Table of Contents

Introduction ........................................................................................................................................... 4
Least-Privilege Objectives .................................................................................................................. 4
Least-Privilege Implementations ....................................................................................................... 4
Sample Regulatory Requirements ........................................................................................................ 9
Conclusion ........................................................................................................................................ 13
About BeyondTrust ............................................................................................................................ 14
This document contains information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of BeyondTrust.

**Warranty**
This document is supplied on an "as is" basis with no warranty and no support.

**Limitations of Liability**
In no event shall BeyondTrust be liable for errors contained herein or for any direct, indirect, special, incidental or consequential damages (including lost profit or lost data) whether based on warranty, contract, tort, or any other legal theory in connection with the furnishing, performance, or use of this material.

The information contained in this document is subject to change without notice.

No trademark, copyright, or patent licenses are expressly or implicitly granted (herein) with this white paper.

For the latest updates to this document, please visit:
http://www.beyondtrust.com

**Disclaimer**
All brand names and product names used in this document are trademarks, registered trademarks, or trade names of their respective holders. BeyondTrust is not associated with any other vendors or products mentioned in this document.
Introduction

PowerBroker® for Windows provides fine-grained, policy-based privileged delegation capabilities for the Microsoft® Windows environment. The solution allows organizations to remove local admin rights from end users and server administrators without hampering productivity. PowerBroker selectively elevates privileges for applications, software installs, system tasks, scripts, control panel applets, management functions, and other application and system operations. Additionally, PowerBroker for Windows provides Session Monitoring, Risk Compliance, and File Integrity Monitoring capabilities for granular tracking of privileged user activity across Windows’ desktop and server environments.

Least-Privilege Objectives

The concept of least privilege states that asset users should have the lowest level of access privileges required to effectively conduct their jobs. However, many basic operating system, management, application and software functions (e.g., configuration utilities) require more than basic privileges. This traditionally requires end user to possess elevated privileges in the form of an administrative username and password. PowerBroker for Windows mitigates the need to distribute and maintain administrative credentials – or reveal these credentials to end users at all.

Administrative tasks, even in modern versions of Windows, are not limited to either servers or desktops. Common tasks like user administration, software updates, and operating system and application maintenance can be broken out for desktops and servers by common use case. For example, an administrator on a server may need access to Microsoft SQL Server Management Studio to perform maintenance, and a desktop user may need access to ODBC to setup a connection to a new or test database. While both cases require providing distributed access to a client/server database, the least-privilege permissions required for each are distinctly different. These examples, and many others, provide the context for this document.

Least-Privilege Implementations

PowerBroker for Windows is most commonly used for managing Windows desktop privileges, as desktop users are generally not considered trusted administrators with elevated privileges. However,
the need to secure privileged accounts on servers is escalating in response to recent security breaches at the U.S. National Security Agency (NSA), major retailers, and other organizations.

Rules for removing administrative privileges from end users can easily be translated back to servers once the complete use case for a rule is mapped out. For example, creating a rule to allow Java to automatically update on a desktop can easily be mapped to a server application or website that provides content for the end-user application. The transition to implementing least privilege from desktops to servers, or from servers to desktops, starts with gaining an understanding of what job functions must be accomplished.

DESKTOP IMPLEMENTATIONS

Operating within the BeyondInsight IT Risk Management Platform, PowerBroker for Windows provides a unique set of tools to help identify which applications require administrative access. For instance, administrators can select events directly within the BeyondInsight Management Console and seamlessly create PowerBroker rules that provide proper permissions to end users and applications without any end user intervention or interruption to their workflow. Use cases for these rules generally fall into very simple categories:

- Operating system tasks that require administrative access, such as time and date or ODBC
- Application installation and automated application updates, such as Java®, Adobe®, VMware®, etc.
- Applications that require administrative access, such as AutoCad®, VMware workstation configuration utilities, or Internet Explorer browser plugins for tools like Salesforce.com®.

PowerBroker for Windows also includes a sample rules library that simplifies rule creation by providing samples and best practices for a typical implementation.

This type of implementation provides the foundation for the vast majority of least-privilege implementations and provides the structured server implementation guidance required by many organizations.

SERVER IMPLEMENTATIONS

When implemented on servers, PowerBroker for Windows is structured around use cases related to which administrative functions are required to maintain the server and fulfill its mission. This is much more straightforward than a desktop implementation since servers generally have targeted roles, and server applications and users are normally less diverse. For example, the vast majority of operating system functions are contained within Microsoft Management Console (MMC). PowerBroker for Windows users can create rules for individual tasks within MMC or a single rule for the entire utility. To ensure that privileges are not abused, PowerBroker for Windows can perform scan capture recordings of the session to document that no malicious activity occurred. The solution can also track file system changes using File Integrity Monitoring to determine if the system has been inappropriately modified.

You can identify server use cases via two distinct philosophies:

1. Using documentation already present within an organization for a server’s role. Such documentation is frequently available as a result of regulatory standards, such as PCI DSS,
which requires determination of which administrative tasks commonly occur, and by whom. Once established, rules and policies can easily be implemented on servers using either passive monitoring in PowerBroker for Windows, in a lab, or through change control.

2. Reverse engineer desktop use cases. While this may sound like a monumental task, it is generally not that difficult with a desktop implementation of PowerBroker for Windows.
   a. First, consider all the administrative tasks on a server that are not locally application-based. These are utilities used to configure a remote system via an installed application. These are typically programs like Altiris® and IBM BigFix® that need administrative authority to execute but rely on other permission models for administration.
   b. Identify which users and systems are being accessed based on reports in the BeyondInsight management console.
   c. Finally, identify which application and operating system functions must be executed directly on the servers rather than via remote clients, such as MMC.

It is important to note that administrative access to servers can never be fully removed from any environment. PowerBroker for Windows enables day-to-day operations and common periodic tasks. Administrative access for disaster recovery, server creation, forensics, etc. continue to require administrative authority until suitable security technologies are developed to mitigate these advanced tasks. To address these and similar cases, BeyondTrust provides PowerBroker Password Safe to vault administrative passwords to these systems with full change control and auditing.

PRIVILEGED USE CASES

Day-to-Day Administrator Access

In the vast majority of organizations, there are typically many system administrators and help desk analysts requiring daily access to servers and workstations. PowerBroker for Windows strengthens security via privileged account management, while also improving user experience – for example:

- **Help Desks**: PowerBroker for Windows can facilitate help desk support tasks requiring privileged access to end-user workstations for troubleshooting and support. Help desk analysts can directly connect to end users’ machines via RDP or various remote access tools (DameWare, VNC, etc.) to assist with support tickets. Analysts can potentially be logged into one or more machines simultaneously, and should have access to these machines without needing any approvals.

- **Server Admins**: PowerBroker for Windows can provide controlled administrative access to servers and monitor this access to maintain accountability. Server admins are often logged into multiple servers concurrently and continuously for several days depending on tasks. Interactive use cases include logging into the servers directly, in person, remotely using single or multi-hop RDP jump servers, Citrix® connections, SSH, Vmware Console, and/or via scripts (DOS batch / or shell scripts, VBscripts, Powershell, etc). Admins often perform the tasks using “RUN-AS” or “SUDO” and may require multiplatform support for UNIX and Linux using the
same credentials (Note: BeyondTrust also offers solutions for least-privilege access on UNIX, Linus and Mac platforms.)

**Administrator Accounts and Shared Accounts**

Many organizations typically have several legacy administrative accounts used on multiple servers and workstations for service accounts and local backdoors. Security and compliance issues can stem not only from the laborious processes required to manage these accounts and change their passwords, but also from the lack of a privileged account inventory.

Managing privileged accounts with PowerBroker for Windows mitigates the risk of administrative account abuse, increases security, and eases administrative burdens. The solution also includes auto-discovery capabilities that identify privileged accounts and audit their usage across all computers reachable on the network.

Shared accounts are sometimes needed, such as when an application does not offer role-based access or when security controls do not allow for delegation of responsibilities. When shared accounts cannot be avoided, PowerBroker for Windows can strictly control permissions to the least privilege needed and log all access via features including keystroke logging and screen captures.

**Workflow Management**

PowerBroker for Windows includes robust workflow management capabilities that enable you to define:

- Workflows for alerting and automated ticket creation when specific, and potentially sensitive applications are launched.
- Workflows in response to suspicious privileged activities, such as the unauthorized creation of local user accounts or changes in a system’s certificates.
- Workflows when vulnerable applications are launched and given administrative privileges that could introduce risk to the host or violate regulatory compliance initiatives.

**Operational Continuity and Disaster Recovery**

Because privileged accounts are sensitive by nature, privileged account management solutions are usually considered to be mission-critical within the organization. Privileged account management solutions should therefore be extremely robust, resilient, and secure, without a single point of failure. In the case of PowerBroker for Windows, policies are distributed via Active Directory, agents utilize store and forward technology when no manager is present, and database architectures support high availability such as clusters and fault-tolerant appliances.

**Compliance Logging, Tracking and Auditing**

One of the most important requirements for any privileged management solution is its ability to log and track all activities that occur when access rules are triggered. PowerBroker for Windows logs privileged account activities in a secure manner and provides tamper-proof audit trails. The solution can also forward logs to an external SIEM system via multiple integration techniques.

PowerBroker for Windows audits and logs the following events:
• Application launches
• Events matching user-defined rules
• Windows event logs
• Applications that have inherent risks (like vulnerabilities)
• Unauthorized File System changes

The solution can also:

• Perform screen captures when applications are executed
• Identify where local accounts exist and when unauthorized new accounts are created
• Track activities associated with the account down to each keystroke and allow searching and sorting on these events
Sample Regulatory Requirements

PowerBroker for Windows enables customers to remove administrative access for users and administrators without impeding their ability to successfully perform their job functions. Security best practices, as well as SOX, PCI DSS and other regulatory compliance initiatives, mandate this form of privileged account management. This section describes how PowerBroker for Windows can be used for PCI DSS compliance initiatives across servers and desktops.

The PCI Security Standards Council (SSC) was established in 2006 by five global payment brands: American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa. The payment brands require through their Operating Regulations that any merchant or service provider must be PCI compliant. Merchants and service providers are required to validate their compliance by assessing their environment against nearly 300 specific test controls outlined in the PCI Data Security Standards (DSS). Failure to meet PCI requirements may lead to fines, penalties, or inability to process credit cards – in addition to potential reputational loss.

The PCI DSS spans six categories with twelve total requirements as outlined below:

<table>
<thead>
<tr>
<th>PCI Data Security Standard – High Level Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Build and Maintain a Secure Network</strong></td>
</tr>
<tr>
<td>1. Install and maintain a firewall configuration to protect cardholder data</td>
</tr>
<tr>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters</td>
</tr>
</tbody>
</table>

| **Protect Cardholder Data**                     |
| 3. Protect stored cardholder data |
| 4. Encrypt transmission of cardholder data across open, public networks |

| **Maintain a Vulnerability Management Program** |
| 5. Use and regularly update anti-virus software or programs |
| 6. Develop and maintain secure systems and applications |

| **Implement Strong Access Control Measures**    |
| 7. Restrict access to cardholder data by business need to know |
| 8. Assign a unique ID to each person with computer access |
| 9. Restrict physical access to cardholder data |

| **Regularly Monitor and Test Networks**         |
| 10. Track and monitor all access to network resources and cardholder data |
| 11. Regularly test security systems and processes |

| **Maintain an Information Security Policy**     |
| 12. Maintain a policy that addresses information security for all personnel |

The following matrix maps PowerBroker for Windows capabilities to the PCI DSS controls. PowerBroker for Windows enables organizations to significantly improve desktop and server security by making it easy to remove administrator privileges from users without impacting productivity.
## PCI DSS V2.0 Applicability Matrix

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Controls Addressed</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Requirement 4:** Encrypt transmission of cardholder data across open, public networks | 4.1.b, 4.1.d | PowerBroker for Windows meets or augments the following specific controls:  
- PowerBroker for Windows directly supports testing procedure 4.1.b by implementing certificate-based SSL V3 encrypted transmission between PowerBroker for Windows and the management console. Any transmission will fail if an incorrect certificate is used.  
- PowerBroker for Windows directly supports testing procedure 4.1.d by using RSA 1024-bit encryption strength for when transmitting between PowerBroker for Windows and the management console. |
| **Requirement 7:** Restrict access to cardholder data by business need to know | 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2 | PowerBroker for Windows meets or augments the following specific controls:  
- PowerBroker for Windows directly supports testing procedure 7.1.1 because the concept of least privilege is the very nature of PowerBroker for Windows. PowerBroker for Windows provides fine-grained, policy-based privilege delegation for the Windows environment by removing local admin rights from end users and selectively elevating privileges for things such as applications, software installs, system tasks, scripts, and control panel applets.  
- PowerBroker for Windows augments support for testing procedure 7.1.2 by deploying rules based on the RBAC model in Active Directory.  
- PowerBroker for Windows directly supports testing procedure 7.1.3 because users with specific admin rights are explicitly defined by authorized personnel.  
- PowerBroker for Windows augments support for testing procedures 7.1.4 and 7.2.1 because PowerBroker for Windows uses Active Directory to perform its functions.  
- PowerBroker for Windows directly supports testing procedure 7.2.2 by using user and group information from Active Directory and applies policies to particular users/groups based on job classification. |
| **Requirement 8:** Assign a unique ID to each person with computer access | 8.1, 8.4.a, 8.4.b | PowerBroker for Windows meets or augments the following specific controls:  
- PowerBroker for Windows augments support for testing procedure 8.1 as it only uses unique user IDs from Active Directory.  
- PowerBroker for Windows directly supports testing procedure 8.4.a and 8.4.b by encrypting transmission using SSL V3 certificates. |
| **Requirement 10:**  | 10.1, 10.2.1 | PowerBroker for Windows meets or augments the following specific controls:  
- PowerBroker for Windows augments support for testing procedure 10.1, as it only uses unique user IDs from Active Directory.  
- PowerBroker for Windows directly supports testing procedure 10.2.1 by encrypting transmission using SSL V3 certificates. |
## PCI DSS V2.0 Applicability Matrix

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Controls Addressed</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Track and monitor all access to network resources and cardholder data</td>
<td>10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.5.1, 10.5.3, 10.6.a, 10.6.b, 10.7.a, 10.7.b</td>
<td>PowerBroker for Windows directly supports testing procedure 10.1 because audit trails for what applications users are launching are enabled by default. PowerBroker for Windows also allows for the configuration of session monitoring. Session monitoring captures screenshots of what actions a user is performing.</td>
</tr>
<tr>
<td>Requirement 11: Regularly test security systems and processes.</td>
<td>11.5.a</td>
<td>PowerBroker for Windows meets or augments the following specific controls:</td>
</tr>
<tr>
<td>Requirement A.1: Shared hosting providers must protect the cardholder data environment</td>
<td>A.1.2.a, A.1.2.d, A.1.3</td>
<td>PowerBroker for Windows meets or augments the following specific controls:</td>
</tr>
</tbody>
</table>
The need for removing administrative access to both desktops and servers is complementary. Regulations such as PCI can impact the end-to-end result of any technology implementation and removing privileges from the entire workflow ensures proper compliance with regulations such as PCI.

**PCI DSS V2.0 APPLICABILITY MATRIX**

<table>
<thead>
<tr>
<th>REQUIREMENT</th>
<th>CONTROLS ADDRESSED</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>

- because you can restrict viewing of logs to authorized parties.
- PowerBroker for Windows directly supports testing procedure A.1.3 by using session monitoring to see all actions a user performs.
Conclusion

PowerBroker for Windows provides fine-grained, policy-based privileged delegation for the Microsoft Windows environment. This patent-pending technology allows organizations to remove local admin rights from end users and server administrators without hampering productivity. PowerBroker selectively elevates privileges for applications, software installs, system tasks, scripts, control panel applets, management functions, and other operations – and reports the findings via BeyondTrust’s BeyondInsight IT Risk Management Platform.
About BeyondTrust

BeyondTrust provides context-aware Privileged Account Management and Vulnerability Management software solutions that deliver the visibility necessary to reduce IT security risks and simplify compliance reporting.

We empower organizations to not only mitigate user-based risks arising from misuse of system or device privileges, but also identify and remediate asset vulnerabilities targeted by cyber attacks. As a result, our customers are able to address both internal and external threats, while making every device – physical, virtual, mobile and cloud – as secure as possible.

BeyondTrust solutions are unified under the BeyondInsight IT Risk Management Platform, which provides IT and security teams a single, contextual lens through which to view user and asset risk. This clear, consolidated risk profile enables proactive, joint decision-making while ensuring that daily operations are guided by common goals for risk reduction.

The company is privately held, and headquartered in Phoenix, Arizona. For more information, visit beyondtrust.com.