WHITE PAPER

BeyondTrust™

VISIBILITY. KNOWLEDGE. ACTION.

Seven Steps to Complete Privileged Account Management

August 2015

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.

Table of Contents

Contents

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 have to 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.

It is clear that 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 have to 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 has to 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 account management 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 account 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 account management to the levels in model. Take a hard look at your organization's privileged account management practices and determine where you are.

Figure 1: Example security maturity model

Security Model Level	**Attributes**
Basic	• Manual processes for managing privileged passwords, including spreadsheets, physical safes or wetware • Nearly all users in the organization have administrator access on their machines • Individual patching, management and inconsistent policies by application • Lack of auditing and control over root accounts and privileged accounts • No session monitoring or recording of privileged use • No singular clear picture of threats or what to do about them • Disorganized and chaotic directory services infrastructure, with multiple logons required and inconsistent policy • No visibility over changes made to AD objects, configurations or permissions; Always reacting
Progressing	• Some automation and some cycling of some privileged passwords • 50% or fewer users with administrator credentials in the organization • More automated scanning on vulnerable systems • Common use of the root account, with some auditing of usage, perhaps sudo • Some session monitoring for compliance purposes, snapshotting • Threat analytics mostly from SIEMs • Few, but not one login to heterogeneous systems • Some change auditing, but lacking recovery of unwanted changes
Advanced	• Automated password and session management of all shared accounts • Rules-based least privilege implemented organization-wide, on all systems and machines • Automated scanning, patching and reporting of vulnerable systems • Full control and accountability over privileged users on any system, eliminating root access or insufficient methods like sudo • Automatic recording of keystrokes/video/over-the-shoulder activities • Integrated threat analytics to improve decision making • Single sign on for heterogeneous systems leveraging familiar infrastructure • Full auditing and recovery of changes across the environment; Ability to proactively know and deliver what auditors are looking for

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 account management program.

A Seven-Step Process to More Effective Privileged Account Management

Implementing an end-to-end privileged account 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 account management. The end result of this seven-step process is that you have greater control and accountability over the accounts, assets, users, systems and activity that make up your privilege environment.

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

Throughout the process of selecting and deploying your privileged account 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. Not effectively managing shared accounts is a problem that has significant scale and risks. You don't have to look much further than recent breaches to understand the implications – or the challenges. Certain systems have embedded or hardcoded passwords, opening up opportunities for misuse. 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. Password rotation is unreliable and manual. Auditing and reporting on access is complex and time consuming.

In 2015 BeyondTrust conducted a survey of more than 700 IT and security practitioners. The results of the survey, Privilege Gone Wild, cleared showed a problem in managing privileged passwords. Just over half (51%) of the respondents to the survey stated that shared passwords are managed "individually." This could include users sharing passwords on an ad hoc basis, or simply by memory. 35% indicate that shared passwords are controlled "locally," including spreadsheets, password vaults, SharePoint, and Active Directory.

How do organizations ensure accountability of shared privileged accounts to meet compliance and security requirements without impacting administrator productivity?

The answer is automation – automating password and session management, providing secure access control, auditing, alerting and recording for any privileged account – from local or domain shared administrator, to a user's personal admin account (in the case of dual accounts), to service, operating system, network device, database (A2DB) and application (A2A) accounts – even SSH keys. By improving the accountability and control over privileged access IT organizations can reduce security risks and achieve compliance objectives.

Top 10 privileged password management capabilities include the following:

1. Full network scanning, discovery and profiling with auto-onboarding
2. Build permission sets dynamically according to data from scans
3. Automatically rotate SSH keys and cycle passwords according to a defined schedule
4. Granular access control, workflow and auditing
5. A clean, uncluttered user interface (HTML5) for end users that speeds adoption
6. Workflow-based and break glass options for requesting access
7. Password and session management together in 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. Leverage an integrated data warehouse and threat analytics across the privilege landscape
10. Flexible deployment options: hardware appliances, virtual appliances, or software

With this solution organizations have the capability to discover all of the accounts in their environment, place those accounts under management, and satisfy auditor requests that accounts are now 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, that the solution includes both password and session management together, and does not require the use of additional third-party tools for session management. PowerBroker Password Safe will provide 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 account 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 endpoint is typically the last mile of security. Secure the last mile first. Some organizations may choose to reverse this order, so depending on the specific business environment and risk, the priorities for these steps could be refined to match the risk level and appetite for 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. And although 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 2014 - 80% - could have been mitigated by removing administrator rights from users. Clearly, this is a security gap that could lead to an embarrassing breach, not to mention a compliance problem.

How do IT organizations reduce the risk of users having excessive privileges and subjecting the organization to potential exploitation or compliance violations without obstructing their productivity or overburdening the Help Desk?

Only through least-privilege access for applications with patented, rules-based technology to elevate application privileges without elevating 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, improves operational efficiency and achieves compliance objectives faster.

Top 10 desktop least privilege capabilities include the following:

1. Default all users to standard privileges while enabling elevated privileges for specific applications and tasks without requiring administrative credentials
2. Enforce restrictions on software installation, usage, and OS configuration changes
3. Eliminate the need for end users to require two accounts
4. Vulnerability-based application management – make least privilege decisions for applications based on that application's vulnerability, risk, and compliance profile
5. Match applications to rules automatically based on asset based policies. Leverage smart rules for alerting and grouping of devices and events
6. Report on privileged access to file systems for all users and document system changes during privileged sessions
7. Monitor sessions, capture screens and log keystrokes during privileged access
8. Provide a technique for using real domain or local privileges when required
9. Integrate with other privilege solutions to achieve comprehensive privileged account management
10. Leverage 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 based on patented technology.

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 is able to 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 solutions provide low TCO, mainly due to the features of automatic rule discovery and automated discovery of any applications requiring administrative privileges.

According to data published by Gartner in their report, *Organizations That Unlock PCs Unnecessarily Will Face High Costs*, when a user is a standard user, the amount of IT labor needed for technical support is 24% or $1200 per desktop less than when a desktop user is an administrator. PowerBroker solves this challenge.

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

Updating passwords for intermittent, remote or mobile systems remain 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. This problem then requires the distribution of these credentials to users, which defeats the purpose of least privilege policies.

To overcome these obstacles, PowerBroker for Windows integrates with PowerBroker Password Safe to create an industry-unique approach to solving remote password change challenges and elevation of applications for real user credentials. The result is a process for account password changes at any time, and in any location, and to overcome the limitations of network segmentation. The integration can process username and password combination requests and "Run As" commands with no user intervention. This technique allows instant access to applications and never exposes the username or password to the end user. The result is quicker access to critical applications and reduced 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 move to a better understanding of vulnerabilities to help make better-informed privilege elevation decisions. The challenge, though, is that 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 and Linux environments

In the current environment, business critical, tier-1 applications are attractive targets for adversaries. Accessing privileged user credentials for these resources can provide access to ecommerce data, ERP systems managing employee data, customer information, and sensitive financial data. Having root passwords, super-user status, or other elevated privileges is important for users to do their jobs. But unfortunately, this practice presents significant security risks stemming from intentional, accidental or indirect misuse of those shared privileges – especially when those shared privileges have access to tier 1 systems that impact the business such as those running on Unix or Linux servers.

Remember that Privilege Gone Wild survey we mentioned above in step 1? Privileged passwords weren’t the only perceived weakness. 58% of the respondents believe their current controls against misuse on business-critical, tier-1 systems are inadequate, immature or non-existent. Clearly, addressing this shortcoming should be an immediate priority for these organizations.

Traditional responses to this problem …

- Are inefficient and incomplete (such as native OS options) lacking the ability to delegate authorization without disclosing passwords
- Are not secure enough (such as open source sudo) to address risk or compliance requirements lacking the ability to record sessions and keystrokes for audits
- Don’t account for activity inside scripts and third-party applications, leaving a shortcut to unapproved applications
- Don’t offer an efficient migration path away from sudo if it is being used

How do IT organizations limit who has assess 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. Integrate all policies, roles and log data via a web-based console
10. Leverage an integrated data warehouse and threat analytics across the privilege landscape

With this capability, you gain the most complete control over root access to Unix and Linux systems and get the most out 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 establish better auditing features for his and his colleagues' use as managers. 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 Unix & Linux helps you achieve control over Unix root account privileges with centralized analytics and reporting, and keystroke logging. With it, you can reduce risk and achieve compliance faster than with native tools or sudo. The product provides a low total cost of ownership (TCO) compared to other alternatives, due to centralizing the management of privileged accounts under a single pane of glass, and taking less time 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 risk of open-source sudo.

Step 5: Unify management, policy, reporting and threat analytics into under a single pane of glass

It is 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 coming from, prioritize them, and quickly mitigate the risks?

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

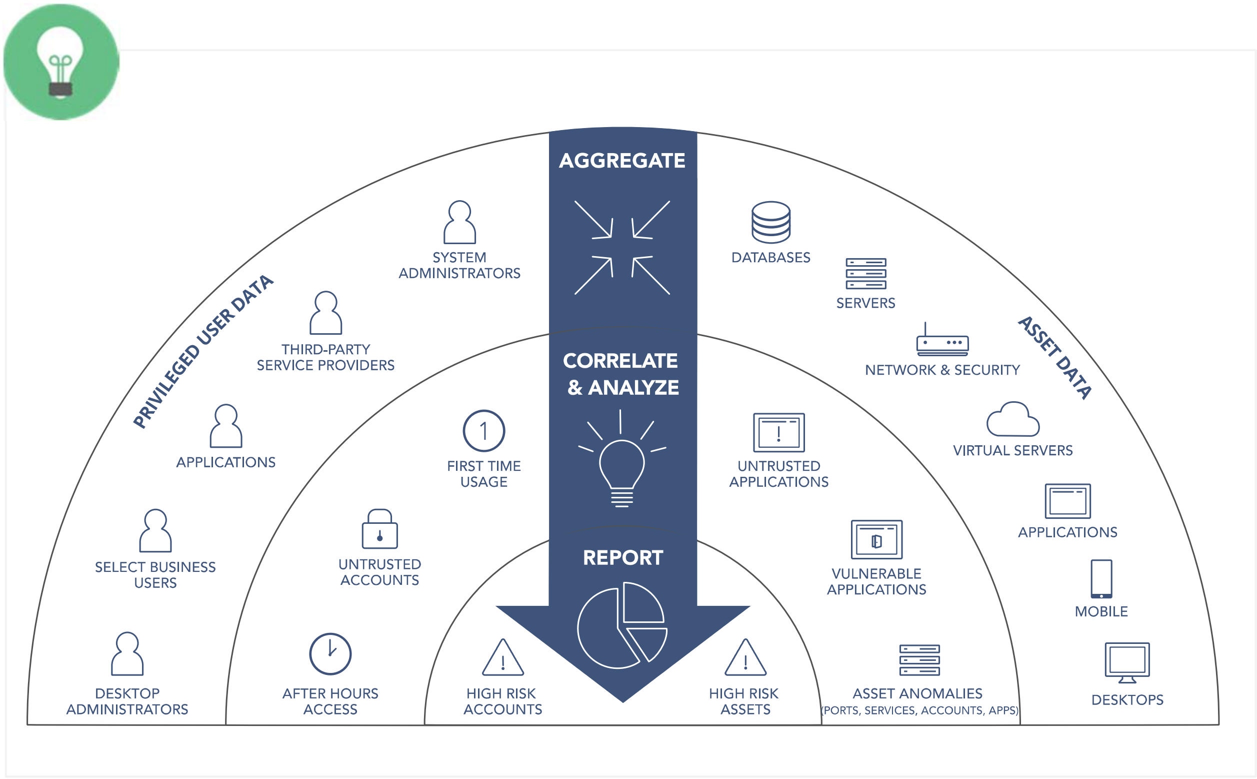
Top 10 management and threat analytics capabilities include the following:

1. Correlate low-level data from a variety of third-party solutions to uncover critical threats
2. Correlate system activity against a constantly updated malware database
3. Report on compliance, benchmarks, threat analytics, what-if scenarios, resource requirements, and more
4. View, sort and filter historical data for multiple perspectives
5. Locate network (local & remote), web, mobile, cloud and virtual assets, as well as privileged accounts
6. Profile IP, DNS, OS, Mac address, users, accounts, password ages, ports, services, software, processes, hardware, event logs, and more
7. Group, assess, & report on assets by IP range, naming convention, OS, domain, applications, business

function, Active Directory, and more

8. Import from Active Directory or set custom permissions
9. Workflow, ticketing and notification to coordinate IT and security teams
10. Share data with leading SIEM, GRC, NMS and help desk solutions

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



By unifying BeyondTrust privileged account management and vulnerability management solutions, BeyondInsight provides IT and security teams a single, contextual lens through 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. By extending Group Policy to these non-Windows platforms you gain 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. Provide a pluggable framework with an interface similar to 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. Provide a single familiar tool set to manage both Windows and Unix systems (ex: Active Directory Users and Computers, ADUC)
5. Allow users to use their Active Directory credentials to gain access to Unix, Linux and Mac, consolidating various password files, NIS 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 account management solution family

This will enable simplified configuration management and policy for non-Windows systems, and will help improve security and the user experience. 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. Using BeyondTrust PowerBroker Identity Services, this company was able to meet organizational security and compliance standards, reduce workload for server and identity administrator, streamline 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, mainly due to centralizing the management of logins and configurations and because it allows you to leverage your Windows Active Directory infrastructure, and helps you take less time to achieve security and audit 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. But 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 infrastructure so they can more effectively protect the business?

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 – without requiring two different solutions to accomplish
2. Restore from the AD recycle bin without having to extract backups – providing continuous back up
3. Audit, report and recover across a complex Windows or heterogeneous environment – AD, Windows File System, Exchange, SQL, NetApp – from a single console
4. One-click access to non-owner mailbox reporting in Exchange
5. Part of a broad privileged account management solution family

With this capability, 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 Management Suite, this company was able to meet organizational security and compliance standards, with PowerBroker given them data they did not have before.

PowerBroker Management 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 with native tools. The solution provides a low total cost of ownership (TCO) compared to other alternatives, mainly due to centralizing management under a single pane of glass, and helping to take less time to achieve security and audit objectives. PowerBroker Management 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 account management? Why BeyondTrust? We believe our differentiation in the privileged account 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

Gartner

PAM Solutions Center

BeyondTrust delivers what industry experts consider to be the complete spectrum of privileged account management solutions available in the market. From establishing and enforcing least privilege on Windows, Mac, Unix and Linux systems; to automating password and session management; to integrating Unix, Linux, and Mac OS X systems with Microsoft Active Directory; to auditing user and administrator activity, BeyondTrust unifies these capabilities into a single, integrated platform that acts as a central policy manager and primary reporting interface.

In its Market Guide for Privileged Account Management, research firm Gartner recognizes BeyondTrust as a representative vendor for all solution categories in the PAM market. What differentiates us from other vendors in this space is that BeyondTrust is the only company that offers these capabilities from a single, integrated reporting and management platform.

This breadth and flexibility enables you to handle today's threat scenarios and prepare for tomorrow's possibilities. Examples of this breadth include:

- Protecting Windows and Mac desktops from misuse and APT attacks
- Protecting In-house Windows, Unix and Linux servers hosting key applications and sensitive data
- Reducing risk of third party access to servers, networking devices and other assets
- Controlling and auditing access to cloud, virtual and SaaS applications by privileged employees, contractors and other third parties
- Implementing threat intelligence that extends beyond detection to include isolation and remediation

This comprehensive model delivers maximum insights, simplifies management, and lowers total cost of ownership. As well, BeyondTrust embraces a modular, integrated approach for customers with existing point solution investments.

Differentiator #2: Value gained from deep analytics and reporting insights

BeyondTrust solutions help security and IT operations teams alike 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.

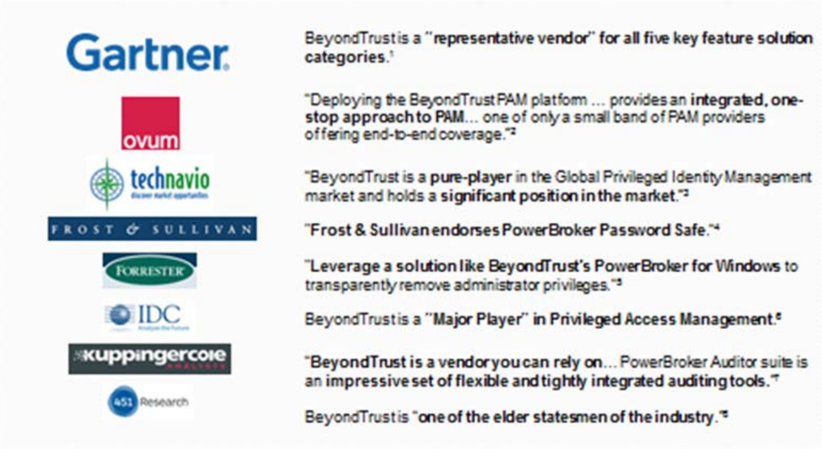
The BeyondInsight IT Risk Management Platform provides security and IT operations teams a single view of all assets and user activity. With behavioral analytics to understand anomalies, reporting to satisfy security, operations and auditors alike, and the ability to export data to other security solutions, 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.

Analysts and Experts Agree

BeyondTrust's approach to solving privileged account management challenges has been validated by the industry as well as by our customers. Read what some of the most influential industry experts have to say:



Gartner	BeyondTrust is a "**representative vendor**" **for all five key feature solution categories.**[1]
ovum	"Deploying the BeyondTrust PAM platform … provides an **integrated, one-stop approach to PAM**… one of only a small band of PAM providers offering end-to-end coverage."[2]
technavio	"BeyondTrust is a **pure-player** in the Global Privileged Identity Management market and holds a **significant position in the market**."[3]
FROST & SULLIVAN	"**Frost & Sullivan endorses PowerBroker Password Safe.**"[4]
FORRESTER	"**Leverage a solution like BeyondTrust's PowerBroker for Windows** to transparently remove administrator privileges."[5]
IDC	BeyondTrust is a "**Major Player**" **in Privileged Access Management.**[6]
kuppingercole	"**BeyondTrust is a vendor you can rely on**… PowerBroker Auditor suite is **an impressive set of flexible and tightly integrated auditing tools.**"[7]
451 Research	BeyondTrust is "**one of the elder statesmen of the industry.**"[8]

[1] Gartner, Market Guide for Privileged Access Management, May 27, 2015.
[2] Ovum, SWOT Assessment: BeyondTrust Privileged Identity Management Portfolio, June 11, 2015.
[3] TechNavio, Global Privileged Identity Management Market 2015-2019, 2014.
[4] Frost & Sullivan, PowerBroker Password Safe – a Frost & Sullivan Product Review, 2014.
[5] Forrester, Introducing Forrester's Targeted Hierarchy of Needs, May 15, 2014.
[6] IDC, IDC MarketScape: Worldwide Privileged Access Management 2014 Vendor Assessment, March 2015.
[7] Kuppinger Cole, Executive View: BeyondTrust PowerBroker Auditor Suite, March 2015.
[8] 451 Research, BeyondTrust looks to platform plan to make the most of its privileged management assets, June 18, 2015.

Conclusion: Delivering Business Value

BeyondTrust has defined what a complete privileged account management solution looks like, creating a holistic program and tying it all together with BeyondInsight. This white paper explained an enterprise deployment of BeyondTrust privileged account management solutions using BeyondInsight, demonstrating how you can completely solve the challenges related to privileged access in the organization and grow to become a more mature security organization. To accomplish this we have diagramed a complete solution deployment in seven progressive steps. See figure 3 below.

The end result of this deployment is that you will realize:

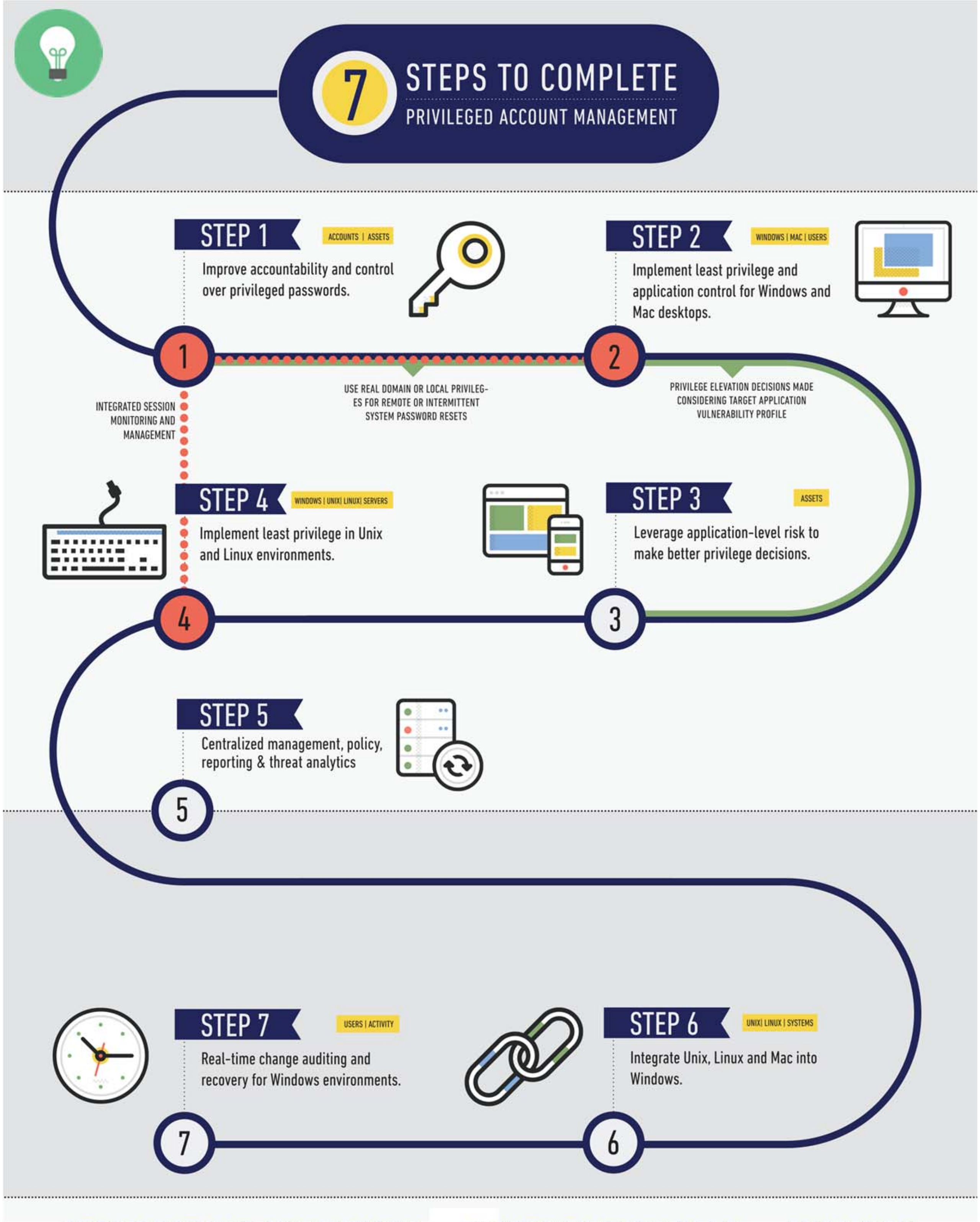
- Uniform, streamlined PAM system (central repository)
- Visibility across the environment (analytics on who does what) regardless of platform
- Firm foundation, regardless of which platform users are coming from (application, operating system or database)

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 30 years of experience in the privilege account 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.

To realize the full benefit of BeyondTrust's privileged account management solutions, utilize the BeyondInsight IT Risk Management platform, and then take control of accounts, assets, users, systems and activity.

Figure 3: Integrated seven-step process to complete privileged account management



7 STEPS TO COMPLETE

PRIVILEGED ACCOUNT MANAGEMENT

STEP 1 — ACCOUNTS | ASSETS

Improve accountability and control over privileged passwords.

STEP 2 — WINDOWS | MAC | USERS

Implement least privilege and application control for Windows and Mac desktops.

USE REAL DOMAIN OR LOCAL PRIVILEGES FOR REMOTE OR INTERMITTENT SYSTEM PASSWORD RESETS

PRIVILEGE ELEVATION DECISIONS MADE CONSIDERING TARGET APPLICATION VULNERABILITY PROFILE

INTEGRATED SESSION MONITORING AND MANAGEMENT

STEP 4 — WINDOWS | UNIX| LINUX| SERVERS

Implement least privilege in Unix and Linux environments.

STEP 3 — ASSETS

Leverage application-level risk to make better privilege decisions.

STEP 5

Centralized management, policy, reporting & threat analytics

STEP 7 — USERS | ACTIVITY

Real-time change auditing and recovery for Windows environments.

STEP 6 — UNIX| LINUX | SYSTEMS

Integrate Unix, Linux and Mac into Windows.

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 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.