PowerBroker for Windows Servers

Privilege and Session Management for Microsoft Windows

BeyondTrust
VISIBILITY. KNOWLEDGE. ACTION.

The case for Windows privilege management is overwhelming. Consider the fact that 94% of critical vulnerabilities reported by Microsoft in 2016 could have been mitigated by removing administrator rights. Whether hijacked by external attackers using phishing or ransomware, or simply misused by insiders, inappropriate access to local and domain admin rights can facilitate devastating data breaches. These privileges are prized by attackers because they can afford freedom of movement and access beneath the radar of detection.

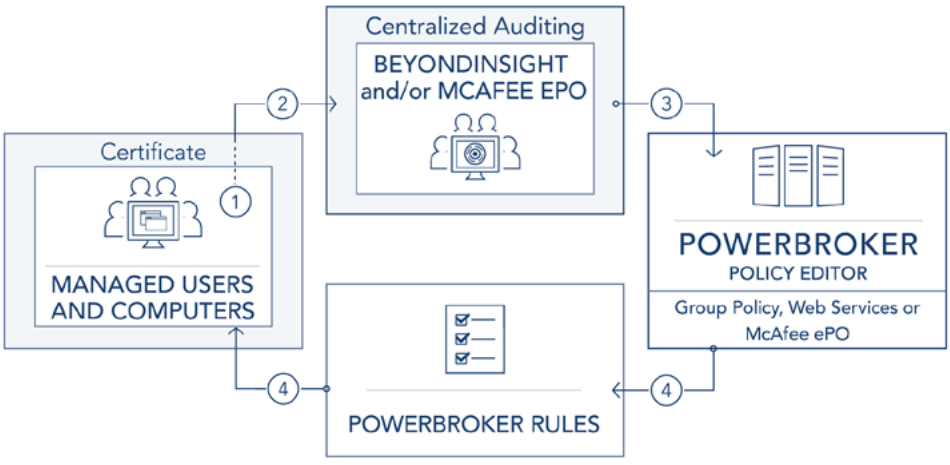
So how do you protect critical Windows servers, prevent and contain data breaches, and eliminate compliance violations stemming from excessive end-user privileges – without obstructing productivity or overburdening your Help Desk?

Comprehensive Privilege Management for Windows Servers

BeyondTrust® PowerBroker® for Windows is a privilege management solution that gives you unmatched visibility and control over physical and virtual Microsoft servers.

- **Reduce attack surfaces** by removing admin rights from end users and employing fine-grained policy controls for all privileged access, without disrupting productivity.
- **Monitor and audit sessions and user activity** for unauthorized access and/or changes to files and directories.
- **Analyze behavior** to detect suspicious user, account and asset activity.

> "With PowerBroker for Windows I could navigate and discover assets, identify vulnerabilities, and most importantly lock down all applications to implement least privilege and remove all admin rights from users' PCs."
>
> — Michael Romious, Sr. Network Systems Admin, FFVA Mutual Insurance



PowerBroker for Windows enables closed-loop least privilege policy enforcement.

Key Capabilities

AUDITING & GOVERNANCE

Analyze user behavior by collecting, securely storing and indexing keystroke logs, session recordings and other privileged events.

COMPREHENSIVE LEAST PRIVILEGE

Elevate privileges for standard users on Windows through fine-grained policy-based controls.

DYNAMIC ACCESS POLICY

Utilize factors such as time, day, location and application/ asset vulnerability status to make privilege elevation decisions.

REMOTE SYSTEM & APPLICATION CONTROL

Enable users to run specific commands and conduct remote sessions based on rules without having to log on as admin. When combined with integrated privileged password management, elevated applications can be launched without exposing the password.

FILE & POLICY INTEGRITY MONITORING

Audit and report on changes to critical policy, system, application and data files.

PRIVILEGED THREAT ANALYTICS

Correlate user behavior against asset vulnerability data and security intelligence from best-of-breed security solutions.

The PowerBroker Privileged Access Management Platform

PowerBroker for Windows is part of the BeyondTrust PowerBroker Privileged Access Management Platform, which delivers visibility and control over all privileged accounts, users and assets. The platform integrates a comprehensive set of PAM capabilities to simplify deployments, reduce costs, improve system security, and reduce privilege-related risks. PowerBroker solutions include:

- **Enterprise Password Security:** Provide accountability and control over privileged credentials and sessions.
- **Server Privilege Management:** Control, audit, and simplify access to business critical systems.
- **Endpoint Least Privilege:** Remove excessive user privileges and control applications on endpoints.

CONTACT

North America
info@beyondtrust.com

EMEA
emeainfo@beyondtrust.com

APAC
apacinfo@beyondtrust.com

LATAM
latam@beyondtrust.com

CONNECT

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

Key Features

PRIVILEGE MANAGEMENT FOR WINDOWS SERVERS

- **Eliminate admin rights:** prevent abuse or misuse of privileges on Windows asset
- **Allow admin where needed:** proactively identify applications and tasks that require administrator privileges — and automatically generate rules for privilege elevation

REPORTING & ANALYTICS

- **Ensure compliance:** meet internal and external compliance needs by enforcing least-privilege and monitoring privileged activities
- **Track and prevent lateral movement:** utilize rules to track and prevent anomalous user activity based on user roles and targeted resources
- **Pinpoint suspicious activity:** monitor Windows Event Logs for anomalies and analyze through BeyondInsight Behavioral Analytics
- **Protect file systems:** add optional file integrity monitoring to identify, and even deny, unauthorized changes
- **Record sessions:** add optional session monitoring to capture screens of privileged user activity with keystroke logging to document all privileged changes to an asset
- **Understand and communicate risk:** leverage an interactive reporting and analytics console with a centralized data warehouse for ongoing audits

GRANULAR APPLICATION RISK MANAGEMENT

- **Application application usage:** blacklist hacking tools, whitelist approved applications, and greylist applications based on rules to keep systems safe
- **Block suspicious activity:** enforce restrictions on software installation, usage, and OS configuration changes
- **Leverage Vulnerability-Based Application Management:** scan apps at runtime and allow, deny or alter privileges based on vulnerability severity, age and/or violations
- **Elevate applications:** elevate application as logged on or another user, without exposing credentials
- **Quarantine files:** leverage threat analytics for malware confidence reporting, enabling better risk decision-making
- **Simplify application management:** rules-based approach eliminates the need to manage complex whitelists for complete application control

MAXIMUM EFFICIENCY

- **Gain control over all accounts:** automatically discover and profile all Windows accounts, and quickly bring them under centralized management
- **Support one-time-passwords (OTPs):** support any multi-factor solution that utilizes the RADIUS protocol for additional verification that the user is the intended recipient
- **Ease policy creation/management:** set policies via AD Group Policy, BeyondInsight or McAfee ePO, with support for air-gapped systems and non-domain assets