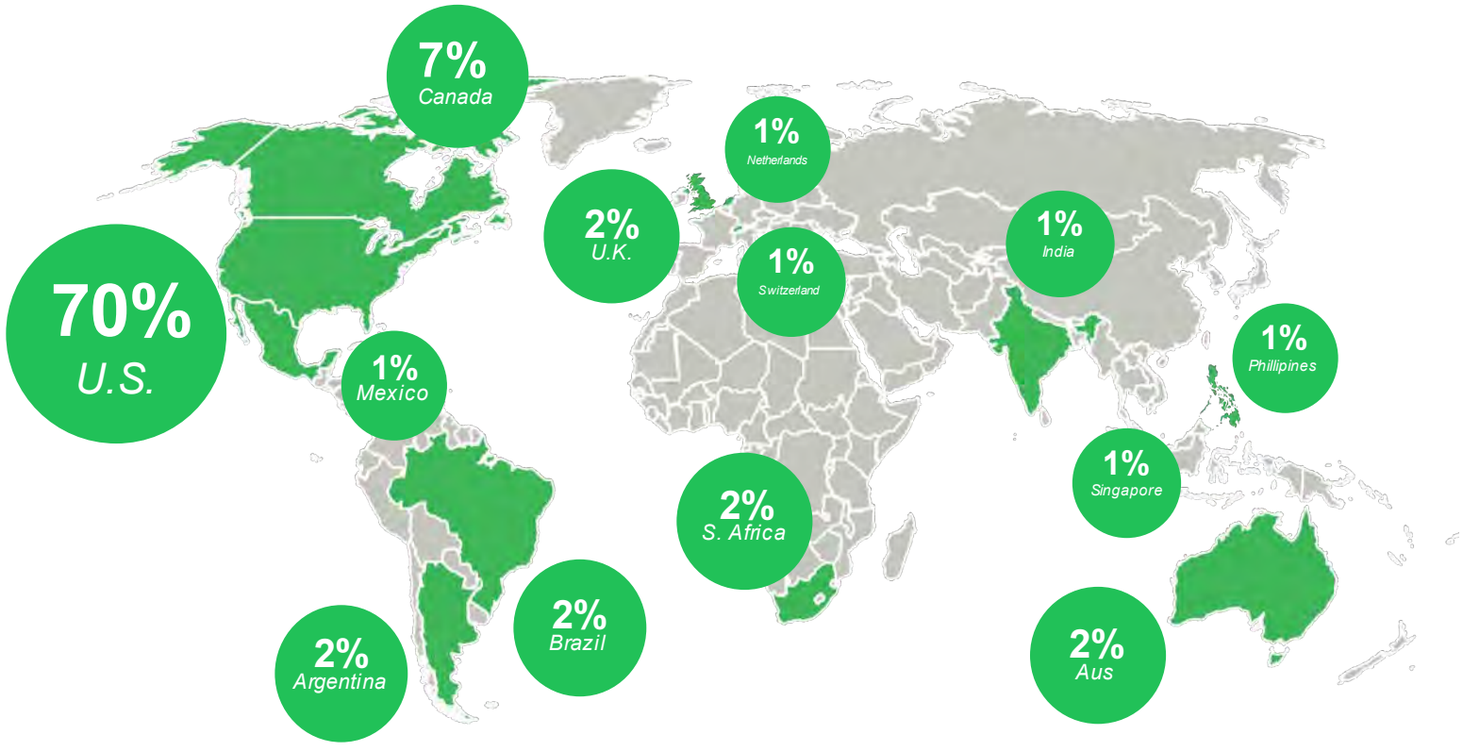
BeyondTrust

THE FIVE DEADLY SINS OF PRIVILEGED ACCESS MANAGEMENT

Introduction

For years, security experts have outlined the best practices for privileged access management in an effort to reduce problems associated with the abuse of privileged credentials. Despite this, IT organizations continue to struggle with privileged access management. Take a look inside any large enterprise and you'll likely find that passwords are still not under complete control, users with administrator privileges are still causing problems and far too many system vulnerabilities open pathways to privileged accounts.

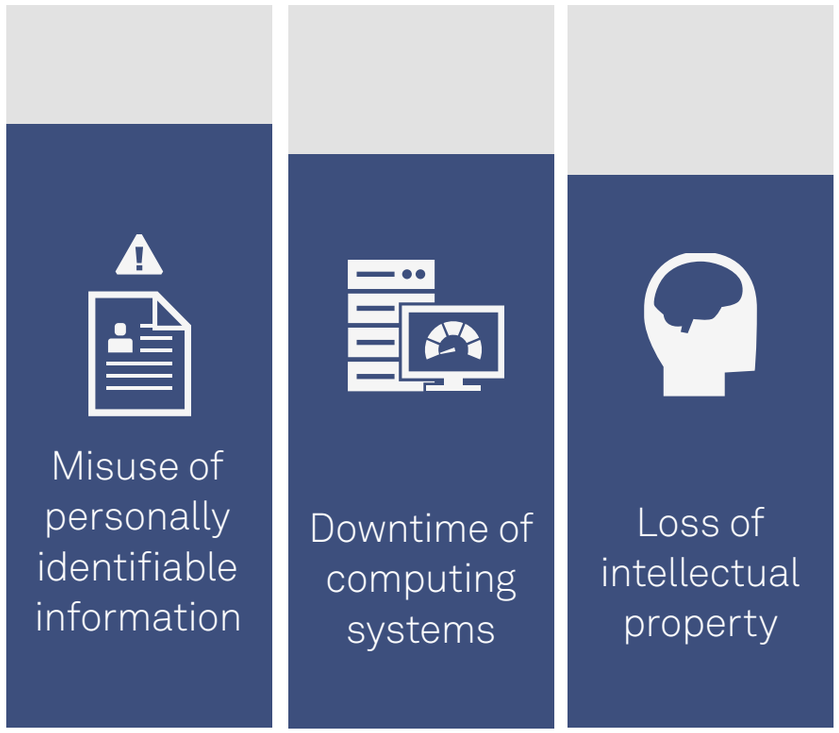


Survey Methodology

BeyondTrust surveyed 474 IT professionals from around the world with involvement in privileged access management in May and June 2017.

Why is that?

BeyondTrust decided to explore this question with our annual Privileged Access Management survey. Having analyzed the results, we've compiled a list of the Five Deadly Sins of Privileged Access Management. Think our title is too dramatic? Consider this: These five deadly sins cost the typical enterprise nearly $4M annually resulting from lost productivity, costs to mitigate incidents and legal or compliance issues.



Why We Care: Protecting Valuable Enterprise Information

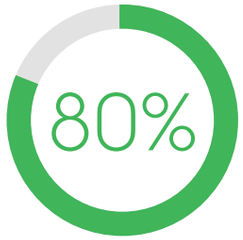
We asked respondents to list the most important enterprise assets they are protecting. The top three assets were personally identifiable information (PII), against downtime and loss of intellectual property (IP). That makes sense: As more and more enterprises engage with digital transformation crucial enterprise information becomes more valuable.

Where do we fall short?

How can enterprises protect their important digital information assets? Respondents told us the most crucial security measures are privileged account management, privileged session management and privilege elevation management. With 80% of data breaches the result of the abuse or misuse of privileged credentials[1], this is to be expected.

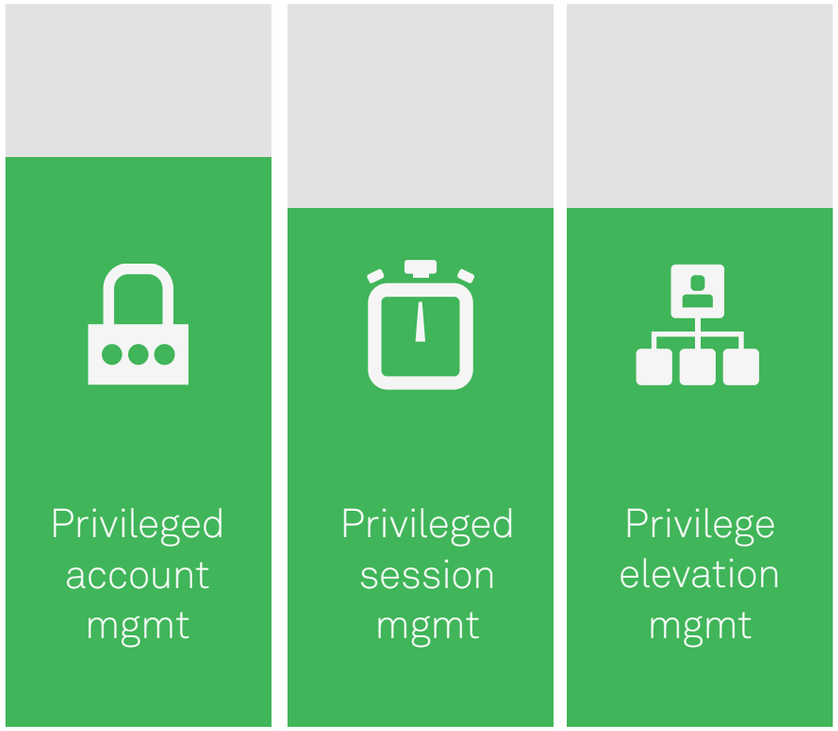
What wasn't expected was how many enterprises continue to struggle in this area. Despite their high motivation to protect enterprise information, and their laser focus on privilege access management, we identified five areas in which many enterprises continue to fall short.

What follows are the Five Deadly Sins of Privileged Access Management.



of data breaches result in the abuse or misuse of privileged credentials[1]

Aspects of privileged access management IT finds important



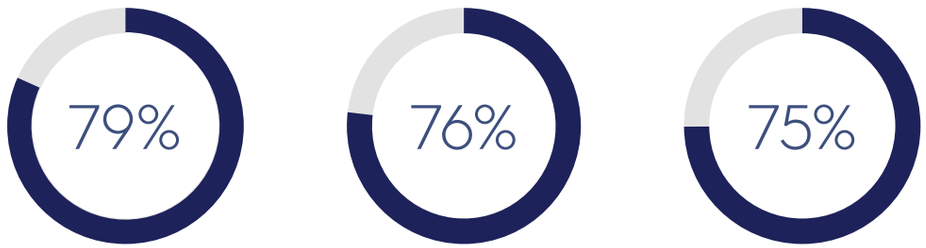
[1] **The Forrester Wave™: Privileged Identity Management, Q3 2016. Forrester. Andras Cser. July 8, 2016.**

The First Deadly Sin: Apathy

It isn't that IT doesn't know better. When asked to list the top threats associated with passwords respondents listed sharing passwords, not changing default passwords and using weak passwords. No surprises there.

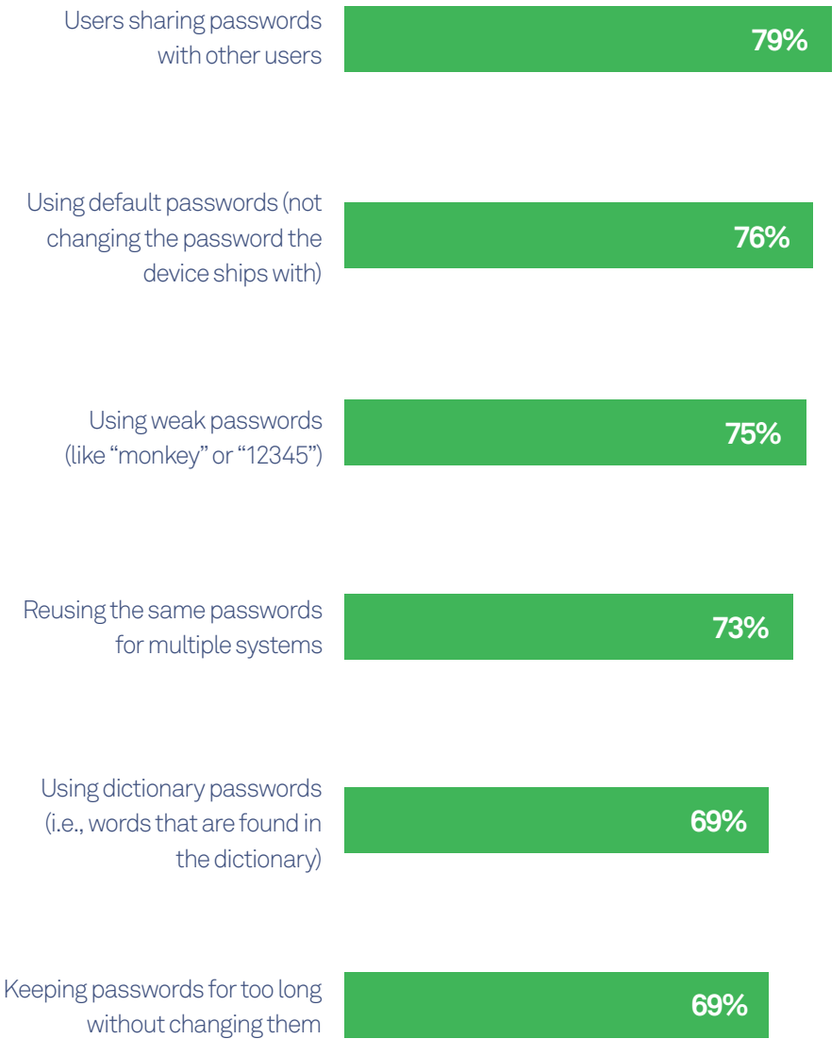
Yet despite knowing better, respondents admitted that many of these same bad practices are common within their organization. A third of the respondents report users routinely share passwords with each other, and a fourth report the use of weak passwords. Shockingly, one in five report many users don't even change the default passwords!

Regarding password practices, organizations believe the threat is high for:

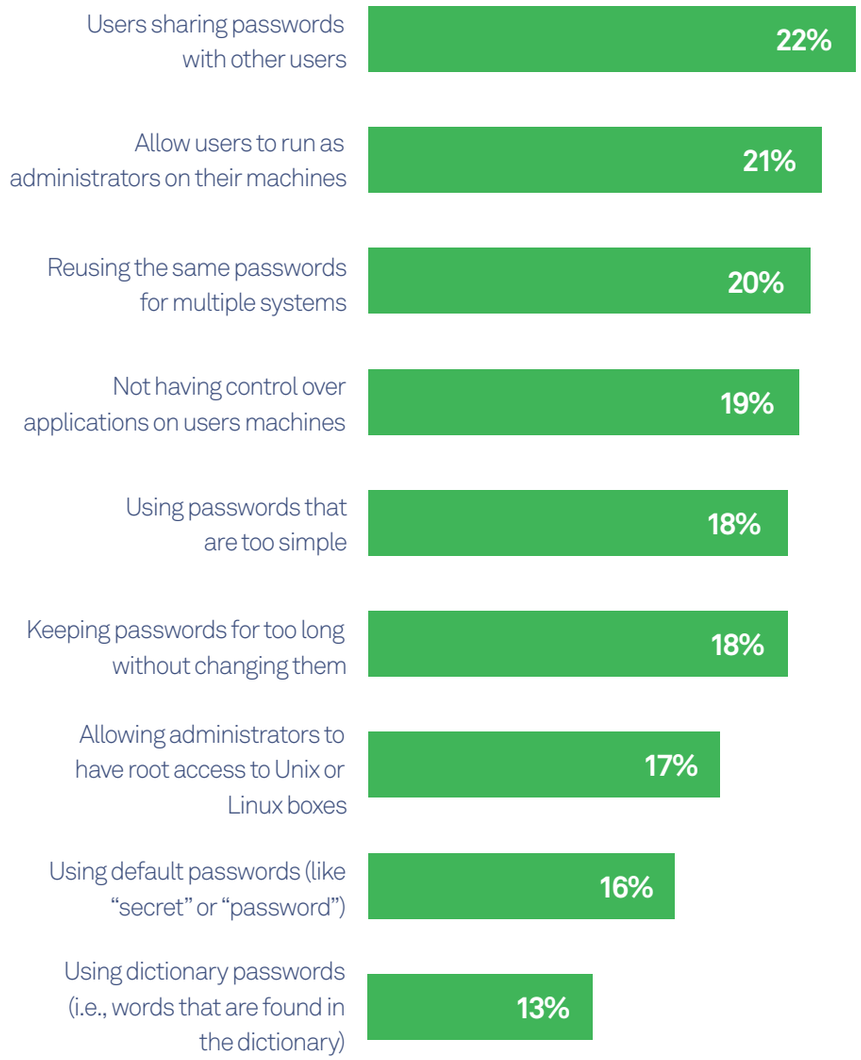


Even though the threat level is high, respondents report bad password practices still persist

Please rate the threat level from each of the following password management (Somewhat/Extremely High)



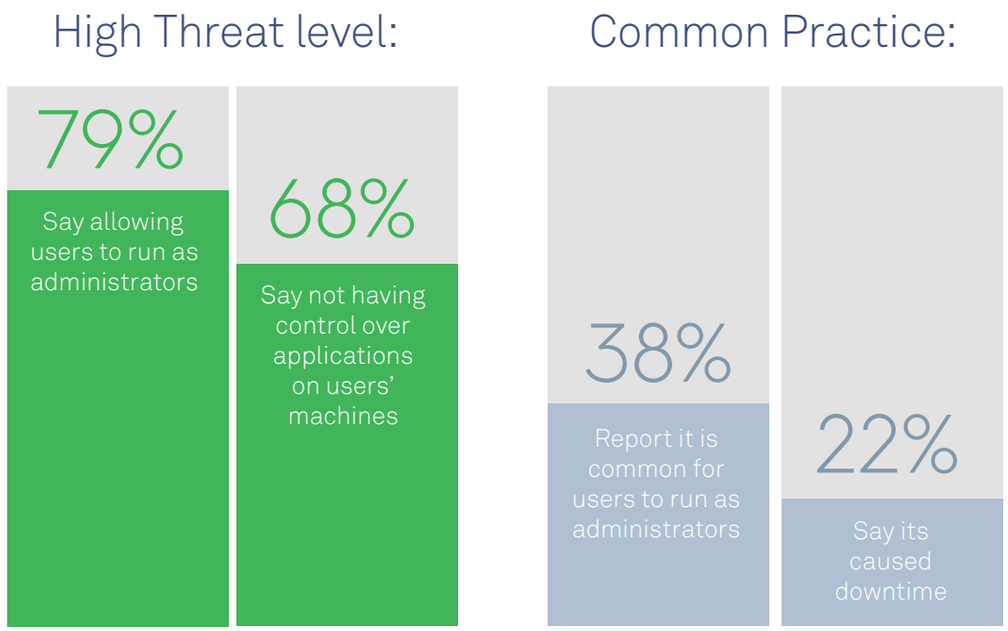
How frequently have you experienced security problems due to the following insecure practices? (Somewhat/Extremely Frequently)



The Second Deadly Sin: Greed

How much privilege does an end user really need? Users will say they need complete privilege. Yet allowing users to run as administrators on their machines is recognized by respondents as their biggest threat, followed by not having control over applications on users' machines.

Despite this knowledge, nearly two in five say it is common for users to run as administrators on their machines. It is no surprise that many respondents say these practices have directly caused downtime of computing systems.

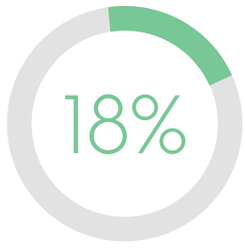


Basic security best practices should be to remove all excessive privileges

The Third Deadly Sin: Pride

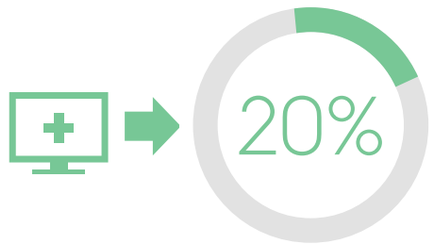
One in five respondents say attacks combining privileged access with exploitation of an unpatched vulnerability are common. These dangerous attack vectors, such as ransomware, thrive on system weaknesses and excessive access that allows lateral movement.

Simply patching known system vulnerabilities can prevent most of today's commonly-reported attack vectors. So why doesn't IT stay current on their patches? As they say, pride cometh before the fall.



Say attacks that combine privileged access with exploitation of an unpatched vulnerability are common

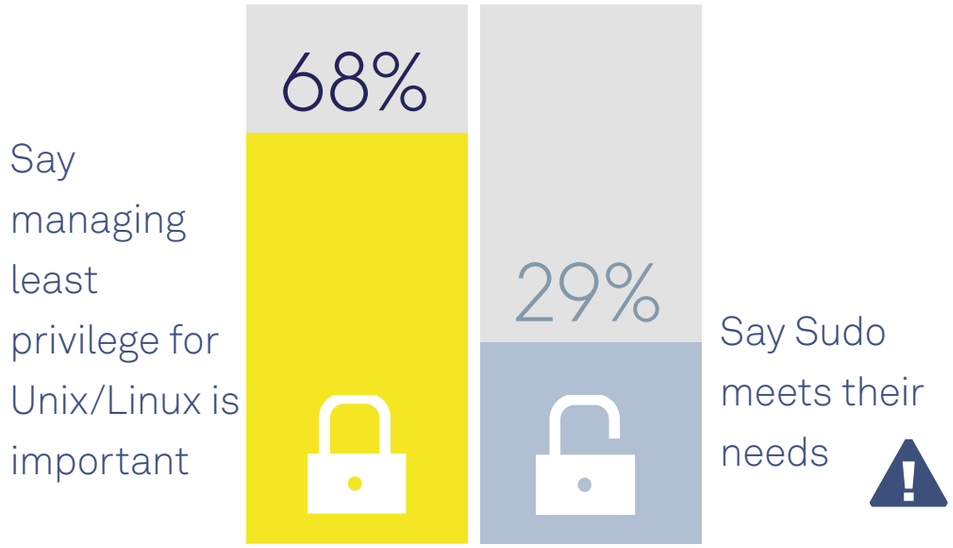
Properly patching your system can reduce your attack surface by nearly 20%



The Fourth Deadly Sin: Ignorance

Two-thirds of respondents say managing least privilege for Unix/Linux servers is somewhat to extremely important. The question is how do you manage it. One popular option is Sudo. However, just 29 percent say Sudo meets their needs. Sudo's failings as a deterrent to successful cyberattacks on Linux platforms is well-documented. Why trust the security, compliance, or continuity of your business to a free tool with known best practice flaws? The most commonly cited problems with Sudo include being time-consuming to use, complexity and poor version control.

Despite this, the typical respondent runs Sudo on 40 workstations and 25 servers.



The Fifth Deadly Sin: Envy

Organizations are moving to the cloud with a vengeance. As with all platforms, protecting against privileged access abuse is crucial for cloud workloads. Unprotected SaaS workloads can lead to a host of problems; some immediate, some longer lasting.

Yet, more than a third report that they are not involved in protecting SaaS applications from privileged access abuse. It is not up to the provider to protect your cloud workloads, it is up to IT. Privileged access must be secured consistently across all channels – on-premises, IaaS, SaaS and PaaS.

37%
not involved in protecting SaaS applications

63%
report protecting SaaS Applications

Privileged access must be secured consistently across all channels

Where to go from here

Personally Identifiable Information (PII) must be protected at all costs, otherwise organizations can face costs of up to $4 million per year mitigating the damages of unwanted access to it. To protect access to this data, organizations tell us that they must protect privileged accounts (but it's done inconsistently), remove admin rights from users (well, most of them anyway), tackle the vulnerabilities that can be used to exploit elevated privileges (sorta), take control over Unix and Linux accounts (sudo), and prioritize the protection of vulnerable SaaS privileges (or not). How do organizations finally, once and for all, implement these measures? We'll cover that next.

Battling the Five Deadly Sins

Below are five steps you can take today to reaffirm that you believe in privileged access management:

1. Deploy enterprise password management globally across all data centers, virtual and cloud.
The data from the study reveals that there is still quite a bit of work to do to get control of enterprise credentials. Namely, eliminating the sharing of credentials and getting control over embedded credentials hardcoded in applications and service accounts. A centralized password management solution that includes built-in session monitoring will ensure that both important capabilities are met with strong workflow and ease of use for your high-maintenance users.

2. Remove local admin rights from ALL Windows and Mac end users immediately.
94% of Microsoft system vulnerabilities in 2016 can be attributed to users with admin rights. Once all users are standard users, IT teams can elevate a user's access to specific applications to perform whatever action is necessary as part of their role without elevating the entire user on the machine. The benefit? When the next ransomware variant breaks out, your end-users' machines will be contained, preventing further propagation. It will save your IT team and help desk many headaches, and save the business from possible downtime. As well, you can use asset and application vulnerability insights to help you make better decisions on elevating privileges.

3. Prioritize and patch vulnerabilities.
Consider the cyber-attack chain. Attackers exploit asset vulnerabilities, hijack elevated privileges or compromised credentials, and move laterally until they achieve their objective. What's the first step in that chain? Right. Vulnerabilities. Like we mentioned above, better prioritization and patching of vulnerabilities gives you better insight into whether to delegate privileges to an asset or application. The result is better intelligence and less risk of unknowns.

4. Replace sudo for complete protection of Unix/Linux servers.
With pressure on budgets, organizations may have to use sudo, but it doesn't offer the industrial-strength capabilities that today's security needs, for example:

- Analyzing user behavior by correlating keystroke logs, session recordings and privileged events against asset vulnerability data and security intelligence from best-of-breed security solutions
- Elevating privileges for standard users through fine-grained, policy-based controls
- Utilizing contextual factors such as time, day and location to make privilege elevation decisions
- Auditing and reporting on changes to critical system, application, and data files
- Achieving policy-driven command control and auditing – down to the system level
- Enabling a host-based and/or proxy-based approach to privilege management
- Unifying policy, management, reporting and analytics, upgrades and more across all privilege management systems

5. Unify privileged access management – on-premise, in the cloud – into a single console for management, policy, reporting and analytics.
As organizations race to adopt *aaS to keep pace with business demands, IT must provide the same level of protection to cloud-based systems as for on-premise systems. This includes capabilities such as:

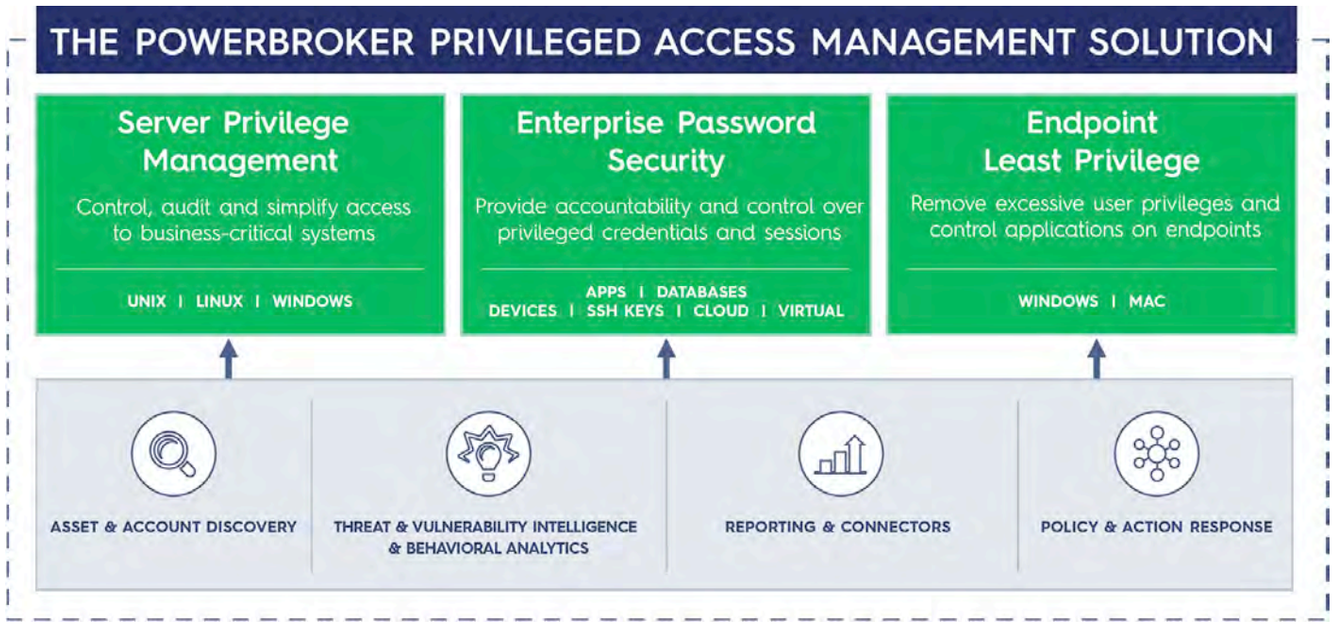
- Enabling automation for DevOps
- Finding, grouping and scanning cloud assets
- Protecting virtual and cloud management consoles and instances
- Using a cloud access service broker to enable third-party access
- Performing vulnerability assessments for hybrid and public cloud infrastructures

The trick, though, is to secure and enable the cloud without gaps – in effect unifying your privileged access policies across on-premise and cloud environments.

Why BeyondTrust?

BeyondTrust delivers what leading industry analysts including KuppingerCole, Forrester, Gartner and Quadrant Research 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 to provide 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 that many alternative providers offer as disjointed tools, the PowerBroker platform simplifies deployments, reduces costs, improves system security and closes gaps to reduce privileged risks. Nearly 4,000 customers worldwide are using PowerBroker every day 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



For more information on how BeyondTrust can help you repent your security sins and be reborn as a Privileged Access Management Saint, contact us at www.beyondtrust.com

THE 5 DEADLY SINS
of Privileged Access Management

Security experts have outlined the best practices for privileged access management for years in an effort to reduce problems associated with the abuse of privileged credentials. Despite this, IT organizations continue to struggle. BeyondTrust decided to explore this issue with our annual Privileged Access Management survey.

What keeps IT awake at night?

- Misuse of personally identifiable information
- Downtime of computing systems
- Loss of intellectual property

Aspects of privileged access management IT find important

- Privileged account management
- Privileged session management
- Privilege elevation management

Enterprises continue to struggle despite their motivation to protect enterprise information

1 APATHY: Not deploying privileged password management

Organizations believe the threat is high for:

- 79% Sharing passwords
- 76% Using default passwords
- 75% Using weak passwords

22% of respondents report bad password practices still persist

2 GREED: Too many holdout admin users

High Threat Level:

- 71% Say allowing users to run as admins
- 68% Say not having control over applications on users machines
- 38% Report it is common for users to run as admins
- 22% Say allowing it has caused downtime

Common Practice:

Basic security standards should be to remove all excessive privileges

3 PRIDE: Ignoring risks of excessive privileges

18% Say attacks that combine privileged access with exploitation of an unpatched vulnerability are common

20% Properly patching your system can reduce your attack surface by nearly 20%

4 IGNORANCE: Believing Sudo is enough

Say managing least privilege for Unix/Linux is important: 68%

29% Say Sudo meets their needs

5 ENVY: Ignoring SaaS risks

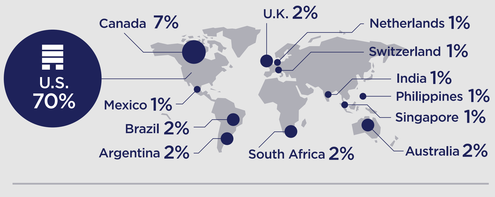
37% Not involved in protecting SaaS application

63% Report protecting SaaS applications

Privileged access must be secured consistently across all channels

Who We Talked To

Main Office location

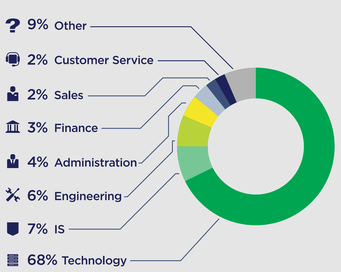


474 responses

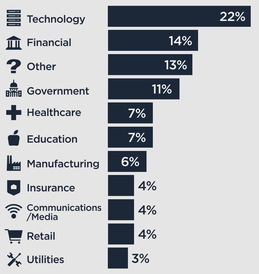
conducted May-June 2017

23 questions

Departments



Industries



For more information, including 5 steps you can take to reaffirm that you believe in privileged access management, download our free report.

DOWNLOAD REPORT

www.beyondtrust.com/5-sins-pam

Source: BeyondTrust 2017 Privilege Benchmarking Study

BeyondTrust