Server Privilege Management

PowerBroker Privileged Access Management Solution

BeyondTrust®
VISIBILITY. KNOWLEDGE. ACTION.

An Integrated Approach to Server Privilege Management

Lack of control over root or admin passwords, super-user status, or elevated privileges could lead to a damaging breach or audit violation. Although least-privilege enforcement on Tier-1 Windows, Unix and Linux servers is critical, IT leaders are usually unable to control what users can do after authenticating into a server. Traditional solutions are not integrated, requiring a password storage tool to manage access and a separate sudo or least-privilege delegation tool for policy enforcement. This approach is inefficient, complex and expensive – plus it lacks behavioral analysis to identify security anomalies. Only BeyondTrust delivers a truly integrated approach to server privilege management.

Secure Privileged Access to Unix, Linux and Windows Servers

The BeyondTrust PowerBroker Server Privilege Management solution enables IT organizations to define who can access Unix, Linux and Windows servers – and what they can do with that access – via fine-grained policy control. Delivered as an integrated solution, PowerBroker enables organizations to improve security across all servers while simplifying deployments and reducing costs.

> "PowerBroker is easy to manage, we are more secure, and we are fully compliant."
>
> — IT Systems Analyst, Rogers Communications

Solution Overview

KEY CAPABILITIES

- Delegate Unix, Linux, and Windows privileges without disclosing root or admin passwords
- Automatically store, rotate and monitor privileged passwords & SSH keys
- Monitor sessions and log keystrokes for full audit accountability
- Bridge Unix and Linux to Active Directory for simplified single sign-on
- Report on password, user and account behavior

INCLUDED PRODUCTS

PowerBroker for Unix & Linux

Control and audit Unix and Linux root account privileges with centralized management, analytics, reporting, and keystroke logging.

PowerBroker for Windows

Eliminate administrator privileges on physical and virtual Windows servers; grant privileges to applications, not users.

PowerBroker Identity Services

Extend Active Directory authentication & single sign-on to Unix, Linux and Mac.

PowerBroker Password Safe

Discover, manage and monitor any privileged account – admin, service, OS, device, database, application, SSH keys, and cloud and social media accounts.
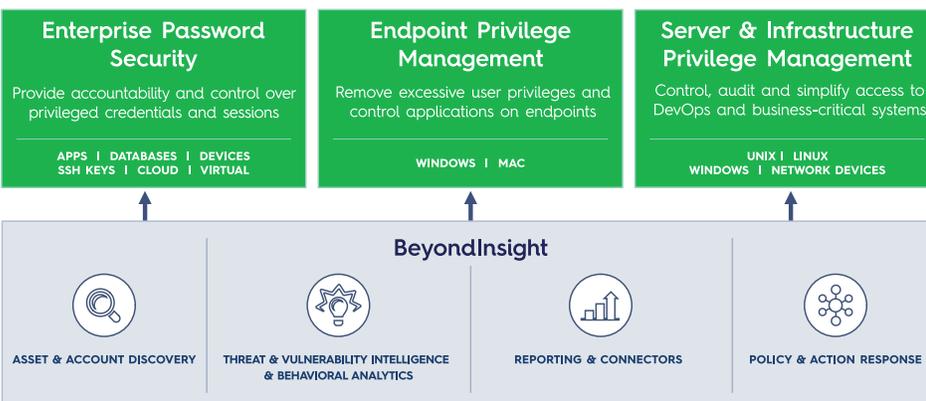
Retina CS

Perform large-scale, cross-platform vulnerability assessment and remediation, with configuration compliance, patch management and compliance reporting.

PowerBroker Platform

Centralized capabilites include: asset and account discovery; threat and vulnerability intelligence and behavioral analytics; reporting and connectors; and policy and action response.

THE POWERBROKER PRIVILEGED ACCESS MANAGEMENT PLATFORM

Enterprise Password Security
Provide accountability and control over privileged credentials and sessions
APPS | DATABASES | DEVICES SSH KEYS | CLOUD | VIRTUAL

Endpoint Privilege Management
Remove excessive user privileges and control applications on endpoints
WINDOWS | MAC

Server & Infrastructure Privilege Management
Control, audit and simplify access to DevOps and business-critical systems
UNIX | LINUX WINDOWS | NETWORK DEVICES

BeyondInsight

ASSET & ACCOUNT DISCOVERY | THREAT & VULNERABILITY INTELLIGENCE & BEHAVIORAL ANALYTICS | REPORTING & CONNECTORS | POLICY & ACTION RESPONSE

The BeyondTrust Server Privilege Management solution is part of the PowerBroker Privileged Access Management platform, which provides visibility and control over all privileged users and accounts in your organization.

Your Ally Against Privilege Misuse and Abuse

BeyondTrust is a global cyber security company dedicated to proactively eliminating data breaches from insider privilege abuse and external hacking attacks. Corporate and government organizations rely on BeyondTrust solutions to shrink attack surfaces and identify imminent threats.

The company's integrated risk intelligence platform presents a unique competitive advantage in its ability to reveal critical risks hidden within volumes of user and system data. This unifies IT and security departments, empowering them with the information and control they need to jointly prevent breaches, maintain compliance, and ensure business continuity.

BeyondTrust's privileged access management and vulnerability management solutions are trusted by over 4,000 customers worldwide, including over half the Fortune 100.

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

LATAM
latam@beyondtrust.com

CONNECT

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

Key Features

CONTROL AND AUDIT USER ACTIVITY

Reduce attack surfaces by combining privileged user auditing with onboard password storage and management. When a user checks out a password to invoke a command, fine-grained policy controls limit the security exposure.

BRIDGE UNIX & LINUX TO ACTIVE DIRECTORY

Manage heterogeneous server environments by bridging Unix and Linux systems into Active Directory for simplified authentication and greater visibility over user activity.

REVEAL PRIVILEGED APPLICATION AND ASSET SECURITY

Leverage vulnerability data from Retina and other solutions for a complete picture of privileged application and asset security. No assets are left unprotected, and privilege decisions are made with asset security in mind.

UNDERSTAND PASSWORD, USER AND ACCOUNT BEHAVIOR

Analyze privileged password, user and account behavior, and assign event Threat Levels based on the user, asset, and application launched. This makes it easier to uncover emerging risks, pinpoint and report on at-risk systems, and take action to proactively eliminate the threat.

SIMPLIFY DEPLOYMENTS WITH A SINGLE PLATFORM

Centrally control privileged access management policies and deployment, and report to multiple stakeholders. PowerBroker simplifies deployments, helps to control costs, and provides a foundation to reduce the evolving risks of privileged access.