lead to excessive risk for your infrastructure. Therefore, the best way to mitigate them is to solve each one as a separate use case but solve them in a single, completely automated solution:

1. Ensure no device has a default password for administrative accounts
2. Guarantee each device has a unique complex password
3. Automatically rotate the passwords based on age and usage
4. Control admin access and even communications to only authorized individuals

## 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 automatically eliminated hard-coded or embedded credentials.

### 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


## PowerBroker Password Safe

With PowerBroker Password Safe, you can bullet proof your Cisco infrastructure with complete control and audit privileged accounts such as shared administrative accounts, application accounts, local administrative accounts, service accounts, database accounts, cloud and social media accounts, devices and SSH keys. PowerBroker Password Safe will enable you to:

- Discover all Cisco devices and verify that no default passwords exist on any device
- Manage all Cisco devices automatically using Smart Rules and store a unique password per each device
- Automatically rotate each device's password based on age or after each login by an administrator occurs
- Provide a complete workflow for device access including an approval process for when administrative access is required
- Record all privileged sessions with playback to document and review what occurs when a device is accessed
- Provide detailed reporting of credentials used and requested when all privileged activity occurs
- Deliver patent-pending analytics for abnormal device and credential access in a wide variety of available reports

In addition, BeyondTrust can provide additional hardening for your Cisco infrastructure by using least privilege tools like PowerBroker for Unix & Linux and PowerBroker for Windows. When additional solutions (including 3rd party applications) are required to manage your Cisco infrastructure, whether they are command line based or have a graphical user interface, PowerBroker can perform least privilege operations with these applications, and reduce the risk by only granting standard user privileges to the administrator.