BeyondTrust

Privilege Gone Wild: The State of Privileged Account Management in 2015

March 2015
# Table of Contents

Privilege Gone Wild: The State of Privileged Account Management in 2015 ........................................ 4

Survey Results ......................................................................................................................................................... 5
  1. Risk is Recognized, and Control is Viewed as a Cross-Functional Need ............................................. 5
  2. There are Gaps in Privileged Account Coverage, but Companies are Concerned about Costs ...... 5
  3. Privileged user risk is expected to increase ......................................................................................... 6
  4. Need for Greater Accountability over Privileged Passwords ................................................................. 7
  5. Inadequate Controls Over Business-Critical, Tier-1 Applications ....................................................... 7

Best Practices for Managing Privileged Accounts ....................................................................................... 8
  1. Assemble Cross-Functional Teams to Address Privileged Account Management ............................ 8
  2. Deploy Policies for Controls And Enforcement ..................................................................................... 8
  3. Prioritize Implementation by the Consequences of a Breach ................................................................. 8
  4. End-User Privileges are a Good Starting Point to Address Gaps ......................................................... 9
  5. Address the Risk of Privileged Password Misuse ................................................................................. 9

How to Get Started .............................................................................................................................................. 10

About BeyondTrust ............................................................................................................................................. 11
PRIVILEGE gone WILD 2

Risk is increasing
84%

of respondents believe that the risk to their organizations from privileged users will increase over the next few years.

Why do they believe this?

47% of respondents reported that users in their organizations possess unneeded privileges not necessary for their roles.

50% of respondents indicate that shared privileges are managed "individually." And 34% are managed locally.

60% of organizations have critical kerberized applications running on Unix or Linux platform, but more than 72% have few if any tools or processes in place to protect against privilege misuse.

Cost is a concern

Respondents are overwhelmed by the cost of solutions like those from CyberArk, DelphiQuest and CA.

What’s most at risk?

42% of Business information, including corporate intellectual property, source code, design documents, trade secrets, and compliance-related data such as PII.

Long Way to Go

ONLY 30% of organizations have a solution in place, and most haven’t deployed globally.

Looking to mitigate your privilege account management issues?

BeyondTrust helps customers:

Reduce risk by delivering an end-to-end PAM scenario, closing gaps in coverage.

Reduce total cost of ownership, speeding and simplifying global deployments vs. CyberArk, DelphiQuest and CA.

Reduce complexity by unifying privileged account management capabilities into a single platform, meeting the needs of multiple stakeholders including Ops, Security and Compliance.

Source: BeyondTrust Privilege Gone Wild 2 – a survey of 726 IT decision makers.
Privilege Gone Wild: The State of Privileged Account Management in 2015

Each year, BeyondTrust conducts a survey to identify trends in the privileged account management market. The survey explores how organizations view the risk from privileged account misuse (malicious or inadvertent), as well as trends in addressing and mitigating the risks. Over 700 information technology professionals participated in the 2015 survey, representing organizations in retail, government, education, manufacturing and technology markets.

Privileged account management was particularly important to organizations participating in the survey this year. You don’t have to look much further than the Sony breach and other recent data breaches to understand why. Data from the 2014 Verizon Data Breach Investigations Report supports this, identifying the use of stolen credentials as the most prevalent attack vector. From an adversary’s standpoint, stolen credentials are the perfect vehicles from which to execute an attack. They provide access to an organization’s sensitive data and a means to move undetected within the corporate network. If the credential’s owner is an executive, system administrator, or other user with elevated privileges, the attacker can access almost any system or data in the organization – or install malicious software to advance his attack.

However, stolen credentials are not the only risk from elevated privileges. Malicious insiders may use their privileges to access, share or steal sensitive data. Inadvertent abuse is also a concern. Employees with elevated privileges may access sensitive data out of curiosity, move data to unauthorized cloud storage for use off-network, or install unauthorized software such as file sharing applications that put data at risk.

User and account management is information security at its most basic level. The concept of “least privilege” states that users should have the lowest level of access privileges required to effectively conduct their jobs. However, many basic operating system, management, application, and software functions (e.g., configuration utilities) require more than basic privileges. Traditionally, these functions require end users to possess elevated privileges in the form of an administrative username and password. Best practices provide users with unfettered access to the data and programs required for their jobs, while preventing other actions that might introduce risk to the organization.
Survey Results

Security, compliance, and IT operations professionals were surveyed in January 2015. Over 700 responses were received, covering industries including defense, government, retail, education, manufacturing, and technology.

As one might expect from such diverse industries, opinions differed on many of the particulars about the need, deployment, and rollout of privileged account management. Despite their many differences, five key points came through across all segments:

1. Risk is Recognized, and Control is Viewed as a Cross-Functional Need

While security teams drive privileged account management purchases in 82% of respondent companies, privileged account management risk crosses functional boundaries. Privileged users may access systems with personally identifiable information (PII) or credit card information subject to PCI-DSS standards. IT is responsible for maintaining these systems, and Security is responsible for the integrity of the information. It therefore makes sense that compliance (57%) and operations (43%) are also involved in decision-making and management. It is also encouraging to note that over 82% of the respondents report that their organizations’ IT operations and security teams “work well together.”

With multiple stakeholders, the ability to view the information needed for each role in the organization is critical. Unified reporting was cited as a critical feature by 56% of the respondents. However, this has not been followed in practice. Of those organizations that have deployed privileged account management solutions, over half (53%) have two or more discrete solutions.

The recognition of risk is also reflected in the fact that over 30% of the organizations surveyed expect to deploy new privileged account management technology in 2015. Password and server security top the list of priorities (at 29% and 26%, respectively), with desktops close behind at 20% of the organizations.

2. There are Gaps in Privileged Account Coverage, but Companies are Concerned about Costs

While their intentions are good, many organizations have some work to do. Over 47% of the respondents reported that users in their organizations possess elevated privileges not necessary for their roles, and 20% report that over ¾ of their user base run as administrators. One third (33%) of the organizations participating in the survey report having no policies (much less, controls) for privileged password management. This may be a cultural
phenomenon within these organizations, eliminating restrictions on how employees manage personal devices or on the type of software installed. This policy choice greatly increases the organization’s attack surface across which malicious or accidental breaches can occur.

The remaining 67% have implemented privileged account management policies. However, enforcement of those policies remains problematic, as 60% believe their users can circumvent the controls in place.

The perceived cost of purchasing, implementing and managing the privileged account management solutions may be a deterrent to faster adoption. Respondents cited CA, Dell, and CyberArk as having the highest perceived price.

3. Privileged User Risk is Expected to Increase

Organizations are planning to implement privileged account management programs at an increasing level. The reason appears related to the anticipated risk. 84% believe the risk to their organizations from privileged users will increase over the next few years.

The greatest perceived risk is business information, including corporate intellectual property, source code, design documents, trade secrets, and compliance-related data such as PII (42%). This makes sense given the increase in media coverage of corporate espionage, which is typically viewed as a risk from insider abuse. Customer information, including personal information used in identity theft, and credit card information subject to PCI regulations, are cited by 32% of the respondents.

The respondents overwhelmingly believed that risk is not restricted to deliberately malicious activity. Most (79%) believe privileged users access sensitive and confidential information out of simple curiosity. While these actions may not result in data loss, they can nonetheless result in regulatory non-compliance.
4. Need for Greater Accountability over Privileged Passwords

The survey shows that organizations believe there is an opportunity to improve their controls over privileged user accounts. These users are often managing IT resources and require root privileges to administer servers, routers and other devices.

The common method for managing privileged accounts is through shared passwords. Just over half (51%) of the respondents state 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.

5. Inadequate Controls Over Business-Critical, Tier-1 Applications

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 e-commerce data, ERP systems managing employee data, customer information, and sensitive financial data.

For those systems (for example Linux and UNIX servers), 58% of the respondents believe their current controls against misuse are inadequate, immature or non-existent. Clearly, addressing this shortcoming should be a priority for these organizations.

How well protected against privilege misuse are tier-1, business critical systems?

- Well protected: 42%
- Not well protected: 32%
- No protection: 26%
Best Practices for Managing Privileged Accounts

To overcome these challenges, consider the implementation of the following best practices.

1. Assemble Cross-Functional Teams to Address Privileged Account Management

Managing and monitoring privileged users is a task that crosses functional boundaries. While many super users and system administrators may reside in IT operations, normal checks and balances would dictate that security groups provide oversight. Reporting requirements also differ between groups. IT operations will audit their own actions; Security will require reporting, auditing and alerts for anomalous behavior; and Compliance requires data for regulatory audits.

It is important to remember that privileged user accounts may not be restricted to internal users. Vendors may require access to your systems (as was the case with the HVAC vendor responsible for the initial Target breach), and contractors who manage their own devices may connect to your network as well.

By including all stakeholders in the selection, implementation and management of privileged user accounts, organizations also have the opportunity to enhance the relationships between these groups, and reporting and analytics needs can be identified early.

2. Deploy Policies for Controls And Enforcement

It is clear that privileged user account policies should be in place in all organizations. However, efforts may be wasted without controls that enforce those policies. Not all breaches of policy will be malicious, but inadvertent errors can still disrupt systems and expose sensitive information. A privileged account management strategy should include provisions for exception handling and workflow to allow users to perform their jobs in an unfettered manner, while maintaining centralized control over critical assets.

3. Prioritize Implementation by the Consequences of a Breach

Often, the most difficult task in managing privileged user accounts is deciding where to start. While beginning with end user accounts is good, rollouts should be prioritized based on the consequences of a breach. Factors to consider include:

- **Financial cost to business** – E-commerce and web services shared with customers are attractive targets for attackers. Taking down or compromising such a site can result in lost revenue and a damaged reputation (reducing future revenue).
- **Reputational costs** – Business partners expect that their intellectual property will be protected when shared. Data breaches resulting in the loss of that IP can affect future relationships and costs.
• **Regulatory costs** – Audits for regulatory requirements such as HIPAA, PCI, GLBA, and NERC-CIP can be difficult for any organization. Breaches can result in monetary fines in addition to business losses.

Prioritizing privileged account management implementations allows organizations to build their own best practices for deployments, including communications with affected users. It can also address internal concerns over costs, spreading the expenses associated with the deployment over time as new platforms are added.

4. **End-User Privileges are a Good Starting Point to Address Gaps**

As seen in the survey results, many organizations do not manage the privileges of any end users. A discovery exercise to identify all the privileged accounts in the organization can provide a baseline. The population of unmanaged end users is an ideal starting point at which to deploy a single solution to address a very large attack vector.

The rule of least privilege offers a compelling solution for security deployments. The majority of users do not typically require the ability to install their own software or make changes to system properties. Providing them with this ability can lead to, at a minimum, inadvertent errors and increased demand on internal IT help desks. Worse, it provides opportunities for malicious employees, or attackers who have compromised employee credentials, to steal sensitive information or disrupt network operations.

5. **Address the Risk of Privileged Password Misuse**

Create and enforce policies for the use of privileged passwords. The rule of least privilege means that users are provided the privileges they require to do their jobs, period. Unsupervised use of privileged accounts, through shared passwords or ad hoc policies, makes it impossible to control, track, or audit actions. If a breach occurs, whether deliberate or inadvertent, you need the ability to identify what happened, when, and by which user’s credentials.

Deploy controls that provide system administrators (and others) with unique, time-limited privileges that can be controlled at a granular level and monitored. Most important, maintain a detailed audit trail for spot-checking and compliance reporting. In the event of a breach, audit logs can be used for forensic analysis and accelerate incident response, limiting damages to corporate assets and brand.
How to Get Started

Privileged users play necessary role in every organization, but not all users require elevated credentials. A logical, enforceable policy for defining the required privileges for each class of users improves security by reducing the organization’s attack surface. Begin with a decision-making team that includes representatives from all affected stakeholders, then:

- **Simplify** – Look for solutions that are cross-platform and will address current and future needs. Remember to account for the reporting and auditing needs of all stakeholders.
- **Discover and Prioritize** – Understand who has elevated privileges, and target your most critical applications and users.
- **Implement** – Start with a single use case to build internal procedures. This provides a less disruptive process for rollouts and reporting before addressing the next use case.
- **Enforce** – Policies without enforceable controls do not address inadvertent errors or malicious behavior from inside or outside the organization.
- **Expand** – Remember to address internal and external users with legitimate access to your data and systems.

Finally, monitor your program and policies. Use products to discover how often users require enhanced privileges and for what purposes. This will allow you to adjust and improve policies based on empirical data within your organization.
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.
This document contains information that is protected by copyright. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of BeyondTrust.

Warranty

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

Limitations of Liability

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

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

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

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.

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