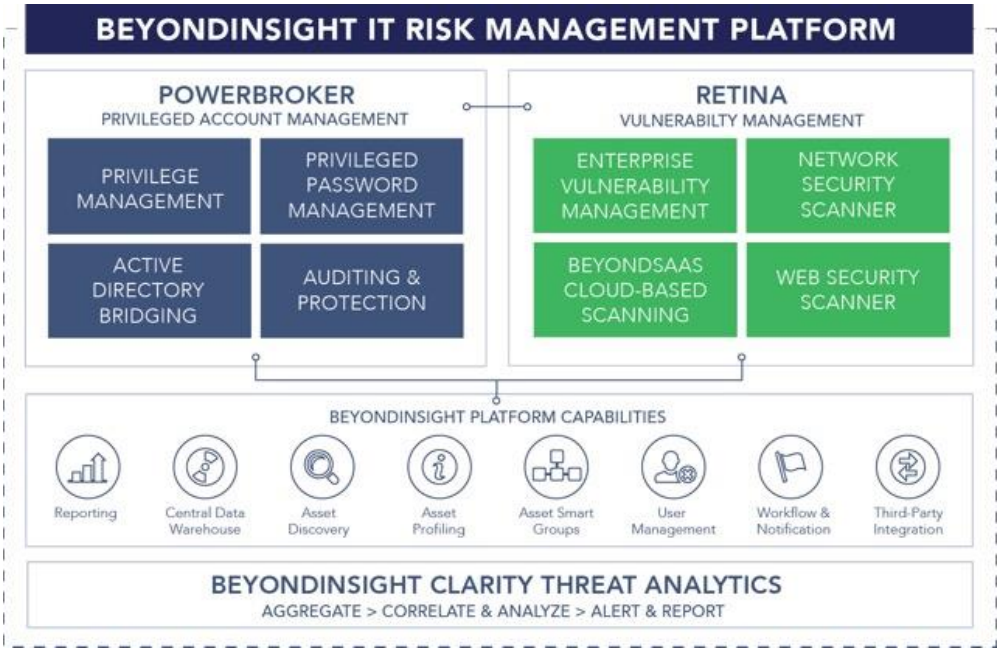
WHITE PAPER

BeyondTrust™

VISIBILITY. KNOWLEDGE. ACTION.

Four Best Practices for Passing Privileged Account Audits

Table of Contents



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

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.

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.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Four Best Practices for Passing Privileged Account Audits

Like most IT organizations, your team may periodically face the "dreaded" task of being audited. Your process for delegating privileged access to desktops, servers, and infrastructure devices is a massive target for the auditor's microscope. An audit's findings can have significant implications on technology and business strategy, so it's critical to make sure you're prepared when the auditor comes knocking at your door.

So where do you start? Most smart IT leaders know that administrative privileges need to be removed from most users – and well managed for those who do need them. This of course is easier said than done, as many applications and OS tasks require administrator privileges to correctly function. Even if you do clear this hurdle, you aren't necessarily going to pass that audit.

Good auditors know that removing administrator rights represents just a single step in the privileged account management process. While the list of specific audit requirements can seemingly go on forever, four essential practices will ensure that you pass your privilege management audits 99% of the time:

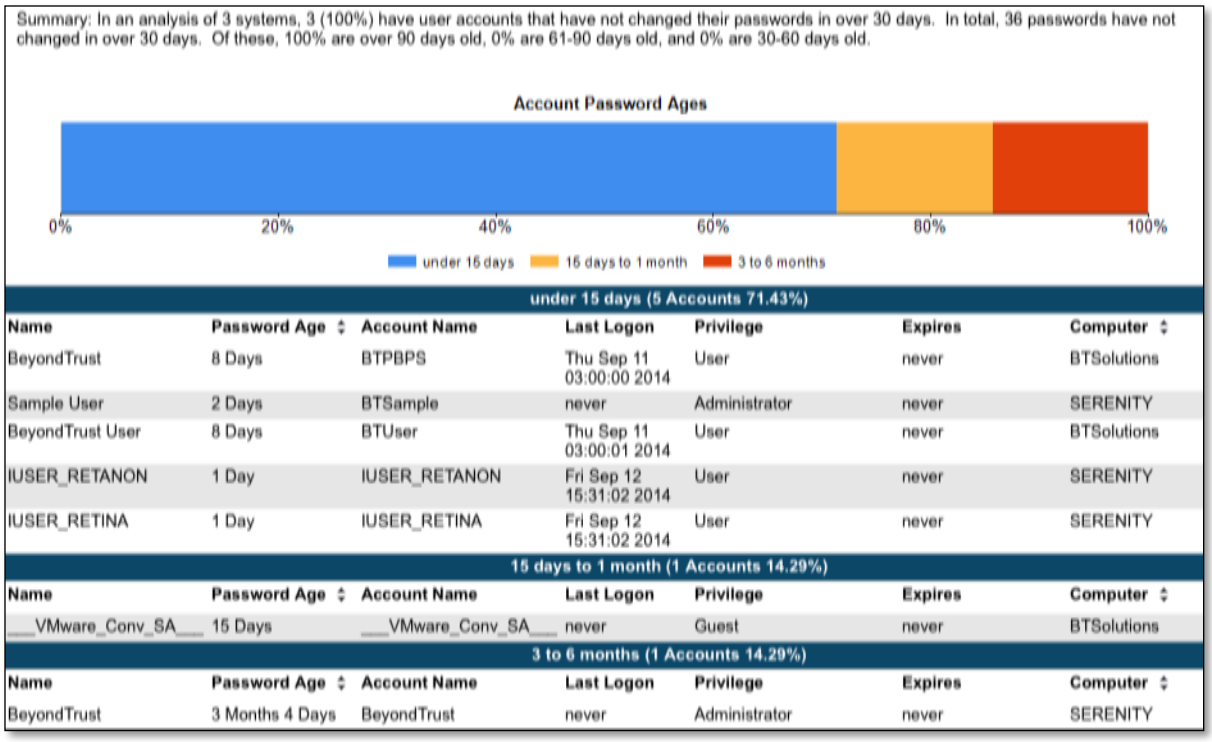
1. **Discover** all accounts that have privileged access regardless of device or platform
2. **Remove** privileged access or change management access to privileged accounts
3. **Report** the "who, what, when and where" behind privileged access
4. **Monitor** all changes executed by privileged users

This whitepaper introduces these practices and describes how BeyondTrust® solutions can help.

1. Discover All Privileged Accounts in Your Environment

Auditors need to be assured that you have a handle on *all* privileged accounts in your environment. Comprehensive discovery is critical, because if you can't find privileged accounts, you will never be able to remove or manage them. They can hide anywhere in your environment, including:

- Users in the domain admin group
- Users in local administrators group
- Users granted root access to UNIX, Linux, or infrastructure
- Service control accounts
- Application administrative accounts including databases
- Passwords encoded in scripts



Summary: In an analysis of 3 systems, 3 (100%) have user accounts that have not changed their passwords in over 30 days. In total, 36 passwords have not changed in over 30 days. Of these, 100% are over 90 days old, 0% are 61-90 days old, and 0% are 30-60 days old.

Account Password Ages

0% 20% 40% 60% 80% 100%

under 15 days | 15 days to 1 month | 3 to 6 months

under 15 days (5 Accounts 71.43%)

Name	Password Age	Account Name	Last Logon	Privilege	Expires	Computer
BeyondTrust	8 Days	BTPBPS	Thu Sep 11 03:00:00 2014	User	never	BTSolutions
Sample User	2 Days	BTSample	never	Administrator	never	SERENITY
BeyondTrust User	8 Days	BTUser	Thu Sep 11 03:00:01 2014	User	never	BTSolutions
IUSER_RETANON	1 Day	IUSER_RETANON	Fri Sep 12 15:31:02 2014	User	never	SERENITY
IUSER_RETINA	1 Day	IUSER_RETINA	Fri Sep 12 15:31:02 2014	User	never	SERENITY

15 days to 1 month (1 Accounts 14.29%)

Name	Password Age	Account Name	Last Logon	Privilege	Expires	Computer
___VMware_Conv_SA___	15 Days	___VMware_Conv_SA___	never	Guest	never	BTSolutions

3 to 6 months (1 Accounts 14.29%)

Name	Password Age	Account Name	Last Logon	Privilege	Expires	Computer
BeyondTrust	3 Months 4 Days	BeyondTrust	never	Administrator	never	SERENITY

Once you've identified your privileged accounts, you need to profile and prioritize them based on the level of risk they present to your environment. Following is one common approach:

- Priority 1: Interactive user accounts with administrator access (regardless of platform)
- Priority 2: Service accounts that do not receive password updates after their initial configuration
- Priority 3: Privileged credentials for databases and business applications

The next step is documenting your findings and building a plan for managing the discovered accounts.

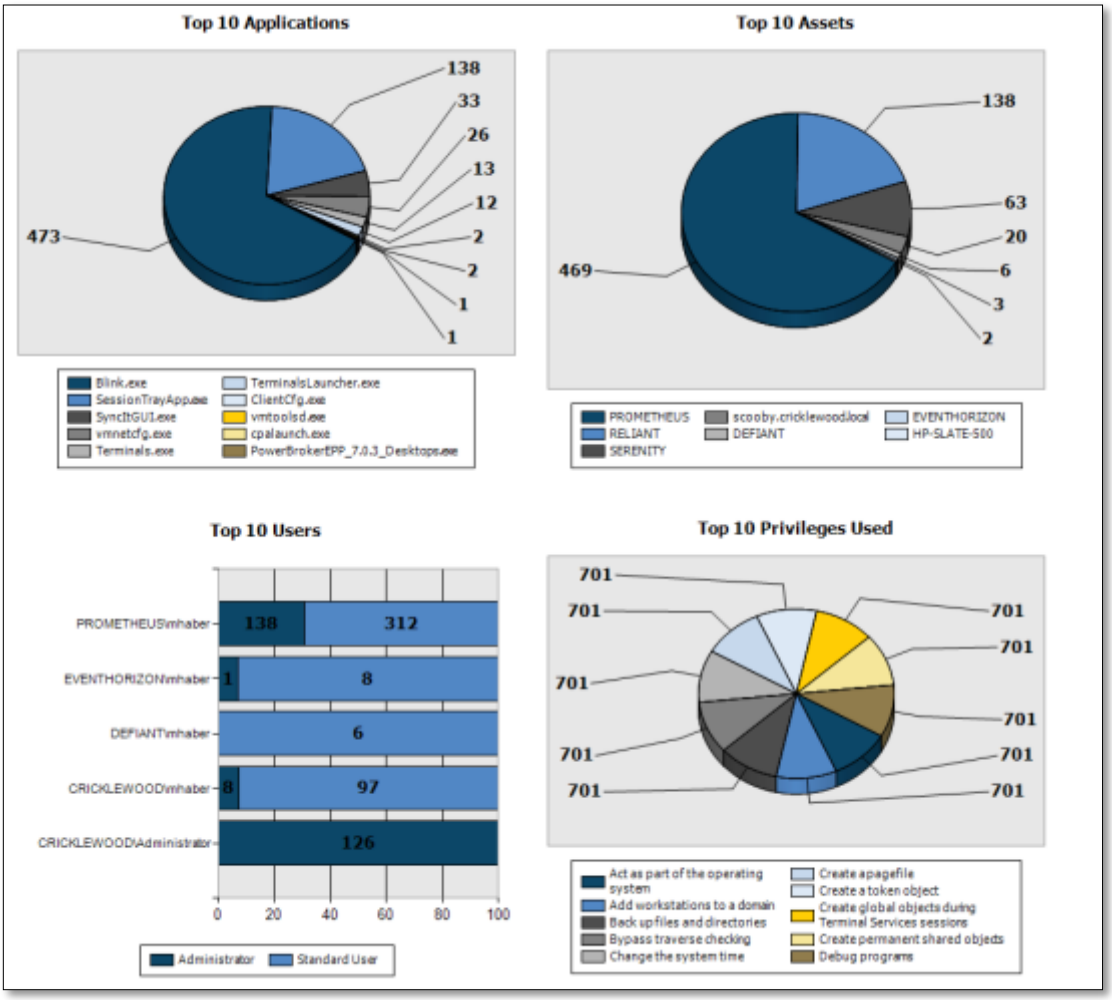
2. Remove Privileged Access / Implement Least Privilege

Once you've identified, profiled and prioritized your privileged accounts, the next step is implementing least-privilege best practices. At its most basic, least privilege involves removing privileges from those users who don't need them and managing access for those who do. However, least privilege can be implemented in several ways depending on the platform and device. On UNIX and Linux, least-privilege access is generally based on SSH connections. On Windows, least privilege is based on the user interface and applications – whether the user is locally logged on or connecting via remote desktop or other tools.

Implementing least privilege in hybrid IT environments normally requires a diverse set of tools. They can leverage Active Directory bridging to process accounts from a single authentication store, but they ultimately manage least privilege in completely different ways.

Ask yourself the following questions to narrow the tools and procedures you'll need to implement least-privilege management in your environment:

- What authentication stores are involved in providing privileged access? How can you consolidate them?
- Are there any cases where standard user accounts are not available? Does the platform require everyone to login with the same permissions?
- What applications, programs, operating system tasks, and service accounts require administrative permissions?
- Are the devices readily connected to the corporate network or are they in cloud, mobile, or air-gapped environments?



3. Report "Who, What, When and Where"

Discovery data and least-privilege management should not live in a bubble. Your audits will go much more smoothly if you're prepared with the right reports to demonstrate your privilege management processes and progress.

The data needs to be normalized, processed for change control, and ultimately presented in straightforward reports. Auditors will examine your reports for answers to the following questions:

- What types of privileged accounts are in your environment?
- Where do they exist?
- Who is using them?
- When did they use them?

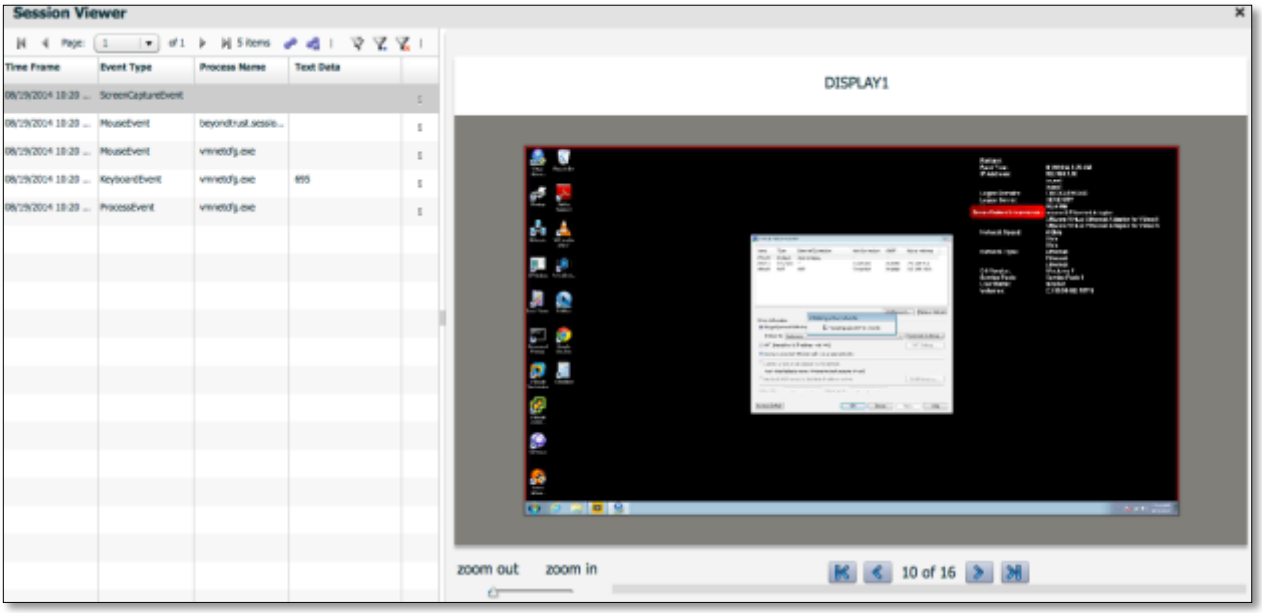
Strong reports demonstrate whether your organization's privilege management tools and processes span all required systems, while revealing whether the processes are correctly implemented or being abused. For example, a simple time/date report can confirm that no unauthorized credentialed access is occurring after hours:

Day/Hour	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
0							
1							
2							
3							
4							
5							
6							
7			17		12	18	
8		17		43	32	26	
9			1			103	
10			14			7	
11						4	
12		3					
13				107	8	17	
14				15		5	
15					15	19	
16						12	
17					10	7	
18					51	9	
19							
20							
21							
22							
23							
Total		20	32	165	128	227	

4. Monitor Privileged Sessions

One of the final questions you can expect to hear during an audit is, "What changes where made to the system and applications while the user was operating with elevated privileges?" It is one thing to know that a program was executed, and another to understand what that program did and what changes where actually made. To that end, your least-privilege monitoring practice should include:

- **Session monitoring** replays privileged activity from any point in time via I/O logging, video recordings, or screen captures.
- **Keystroke logging** can quickly identify red flags in a user's keystroke activity and properly mask when additional credentials where used.
- **File integrity monitoring** monitors key areas of the file system for unauthorized changes.
- **Event logging** provides a condensed event stream that can drive alerts or be fed into security information and event management (SIEM) solutions.



BeyondTrust Solutions for Privileged Account Management

By adhering to the above best practices, you will demonstrate to auditors where all privileged accounts live, who is using them, when are they being used, and what's happening during privileged sessions.

BeyondTrust offers an integrated suite of PowerBroker® Privileged Account Management (PAM) solutions that enable you to implement privilege management best practices with maximum efficiency and effectiveness. In fact, a recent Gartner Market Guide* recognizes

BeyondTrust as providing a comprehensive privileged account management solution suite: http://go.beyondtrust.com/gartnerpam

**Gartner, "Market Guide for Privileged Account Management" Felix Gaehtgens et al, 17 June 2014.*

PowerBroker solutions enable you to control administrative access while reducing costs by consolidating authentication stores, controlling application installation and access, and auditing privileged access. Key capabilities include:

- Discover all privileged accounts across servers and desktops
- Remove administrator rights across Windows, Mac, UNIX and Linux platforms
- Analyze and report on privileged accounts and elevated activities using secure communications
- Playback, report, and alert privileged sessions, regardless of platform, using secure communications

PowerBroker makes it easy to enforce consistent policies across all of your secure environments with a unique blend of guest control capabilities, asset control capabilities, and cost-effective deployment options.

PowerBroker for UNIX & Linux

PowerBroker for UNIX & Linux allows system administrators to delegate UNIX, Linux and Mac OS X privileges and authorization without disclosing root passwords. The solution can also record all privileged sessions for audits, including keystroke information. These and other capabilities enable PowerBroker customers to meet the privileged access control requirements of government mandates including SOX, HIPAA, PCI DSS, GLBA, PCI, FDCC and FISMA.

PowerBroker for Windows

PowerBroker for Windows is a simple, fast and flexible solution for privilege management and application control on physical and virtual Microsoft® Windows desktops and servers. Its patented technology can leverage Active Directory Group Policy or BeyondInsight Web Services to eliminate administrator privileges. This speeds least privilege enforcement across all Windows assets, while enabling granular application control and privileged activity logging.

PowerBroker Password Safe

Password Safe is an automated password management solution offering access control and auditing for any privileged account, such as shared administrative accounts, application accounts, and local administrative accounts. Password Safe is easily deployable and offers broad and adaptive device support. The solution even simplifies traditionally challenging tasks,

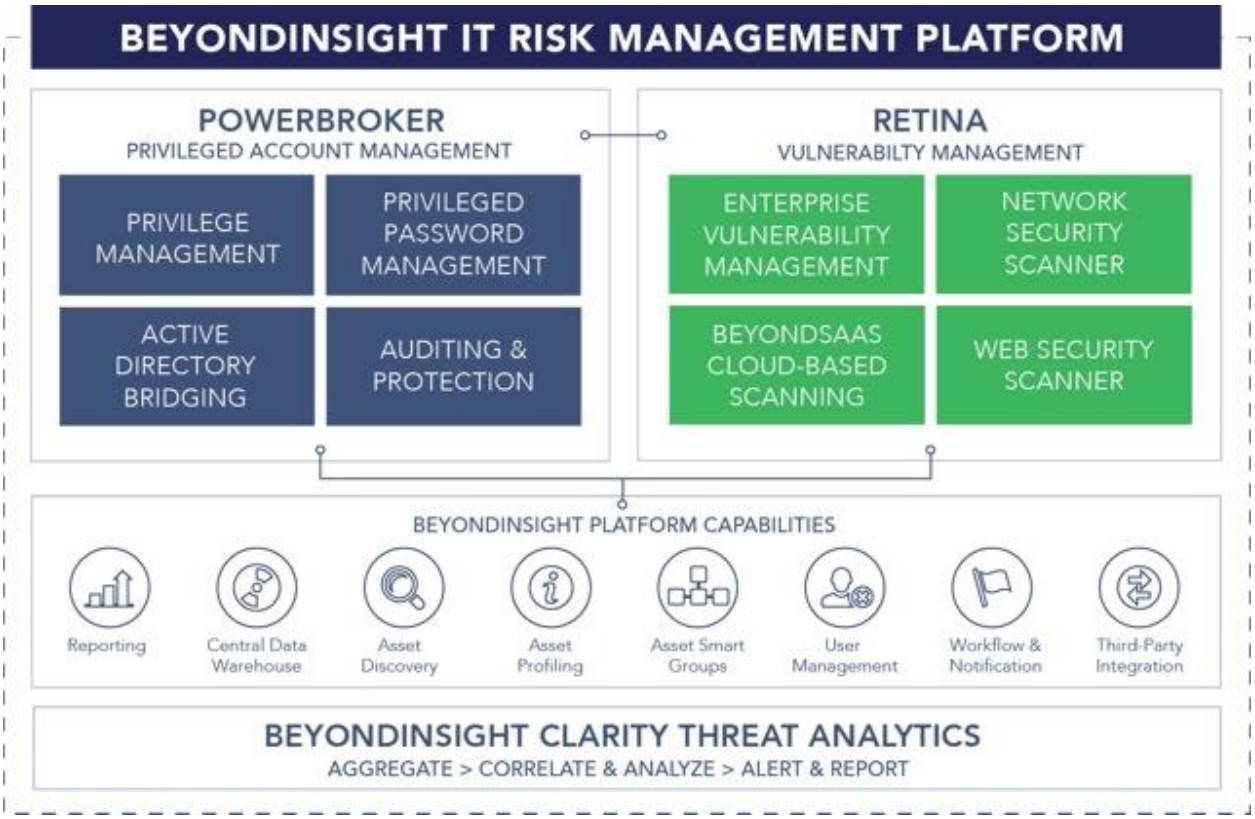
such as managing privileged passwords for service accounts between applications (A2A) and to databases (A2DB).

The BeyondInsight™ IT Risk Management Platform

BeyondInsight is a centralized management, analytics and reporting platform that is included standard with each of the above solutions, unifying them with one another as well as with BeyondTrust Retina Vulnerability Management solutions. Capabilities include:

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

With BeyondInsight, IT and security teams have a single platform through which to view and manage privileged accounts and privileged activity enterprise-wide. This clear, consolidated approach enables proactive, joint decision-making while ensuring that daily operations are guided by common goals for privilege management and risk reduction.



How BeyondTrust Compares

Here's a high-level comparison between BeyondTrust's ability to deliver on the four best practices and that of competitors for Windows:

	BeyondTrust	Avecto	Viewfinity
Discovery	Comprehensive, automated asset and user discovery	No discovery capability	No discovery capability
Least Privilege	Included; multiple patents	Included	Included
Reporting	Included for encrypted web services communications	Included, limited to Windows event forwarding only	Included
Activity Monitoring	Session, file integrity, and event log monitoring via web services and secure database storage	No monitoring capability	Session monitoring only and requires UNC file shares for on-premise playback

Only BeyondTrust delivers the comprehensive privileged account management capabilities you need to confidently fulfill your audit requirements, from account discovery to least-privilege activity reporting.

About BeyondTrust

BeyondTrust® is a global security company that believes preventing data breaches requires the right visibility to enable control over internal and external risks.

We give you the visibility to confidently reduce risks and the control to take proactive, informed action against data breach threats. And because threats can come from anywhere, we built a platform that unifies the most effective technologies for addressing both internal and external risk: Privileged Account Management and Vulnerability Management. Our solutions grow with your needs, making sure you maintain control no matter where your organization goes.

BeyondTrust's security solutions are trusted by over 4,000 customers worldwide, including over half of the Fortune 100. To learn more about BeyondTrust, please visit www.beyondtrust.com.