Seven Steps to Complete Privileged Access Management
## Contents

Today’s Reality: Balancing Breaches & Compliance Requirements Against User Productivity ...... 3
Toward a More Mature Security Organization ................................................................. 4
A Seven-Step Process to More Effective Privileged Access Management.......................... 5
  Step 1: Improve accountability and control over privileged passwords .................................. 5
  Step 2: Implement least privilege, application control for Windows & Mac desktops .................. 7
  Step 3: Leverage application-level risk to make better privilege decisions ............................ 8
  Step 4: Implement least privilege in Unix and Linux environments .................................... 9
  Step 5: Unify management, policy, reporting and threat analytics into under a single pane of glass ... 10
  Step 6: Integrate Unix, Linux and Mac into Windows ...................................................... 11
  Step 7: Real-time change auditing and recovery for Windows environments ........................... 12
The PowerBroker Difference .............................................................................................. 14
  Differentiator #1: Breadth and depth of our solution lowers total cost of ownership ............... 14
  Differentiator #2: Value gained from deep analytics and reporting insights .......................... 14
  Differentiator #3: Better understanding of threats in context from experience ....................... 14
Analyst Recognition ............................................................................................................. 15
Conclusion: Delivering Business Value ................................................................................ 16
About BeyondTrust .............................................................................................................. 18
Today’s Reality: Balancing Breaches and Compliance Requirements Against User Productivity

Controlling, monitoring, and auditing privileged access is essential to mitigating the risks posed by insider threats, preventing data breaches, and meeting compliance requirements. But security and IT leaders must walk a fine line between protecting the organization’s critical data to ensure business continuity, and enabling users and administrators to be productive. Dial up security? Frustration goes up. Dial down security, and you are the organization on the front page of the newspaper.

There is a gap between business protection and user enablement. What keeps security and IT leaders from closing that privilege gap? First, security leaders and their IT counterparts often must patch together multiple different point solutions that address only part of the problem and do not provide the visibility to solve the entire problem. Next, better intelligence is needed to make better risk and compliance decisions. Reporting and analytics must be delivered to many different stakeholders – from security to operations to compliance auditors. And finally, the last thing security and IT leaders need is another point tool. Wouldn’t you rather have contextual solutions delivered by a strategic partner with an understanding of your security environments?

Further complicating these challenges is that security and IT leaders face a lack of understanding on where to start. Is Unix the biggest area of risk? Or, is it privileged passwords? End user machines?

This white paper will help you answer just that – where to begin a privileged access management (PAM) project, how to progress to a higher level of security maturity, and what business outcomes to expect. To set the stage, we will first identify levels of security maturity and map attributes of a privileged access management program into those levels of maturity.

Throughout this paper, you will see various icons to help guide you along. Watch for these!

- **Statistics**
  *The facts and figures to back up our conclusions*

- **Tips & Best Practices**
  *What we’ve learned along the way*

- **Technical Attributes**
  *Key capabilities*

- **Case Study**
  *What real customers are doing to solve this problem*
Toward a More Mature Security Organization

A lack of maturity – rather a lack of *security maturity* to borrow a phrase from Brian Krebs – leads to the gap between security and productivity. Being security immature is not necessarily anyone’s fault; rather it has more to do with how culturally ingrained security is in your organization. Very small and understaffed organizations can be mature, while large organizations with ample resources can be security immature. What matters is that the organization is taking steps to move forward in its security maturity. But how can security and IT organizations initiate this shift?

We will borrow a simple security model developed by the Enterprise Strategy Group (and noted in the Krebs article mentioned above) that will help you assess where you are now on your journey to becoming a more mature security organization. For illustration purposes, this model incorporates common attributes in the context of privileged access management to the levels in the model. Take a hard look at your organization’s privileged access management practices and determine where you are.

*Figure 1: Example security maturity model*

<table>
<thead>
<tr>
<th>Security Model Level</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic</td>
<td>• Manual processes for managing privileged passwords, including spreadsheets, physical safes, or wetware</td>
</tr>
<tr>
<td></td>
<td>• Nearly all users in the organization have administrator access on their machines</td>
</tr>
<tr>
<td></td>
<td>• Individual vulnerability patching, management, and inconsistent policies by application</td>
</tr>
<tr>
<td></td>
<td>• Lack of auditing and control over root and privileged accounts</td>
</tr>
<tr>
<td></td>
<td>• No session monitoring or recording of privileged use</td>
</tr>
<tr>
<td></td>
<td>• No singular, clear picture of threats or what to do about them</td>
</tr>
<tr>
<td></td>
<td>• Disorganized and chaotic directory services infrastructure, with multiple logons required, and inconsistent policy</td>
</tr>
<tr>
<td></td>
<td>• No visibility over changes made to AD objects, configurations, or permissions; Always reacting</td>
</tr>
<tr>
<td>Progressing</td>
<td>• Some automation and some cycling of some privileged passwords</td>
</tr>
<tr>
<td></td>
<td>• 50% or fewer users with administrator credentials in the organization</td>
</tr>
<tr>
<td></td>
<td>• More automated scanning on vulnerable systems</td>
</tr>
<tr>
<td></td>
<td>• Common use of the root account, with some auditing of usage, perhaps sudo</td>
</tr>
<tr>
<td></td>
<td>• Some session monitoring for compliance purposes, snapshotting</td>
</tr>
<tr>
<td></td>
<td>• Threat analytics mostly from SIEMs</td>
</tr>
<tr>
<td></td>
<td>• Few (but not one) logins to heterogeneous systems</td>
</tr>
<tr>
<td></td>
<td>• Some change auditing, but lacking recovery of unwanted changes</td>
</tr>
<tr>
<td>Advanced</td>
<td>• Automated password and session management of all shared accounts</td>
</tr>
<tr>
<td></td>
<td>• Rules-based least privilege implemented organization-wide, on all systems</td>
</tr>
<tr>
<td></td>
<td>• Automated scanning, patching, and reporting of vulnerable systems</td>
</tr>
<tr>
<td></td>
<td>• Full control and accountability over privileged users on any system, eliminating root access or insufficient methods like sudo</td>
</tr>
<tr>
<td></td>
<td>• Automatic recording of keystrokes/video/over-the-shoulder activities</td>
</tr>
<tr>
<td></td>
<td>• Integrated threat analytics to improve decision-making</td>
</tr>
<tr>
<td></td>
<td>• Single sign on for heterogeneous systems leveraging familiar infrastructure</td>
</tr>
<tr>
<td></td>
<td>• Full auditing and recovery of changes across the environment; Ability to proactively know and deliver what auditors are looking for</td>
</tr>
</tbody>
</table>
The path to maturity is not an easy one. It’s not fast. There are no shortcuts. But, by investing in the right people, processes, and technology you can achieve greater levels of automation that will ultimately enable you to improve on the productive capacity of your IT security. This will help you align your efforts with your priorities. The next section of this paper discusses a seven-step approach to achieving a more mature and effective privileged access management program.

A Seven-Step Process to More Effective Privileged Access Management

Implementing an end-to-end privileged access management solution should follow a defined process to minimize costs and distractions, and speed results. This section of the white paper identifies the seven-step deployment plan for privileged access management. The result of this seven-step process is that you have more control and accountability over the accounts, assets, users, systems, and activity that comprise your privilege environment.

A critical success factor in ensuring a smooth path to end-to-end privileged access management is centralization. Management, policy, reporting, and analytics should all be centralized to speed deployments, get results quickly, and mitigate risks with consistency. This capability is discussed in detail in step 5.

Throughout the process of selecting and deploying your privileged access management solution, keep in mind these business requirements, as they will help you sell this program higher in the organization:

- Minimize total cost of ownership
- Provide a fast time-to-value
- Deliver the best information to make the best risk-based decisions

Step 1: Improve Accountability and Control Over Privileged Passwords

The most logical starting point for gaining greater control over privileges is by improving accountability over privileged passwords. Failure to effectively manage shared accounts poses considerable risks. You don’t have to look much further than recent breaches to grasp the implications – or the challenges. Moreover, certain systems have embedded or hardcoded passwords, opening opportunities for exploitation. Passwords are needed for application-to-application and application-to-database access. Passwords are generally static so there must be protections against passwords leaving the organization. Manual password rotation is unreliable and won’t scale well. On top of all of this, auditing and reporting on privileged access is complex and time-consuming.

In 2017 BeyondTrust conducted a survey of nearly 500 IT and security practitioners. The results of the survey, The 5 Deadly Sins of Privileged Access Management, clearly revealed a problem in managing privileged passwords. When asked to list the top threats associated with passwords, respondents listed employees sharing passwords with colleagues (79%), employees not changing default passwords their devices ship with (76%), and using weak passwords like “12345” (75%). Despite knowing better, respondents admitted that many of these same bad practices are common within their organization. A third of the respondents reported that users routinely share passwords with each other, and a fourth reported the use of weak passwords. Shockingly, one in five reported that many users don’t even change the default passwords!
How do organizations ensure accountability of shared privileged accounts to meet compliance and security requirements—without impacting administrator productivity?

The answer is automation. Privileged password and session management automation can enable secure access control, auditing, alerting, and recording for any privileged account (from local or domain shared administrator, to a user’s personal admin account, to service, operating system, network device, database (A2DB) and application (A2A) accounts – even SSH keys, cloud and social media accounts).

By improving the accountability and control over privileged access, such as through automation, IT organizations can reduce security risks and simplify the fulfillment of compliance objectives.

Top 10 privileged password management capabilities include the following:

1. Full network scanning, discovery, and profiling with auto-on-boarding
2. Builds permission sets dynamically according to data from scans
3. Automatically rotates SSH keys and cycles passwords according to a defined schedule
4. Provides granular access control, workflow, and auditing
5. A clean, uncluttered user interface (HTML5) for end users that expedites adoption
6. Workflow-based and break glass options for requesting access
7. Password and session management integrated within the same solution – no requirement for two different interfaces, or to be charged separately for each
8. No requirement for additional third-party tools or Java for session management – utilize native tools (MSTSC, PuTTY) instead
9. Leverages an integrated data warehouse and threat analytics across the privilege landscape
10. Flexible deployment options: hardware appliances, virtual appliances, or software

With such an automated solution, organizations can seamlessly discover all the accounts in their environment, place those accounts under management, and satisfy auditor requests that accounts are adequately managed.

DCI is an independent, privately owned company with several bank clients serving as owners, board members, and user-group leaders. Facing the challenge of securing and managing privilege accounts to meet audit and compliance requirements, DCI turned to BeyondTrust PowerBroker Password Safe. With Password Safe, DCI now has password rotation, delegation, and auditing capabilities, can ensure security and accountability over privileged passwords, and has efficient workflow time-limited requests.

PowerBroker Password Safe reduces the risk of privilege misuse and addresses compliance requirements through automated password and session management. With Password Safe, organizations can secure, control, alert, and record access to privileged accounts. The solution provides a low total cost of ownership (TCO) compared to other alternatives in the market, due to automatic discovery of any applications requiring privileges, and by integrating powerful, full-featured password and session management capabilities into the solution together. PowerBroker Password Safe provides a solid return-on-investment (ROI) via increased productivity for users and server administrators.
Step 2: Implement Least Privilege, Application Control for Windows & Mac Desktops

Once accounts and assets have been discovered and are being consistently managed, the next step to complete privileged access management is implementing least privilege on end-user machines. We recommend reducing risk on desktops before servers (such as Windows, Unix, or Linux as indicated in step 4) as the user’s endpoint is typically “the first mile of security” in cases of ransomware, phishing, and other user-based risks. Some organizations may choose to reverse this order, so depending on the specific business environment and risk tolerance, the priorities for these steps could be refined to match the risk appetite of the business.

The process for IT to restrict or enable end user privileges is complex and time-consuming, but it must be done to support audit or compliance mandates. While users should not be granted local administrator or power user privileges in the first place, sometimes certain applications require elevated privileges to run. The majority of Microsoft system vulnerabilities disclosed in 2016 - 94% - could have been mitigated by removing administrator rights from users. Clearly, this is a security gap that could lead to a damaging breach, not to mention a compliance problem.

How do IT organizations reduce the risk of potential exploitations and compliance violations arising from excessive user privileges, without obstructing end user productivity or overburdening the Help Desk?

The optimal way to accomplish this balancing act is by enforcing least-privilege access for applications with rules-based technology that can elevate application privileges without having to elevate individual user privileges. By eliminating Windows and Mac administrator privileges, simplifying the enforcement of least-privilege policies, maintaining application access control, and logging privileged activities, IT closes security gaps, while improving operational efficiency and compliance.

Top 10 desktop least privilege capabilities include the following:

1. Defaults all users to standard privileges while enabling elevated privileges for specific applications and tasks without requiring administrative credentials
2. Enforces restrictions on software installation, usage, and OS configuration changes
3. Eliminates the need for end users to require two accounts
4. Vulnerability-based application management – makes least privilege decisions for applications based on that application’s vulnerability, risk, and compliance profile
5. Matches applications to rules automatically based on asset-based policies. Leverages smart rules for alerting and grouping of devices and events
6. Reports on privileged access to file systems for all users and documents system changes during privileged sessions
7. Monitors sessions, captures screens, and logs keystrokes during privileged access
8. Provides a technique for using real domain or local privileges when required
9. Integrates with other privilege solutions to achieve comprehensive privileged access management
10. Leverages an integrated data warehouse and analytics across the privilege landscape

With this solution, customers gain the ability to efficiently eliminate local admin rights, and make vulnerability-based application elevation decisions.
RWE Supply & Trading is a leading energy trading house and a key player in the European energy sector. Facing the challenges of reducing the high number of calls to the IT Help Desk resulting from out-of-policy employee downloads, RWE chose BeyondTrust PowerBroker for Windows. With PowerBroker for Windows, RWE can eliminate admin rights on all users’ PCs as well as allow fine-grained control of privileges on the Windows Servers. RWE can now control servers, whether accessed by local employees, contractors, employees from other divisions, or by groups to which RWE outsourced.

PowerBroker for Windows and PowerBroker for Mac enforce least privilege access and help to achieve compliance across physical and virtual Microsoft Windows desktops and servers and Mac desktops efficiently, without disrupting user productivity or compromising security. The capabilities for automatic rule discovery and automated discovery of any applications requiring administrative privileges contribute to the solution’s low TCO.

Use Case: Solving remote password change challenges and elevation of applications for real user credentials.

Updating passwords for intermittent, remote, or mobile systems remains a challenge for customers that need to conduct business while on the move. Without instant updates, the capabilities and benefits of enterprise password managers are quickly negated. And, in some cases, the only way for privilege management products to properly elevate application privileges is to use a real username and password combination with administrator permissions. Problematically, this then requires the distribution of these credentials to users, which completely undermines the purpose of least privilege policies.

To overcome these obstacles, PowerBroker for Windows integrates with PowerBroker Password Safe to create an industry-unique approach for solving remote password change challenges and elevation of applications for real user credentials. This solution synergy enables the process for account password changes at any time, and in any location, and to overcome the limitations of network segmentation. Through this integration, organizations can process username and password combination requests and “Run As” commands with no user intervention. This technique allows instant access to applications while never exposing the username or password to the end user, which reduces security risk.

Step 3: Leverage Application-Level Risk to Make Better Privilege Decisions

Now that shared credentials are under management and end users have the privileges they need to perform their jobs – and nothing more – you can focus on understanding vulnerabilities with respect to helping your organization execute better-informed privilege elevation decisions. Most vulnerability management solutions do little to help security leaders put vulnerability and risk information in the context of business. Saddled with volumes of rigid data and static reports, the security team is left to manually discern real threats and determine how to act upon them.

BeyondTrust Retina CS is the only vulnerability management software solution designed from the ground up to provide organizations with context-aware vulnerability assessment and risk analysis. Retina’s architecture works with users to proactively identify security exposures, analyze business impact, and plan and conduct remediation across disparate and heterogeneous infrastructure.
Vulnerability-based application management is patented technology that automatically scans applications for vulnerabilities at run time – triggering alerts, reducing application privileges, or preventing launch altogether based on policy. This industry-unique integration comes standard in BeyondTrust PowerBroker for Windows.

Step 4: Implement Least Privilege in Unix & Linux Environments

Business-critical, Tier-1 applications are particularly attractive targets for adversaries. Accessing privileged user credentials for these resources can provide access to e-commerce data, ERP systems managing employee data, customer information, and sensitive financial data. While users rely on access to root passwords, super-user status, or other elevated privileges to perform their jobs, this practice presents tremendous security risks.

Remember that 5 Deadly Sins survey we mentioned above, in step 1? Privileged passwords weren’t the only perceived weakness. Two-thirds say managing least privilege for Unix/Linux servers is somewhat to extremely important. One popular option is Sudo. However, just 29 percent say Sudo meets their needs. The most commonly cited problems with Sudo include being time-consuming to use (32%), complexity (31%), and poor version control (29%). Despite this, the typical respondent runs Sudo on 40 workstations and 25 servers.

Traditional responses to this problem have many shortcomings, such as being:

- Inefficient and incomplete (such as native OS options), lacking the ability to delegate authorization without disclosing passwords
- Insufficiently secure (such as open source sudo) and inadequate when it comes to addressing risk or compliance requirements (such as lacking the ability to record sessions and keystrokes for audits)
- Incomplete – many “solutions” don’t account for activity inside scripts and third-party applications, leaving a shortcut to unapproved applications
- Incompatibility – such as lacking an efficient migration path away from sudo, if it is being used

How do IT organizations limit who has access to root accounts to reduce the risk of compromises without hindering productivity?

Organizations must be able to efficiently delegate Unix and Linux privileges and authorization without disclosing passwords for root or other accounts. Recording all privileged sessions for audits, including keystroke information, helps to achieve privileged access control requirements without relying on native tools or sudo.

Top 10 Unix and Linux server privilege management capabilities include the following:

1. Pluggable Authentication Module (PAM) support to enable utilization of industry-standard authentication systems
2. Advanced control and audit over commands at the system level
3. Powerful and flexible policy language to provide a migration path from sudo
4. Extensive support for many Unix and Linux platforms
5. Record and index all sessions for quick discovery during audits
6. Broker permissions transparently, ensuring user productivity and compliance
7. Change management of all settings and policy configuration, allowing full audit of who has changed what, version control, and rollback of all existing configuration files
8. REST API for easier integration with third-party products
9. Integrates all policies, roles, and log data via a web-based console
10. Leverages an integrated data warehouse and threat analytics across the privilege landscape

Such a solution provides you with the most comprehensive control over root access to Unix and Linux systems, while optimizing any use of sudo.

Based in Germany, XING is the social network for business professionals. XING found that its former privilege elevation process was too time-consuming and did not allow for a consistent set of access rights. The company was seeking to improve command elevation from an administrative point of view, as well as to establish better auditing features. In choosing BeyondTrust PowerBroker for Unix & Linux, XING has improved overall security, supported an increase in the level of privileged accounts and enabled a less time-consuming process.

PowerBroker for Unix & Linux is an enterprise-class, gold-standard privilege management solution that helps security and IT organizations achieve compliance, control privileged access, and prevent and contain breaches that can affect Unix and Linux systems – without hurting productivity. The product provides a low total cost of ownership (TCO) compared to alternatives by centralizing the management of privileged accounts under a single pane of glass, and by slashing the time it takes to achieve security and audit objectives. PowerBroker for Unix & Linux will provide a solid return-on-investment (ROI) via increased productivity for users and server administrators, without the security, compliance, and productivity drawbacks of open-source sudo.

Step 5: Unify Management, Policy, Reporting, and Threat Analytics Within a Single Pane of Glass

It’s no secret that IT and security professionals are overloaded with privilege, vulnerability, and attack information. Unfortunately, advanced persistent threats (APTs) often go undetected because traditional security analytics solutions are unable to correlate diverse data to discern hidden risks. Seemingly isolated events are written off as exceptions, filtered out, or lost in a sea of data. The intruder continues to traverse the network, and the damage continues to multiply.

How do security and IT operations teams gain an understanding of where threats are originating, prioritize them, and quickly mitigate the risks?

Advanced threat analytics enables IT and security professionals to identify the data breach threats routinely missed by other solutions. Advance threat analytics solutions pinpoint specific, high-risk users and assets by correlating low-level privilege, vulnerability, and threat data from a variety of third-party solutions.

Top 10 management and threat analytics capabilities include the following:

1. Correlates low-level data from a variety of third-party solutions to uncover critical threats
2. Correlates system activity against a constantly updated malware database
3. Reports on compliance, benchmarks, threat analytics, what-if scenarios, resource requirements, and more
4. Views, sorts, and filters historical data for multiple perspectives
5. Locates network (local & remote), web, mobile, cloud and virtual assets, as well as privileged accounts
6. Profiles IP, DNS, OS, Mac address, users, accounts, password ages, ports, services, software, processes, hardware, event logs, and more
7. Groups, assesses, and reports on assets by IP range, naming convention, OS, domain, applications, business function, Active Directory, and more
8. Imports from Active Directory or sets custom permissions
9. Provides workflow, ticketing, and notification to coordinate IT and security teams
10. Shares data with leading SIEM, GRC, NMS, and help desk solutions

**Figure 2: Integrated threat analytics and management for privileges and external vulnerabilities**

PowerBroker – powered by BeyondInsight, BeyondTrust’s unified management, reporting and threat analytics platform – unifies BeyondTrust privileged access management and vulnerability management solutions to provide IT and security teams with a single, contextual lens with which to view and address user and asset risk.

**Step 6: Integrate Unix, Linux, and Mac into Windows**

Think back to step 4 for a moment. Once you have greater control over privileged access in Unix and Linux environments, the next logical step is to bring those systems under consistent management, policy, and single sign-on. Unix, Linux, and Mac have traditionally been managed as standalone systems – each a silo with its own set of users, groups, access control policies, configuration files, and passwords to remember. Managing a heterogeneous environment that contains these silos – plus the Microsoft environment – leads to inconsistent administration for IT, unnecessary complexity for end users, and risk to the business.

How do IT organizations achieve consistent policy configuration to achieve compliance requirements, a simpler experience for users and administrators, and less risk from an improperly managed system?
The ideal solution is to centralize authentication for Unix, Linux, and Mac environments by extending Microsoft Active Directory's Kerberos authentication and single sign-on capabilities to these platforms. Extension of Group Policy to these non-Windows platforms enables centralized configuration management, reducing the risk and complexity of managing a heterogeneous environment.

Top 7 Active Directory bridge capabilities include the following:

1. No requirement to modify Active Directory schema to add Linux, Unix, or Mac OS X systems to the network
2. Provides a pluggable framework with an interface like Microsoft’s Management Console on Linux or Mac OS X; Full support for Apple’s Workgroup Manager application would allow for seamless management and control of Mac system settings
3. Single sign-on for any enterprise application that supports Kerberos or LDAP
4. Provides a single familiar tool set to manage both Windows and Unix systems (ex: Active Directory Users and Computers, ADUC)
5. Allows users to use their Active Directory credentials to gain access to Unix, Linux, and Mac, consolidating various password files, NISs and LDAP repositories into Active Directory and removing the need to manage user accounts separately
6. Proven track record of successful deployments and user support
7. Part of a broad privileged access management solution family

Such an AD Bridging solution will enable simplified configuration management and policy for non-Windows systems, while also supporting a better user experience and security. The solution must help you be more efficient by reducing the number of logins (and the accordant help desk calls when they are forgotten), and the number of different systems, configurations, and policies to manage.

A Global 500 North American telecom provider had discovered through an internal security audit that the company was not compliant with Sarbanes-Oxley; they needed a more modern identity management structure. The company had a very inefficient user on-boarding and off-boarding process due to the size and complexity of the environment. By leveraging BeyondTrust PowerBroker Identity Services, this company was able to meet organizational security and compliance standards, reduce workload for the server and identity administrator, streamline the logon processes for users, and consolidate over 100 NIS domains into a single cell.

PowerBroker Identity Services extends Microsoft Active Directory authentication, single sign-on and Group Policy configuration management to Unix, Linux, and Mac systems to improve efficiency, simplify compliance, and reduce risk. The solution provides a low total cost of ownership (TCO) compared to other alternatives, by allowing you to centralize the management of logins and configurations and by helping you reduce the time it takes to achieve security and compliance objectives. PowerBroker Identity Services will provide a solid return-on-investment (ROI) via increased productivity for users and server administrators.

Step 7: Real-Time Change Auditing and Recovery for Windows Environments

Once you have your non-Windows systems integrated into Active Directory, the next step is to audit user activity to gain additional insight into AD changes that could impact the business. Trying to keep up with all the changes made in Active Directory is an extremely time-consuming and complex process, with delays in discovering and addressing changes possibly leading to business disruption, not to mention the security and compliance implications of such changes.
When you include Exchange, Windows File Systems, SQL, and NetApp in the mix, understanding the “Who, What, When, and Where” of changes across the Windows infrastructure is even more complex.

How do IT organizations better understand changes, have the capability to roll them back if necessary, and establish the right entitlements in the first place across a complex Windows?

Organizations need centralized real-time change auditing for Active Directory, File Servers, Exchange, SQL, and NetApp, the ability to restore Active Directory objects or attributes, and to establish and enforce entitlements across the Windows infrastructure. Through simpler administration, IT organizations can mitigate the risks of unwanted changes and better understand user activity to meet compliance requirements.

Top 5 auditing and protection capabilities include the following:

1. Audit and roll back changes from a single product
2. Restores from the AD recycle bin without having to extract backups – providing continuous back up
4. One-click access to non-owner mailbox reporting in Exchange
5. Part of a broad privileged access management solution family

With such a solution, you gain detailed, real-time auditing of AD environments, and the ability to restore unwanted changes.

Ameritas Life Insurance was facing the challenges of reducing risk from security breaches and meeting compliance regulations – especially HIPAA. Using BeyondTrust PowerBroker Auditing & Security Suite, this company could meet organizational security and compliance standards, with PowerBroker given them data they lacked before.

PowerBroker Auditing & Security Suite audits and rolls back changes made in Active Directory in real-time, establishes and enforces entitlements across the Windows infrastructure, and helps to achieve compliance requirements in less time than it takes with native tools. The solution provides a low total cost of ownership (TCO) compared to other alternatives by centralizing management under a single pane of glass, and by reducing the time it takes to meet security and audit objectives. PowerBroker Auditing & Security Suite will provide a solid return-on-investment (ROI) via increased productivity for administrators.
The PowerBroker Difference

Why select a single vendor to achieve complete privileged access management? Why BeyondTrust? We believe our differentiation in the privileged access management market lies in the breadth and depth of our solution offering, the value you gain from analytics and reporting insights, and the context you gain with our solutions. Each differentiator is explored below.

Differentiator #1: Breadth and Depth of Our Solution Lowers Total Cost of Ownership

BeyondTrust delivers what leading industry analysts and others consider to be the most complete and integrated privileged access management platform available on the market. The PowerBroker Privileged Access Management Platform is an integrated solution that provides control and visibility over all privileged accounts and users across Windows, Mac, Unix, and Linux desktop and server platforms. By uniting best of breed capabilities within a single pane of glass, the PowerBroker platform simplifies deployments, reduces costs, improves system security, and closes gaps to reduce privileged access risks. Customers are using PowerBroker today to:

- Reduce the attack surface by eliminating the sharing of privileged accounts and delegating permissions without exposing credentials
- Monitor privileged user, session, and file activities for unauthorized access and/or changes to key files and directories
- Analyze asset and user behavior to detect suspect and/or malicious activities of insiders and/or compromised accounts

This comprehensive model delivers maximum insights, simplifies management, and lowers total cost of ownership.

Differentiator #2: Value Gained from Deep Analytics and Reporting Insights

BeyondTrust solutions help security and IT operations teams make informed decisions. Since a privilege problem tends to involve more than one department in the organization, our solutions satisfy the reporting, auditing, and management needs of multiple stakeholders, from operations to security to compliance.

The PowerBroker Platform provides security and IT operations teams a single view of all assets and user activity. With behavioral analytics to understand anomalies, reporting to satisfy security, operations, and auditors, and the ability to export data to other security solutions, BeyondInsight reduces risks while helping to maximize the value of existing security investments.

Differentiator #3: Better Understanding of Threats in Context from Experience

The last thing we think you need is another siloed security point solution. BeyondTrust provides a complete understanding of the modern threat landscape across both internal and external risk. Our solutions incorporate relevant security data – available exploits, risky privileged activity, vulnerable systems and applications, compliance requirements, mitigations etc. – to help our customers drive better, more informed security decisions.
Analyst Recognition

BeyondTrust’s approach to solving privileged access management challenges has been recognized by the industry as well as by our customers. Read what some of the most influential industry experts say:

- Gartner: BeyondTrust is a listed as a representative vendor in the Gartner Market Guide for Privileged Access Management.¹
- Forrester: “BeyondTrust is a Leader.” “BeyondTrust excels with its privileged session management capabilities.”²
- Ovum: “Deploying the BeyondTrust platform ... provides an integrated, one-stop approach to PAM ... one of only a small band of PAM providers offering end-to-end coverage.”³
- SC Magazine: “For its traditional BeyondTrust quality and complete integration into the BeyondTrust platform, we make this our Recommended product.”⁴


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.
Conclusion: Delivering Business Value

BeyondTrust has defined what a complete privileged access management solution looks like, creating a holistic program and tying it all together with the PowerBroker platform. This white paper explained an enterprise deployment of BeyondTrust privileged access management solutions using PowerBroker, demonstrating how you can completely solve the challenges related to privileged access in the organization and grow to become a more mature security organization.

The result of a comprehensive PAM deployment is that you will realize:

- Uniform, streamlined PAM system (central repository)
- Visibility across the environment (analytics on who does what) regardless of platform
- Firm foundation, regardless of which platform users are coming from (application, operating system, or database)

The ultimate value BeyondTrust can deliver is to reduce risk and streamline user and application privilege management through simplified deployment, ease of use, and prioritization of security and compliance risks.

Through tightly integrated vulnerability management, patented technology, and 25 years of experience in the privileged access management market, BeyondTrust is the only security solution provider to provide zero-gap visibility across all physical, virtual, cloud and mobile assets, in addition to traditional desktops and servers.

For a diagram of a complete PAM deployment across the seven progressive steps, see figure 3 on the next page.
Figure 3: Integrated seven-step process to complete privileged access management

1. **STEP 1**
   - Accounts | Hosts
   - Improve accountability and control over privileged passwords.

2. **STEP 2**
   - Windows | Mac Users
   - Implement least privilege and application control for Windows and Mac desktops.

3. **STEP 3**
   - Assets
   - Leverage application-level risk to make better privilege decisions.

4. **STEP 4**
   - Windows | Unix Linux Servers
   - Implement least privilege in Unix and Linux environments.

5. **STEP 5**
   - Centralized management, policy, reporting & threat analytics

6. **STEP 6**
   - Unix Linux Systems
   - Integrate Unix, Linux and Mac into Windows.

7. **STEP 7**
   - Users | Activity
   - Real-time change auditing and recovery for Windows environments.

**LESS COST AND COMPLEXITY • FASTER TIME TO VALUE • LESS RISK**
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 Access 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.