the STATE of ★★ PAM ★★ SECURITY

FAILURE TO SECURE:

The 2016 State of Privileged Account Management Report

Co-sponsored by Thycotic and Cybersecurity Ventures

550+ organizations benchmarked their privileged account management score. Of them, 80% consider PAM security a high priority, but, 52% received a failing grade.

Learn about the top PAM challenges of 2016 in this comprehensive report.

thycotic

CYBERSECURITY VENTURES

TABLE OF CONTENTS

FAILURE TO SECURE:

THE 2016 STATE OF PRIVILEGED ACCOUNT MANAGEMENT REPORT

EXECUTIVE SUMMARY

Global Survey shows Privileged Account Management is a Top Security Priority, but Failing in Enforcement

This report describes the latest results from a groundbreaking global benchmark study by Thycotic that reveals several security gaps in how organizations manage and secure their privileged account passwords and network access. The 2016 State of Privileged Account Management Report highlights the major areas of concern and provides recommendations for how to address the most common shortcomings in PAM security.

Here's the Challenge

Launched in early 2016, the Thycotic Privileged Password Vulnerability Benchmark survey has engaged more than 500 IT security professional participants to date from around the globe. Results from the survey indicate a growing awareness among organizations of the importance of securing privileged credentials throughout the enterprise.

80% **Consider Privileged Account Management (PAM) security a high priority**

60% **Indicate that PAM security is required to demonstrate compliance with government regulations**

However...

The study also shows that far too many organizations fall short when it comes to adopting and maintaining best practices in the protection of privileged account credentials.

30% **Of organizations have not communicated the importance of following IT security policies to their stakeholders**

66% **Still rely on manual methods to manage privileged accounts**

10% **Have implemented an automated security vendor solution**

EXECUTIVE SUMMARY

Significant Security Gaps Indicated by Research Results

Even more alarming are survey results that reveal serious gaps in the enforcement of basic security measures when it comes to securing privileged account credentials:

20% of organizations

have never changed their default passwords on privileged accounts

30% of organizations

allow accounts and passwords to be shared

40% of organizations

use the same security for Privileged Accounts as Standard Accounts

70% of organizations

do not require approval for creating new Privileged Accounts

50% of organizations

do not audit privileged account activity

Why It's Important

The results of this landmark survey suggest many organizations throughout the world need to take action immediately to improve security practices associated with privileged account management. This report provides a compelling case for making privileged account management security an urgent priority. Because privileged account passwords and access are a prime target for hackers and one of the biggest cybersecurity risks for breaching the defenses of any organization, it is imperative that we work together to achieve better privileged account protections.

> **63% of confirmed data breaches involved leveraging weak/default/ stolen passwords."**
>
> - 2016 Verizon Data Breach Investigations Report

> **90% of Advanced Persistent Threat breaches involve stolen credentials."**
>
> - Mandiant

WHAT CAN YOU DO ABOUT IT?

The 2016 State of PAM Report provides several recommended actions to help secure privileged credentials throughout the enterprise. These recommendations represent a cross section of best practices for PAM security generally accepted by experts and analysts in the industry.

Step 1: Educate Key Stakeholders

Educate key stakeholders in your organization about the urgency and value of Privileged Account and Access Management Security. You can use the 2016 State of PAM report executive summary as a starting point to get their attention.

Take the survey yourself to see how your current PAM practices compare with others, and share the results along with specific recommendations to address issues you've identified within your organization.

Step 2: Discover Privileged Accounts

Discover where your privileged accounts are located across your entire enterprise environment. You can't protect what you don't know exists. There are free tools you can use to discover where your privileged accounts are located for both Windows and Unix environments.

Step 3: Automate the Management and Security

Automate the management and security of privileged account passwords. It's shocking that 6 out of 10 organizations, according to the report, still use manual methods such as spreadsheets and lists to keep track of privileged account passwords. There are affordable PAM solutions available for any size organization and you learn more about the top five tasks you can automate in this free eBook.

Step 4: Adopt and Implement Security Policies

Adopt and implement security policies to help ensure least privilege strategy for account access. Too many accounts have been granted broad and deep privileges, and if only one of these accounts is compromised, it can quickly be used by an attacker to exploit your entire IT infrastructure. You should explore employing software tools to limit privileged access without impacting user productivity.

Step 5: Provide Greater Visibility

Provide greater visibility in PAM for CISOs while helping to assure you can demonstrate compliance with audits and policies affecting privileged account credentials. You can get a **free template for best practice privileged account security policies** as well as PAM software to help automate and enforce those policies to improve security and satisfy auditors.

PART 1: RECOGNIZING THE SPECIAL THREAT TO PRIVILEGED CREDENTIALS

Why Privileged Accounts Make an Attractive Target

A privileged account is an account used by IT Security and Operations administrators to access or logon to laptops, desktops, servers, switches, firewalls, routers, applications, and/or database servers. Privileged accounts are necessary to enable IT staff to manage, configure, troubleshoot, or perform maintenance tasks. In larger organizations there can be hundreds if not thousands of these accounts across the enterprise in any number of locations.

Many privileged accounts are machine-to-machine accounts that allow applications to communicate to dependent services or systems to perform their tasks. Almost all of these accounts come with basic or simple default accounts and passwords that when left unmanaged pose a major security risk.

Hackers Target Privileged Accounts To Gain Unfettered Access

Hackers are targeting privileged account credentials for good reasons. The past year has been busy for cyber criminals, with public reports describing more than 500 data breaches and more than 500 million records exposed in 2015. This includes the disclosure of 21 million U.S. Office of Personnel Management records, 70 million medical records at Anthem, and 37 million user details at Ashley Madison. The healthcare, retail, technology, financial, and governmental sectors head the list of business areas that were the most targeted throughout the year.

In the vast majority of breaches, stolen credentials and privileged accounts continue to be the prime target for hackers because they unlock the access required to exploit virtually any part of an organization's network, including critical and sensitive data. Hacking privileged credentials can mean the difference between a simple perimeter breach and one that could lead to a cyber catastrophe. Once attackers gain access, they can escalate their privileges and move through networks to identify and compromise confidential information or use ransomware to encrypt critical business data.

Hijacking the privileged credentials of an authorized user, an attacker can easily blend in with legitimate traffic and be extremely difficult to detect. This makes it more difficult for organizations to detect a breach in which the average dwell time today is more than 200 days meaning that most breaches go undetected for many months. In almost all Advanced Persistent Threats and major data breaches, compromised accounts have been the target of many of the bad actors.

Privileged Account Management Security Provides Proven Protection

Privilege Account Management security offers mission-critical solutions to protect privileged credentials from unauthorized access and misuse. It helps assure that if and when perimeter defenses are breached, privileged account controls will act to limit access to sensitive information and curtail an attacker's ability to circulate unhindered throughout the IT environment.

Privileged Account Management security provides automated tools to discover and manage accounts, determine who has access, when access occurs, how privileged accounts can be used, along with auditing, granting and revoking access, as well as the regular rotation of passwords. In the event of a breach, for example, recently used accounts can be quickly randomized to lock down the environment and enable additional security layers to protect privileged accounts.

1. **A compromised privileged account is the difference between a perimeter breach and a cybersecurity catastrophe.**

2. **It only takes one compromised privileged account for an attacker to perform malicious activity.**

Why A Privileged Account Benchmark Study Now?

Over more than a decade of helping companies to manage privileged account passwords, Thycotic observed that many organizations failed to completely understand the current state of their privileged accounts and the major risks associated with those accounts. In our experience, there are a substantial number of rogue privileged accounts that continue to remain hidden, unknown and therefore unmanaged—posing a major cybersecurity risk. In addition, we've found that many organizations frequently do not retire privileged accounts when they are no longer needed, and in many cases have never changed the default passwords on third party accounts.

Half of organizations do not audit privileged account activity

To verify the accuracy of these impressions, Thycotic developed a global Privileged Password Vulnerability Benchmark survey. The online survey gives organizations a means to score their privileged account management practices against a best practices grading system, as well as compare their responses with those of their peers. The 2016 State of Privileged Account Management Report summarizes the findings of more than 500 participants from across the world, and provides recommendations based on those findings.

80% of organizations
consider PAM as a high security priority.

60% of organizations
face compliance requirements involving PAM security.

10% of organizations
have implemented a commercial solution.

30% of organizations
fail to educate employees on critical security policies.

20% of organizations
do NOT change default vendor passwords.

60% of organizations
MANUALLY manage privilege accounts.

30% of organizations
allow accounts and passwords to be shared.

40% of companies
use the same security for Privileged Accounts as Standard Accounts.

PART 2: ACKNOWLEDGING THE IMPORTANCE OF PAM SECURITY CONTROLS

80% Consider Privileged Account Management (PAM) security a high priority

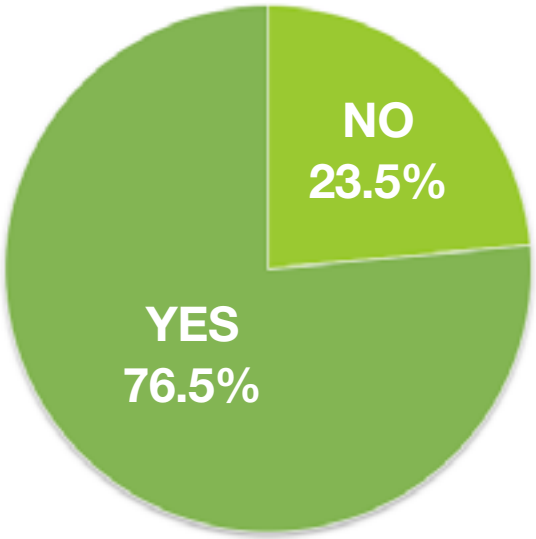
60% Indicate that PAM security is required to demonstrate compliance with government regulations

8 IN 10 ORGANIZATIONS CONSIDER PAM AS A HIGH PRIORITY TO DEFEND AGAINST CYBER-CRIME

Most respondents in our survey indicated that Privileged Account Management is a cybersecurity priority. This shows growing awareness that privilege account management is an important cybersecurity control for reducing and mitigating the impact of cyber breaches. Protecting critical assets and sensitive information as well as meeting regulatory requirements means securing access, centralizing and automating privileged account management, as well as implementing automated security controls.

FIGURE 1

Is controlling privileged users and their credentials and access a security priority for your organization?

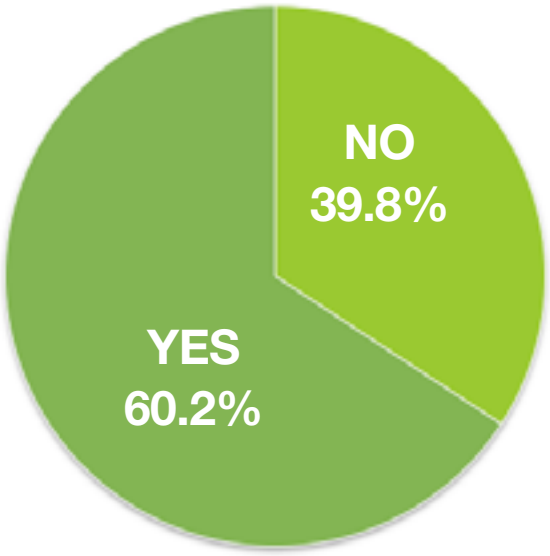


6 IN 10 ORGANIZATIONS SAY THEY MUST DEMONSTRATE COMPLIANCE & AUDITING OF PRIVILEGED ACCOUNTS

Among organizations surveyed, more than half of the respondents indicated that privileged account management is a required or regulated compliance issue within their organization or industry. While PAM security adoption is being driven by regulatory requirements, it also appears that many organizations are adopting privileged account security measures to reduce the risk of the growing cyber threats and to protect against both external and internal attacks. Thus, establishing privileged account access controls is a growing priority driven by auditors, controllers, and greater awareness of threats targeting privileged accounts.

FIGURE 2

Is privileged user management and control of privileged user passwords a compliance requirement for your organization?



PART 3: UNDERSTANDING CURRENT LIMITATIONS IN PAM FUNDAMENTALS

30% Of organizations have not communicated the importance of following IT security policies to their stakeholders

66% Still rely on manual methods to manage privileged accounts

10% Have implemented an automated security vendor solution for privileged accounts

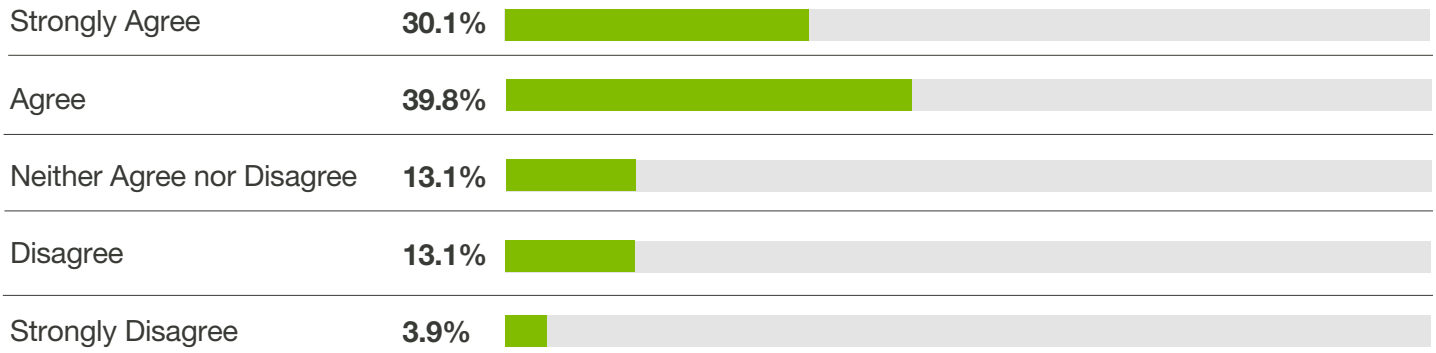
3 OUT OF 10 ORGANIZATIONS FAIL TO EDUCATE EMPLOYEES ON CRITICAL SECURITY POLICIES

With the ever growing need for cybersecurity regulations and controls, developing well-defined IT Security Policies is typically a first step for most organizations — and one that must be endorsed from the top of the organization. All employees need to recognize how their behavior affects security and therefore treat security measures as an important part of their job. But, according to our survey respondents, 4 out 10 companies fail to ensure that their IT security policies around passwords are understood by employees. This puts organizations at risk since human error or malicious intention are frequent causes of security breaches.

Ensuring that employees are well informed and that the IT security password policies are clearly communicated to employees is an obvious first step in reducing the risk against both external and internal threats against an organization.

FIGURE 3

Our organization has a password policy that is fully understood and endorsed by senior IT and business leadership who have communicated the importance of following security policies to employees.

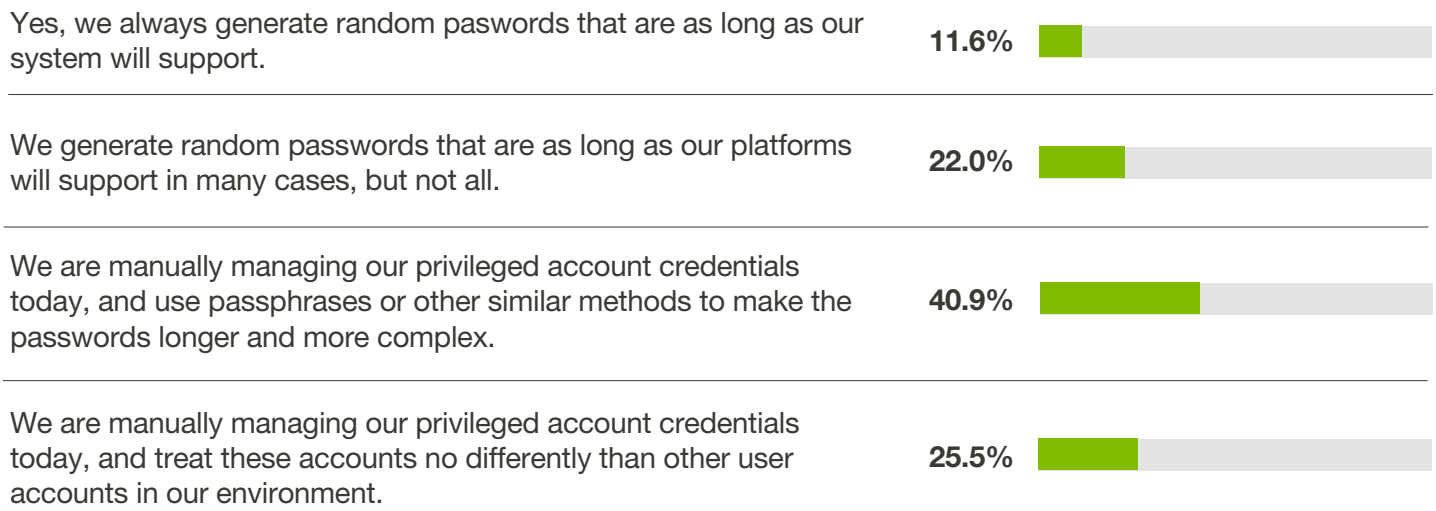


7 OUT OF 10 ORGANIZATIONS MANUALLY MANAGE PRIVILEGE ACCOUNTS

Unfortunately, a majority of survey respondents are manually managing and maintaining privileged accounts. Considering that over 60% of cyber breaches are due to human error, this creates a significant barrier to properly managing privileged account password security. In practice, mistakes and inconsistencies can easily occur in managing hundreds or even thousands of privileged account passwords.

FIGURE 4

For privileged accounts, please select all of the following that are applicable to your organization:



ONLY ABOUT 1 IN 10 ORGANIZATIONS HAVE IMPLEMENTED A COMMERCIAL PAM SOLUTION

Your privilege account management solution should:

#1 Automatically discover rogue accounts and secure them

#2 Actively audit and monitor privileged user access

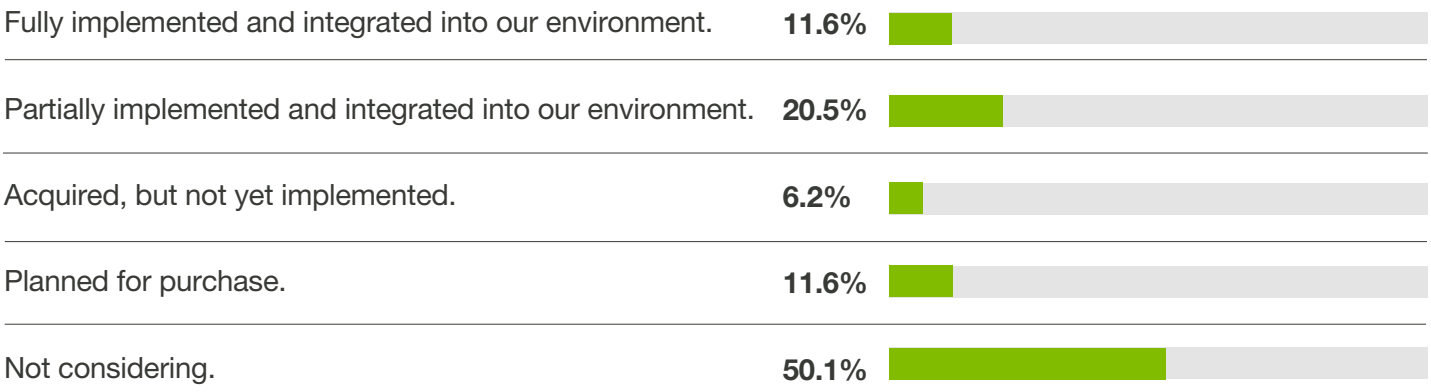
#3 Rotate passwords on privileged accounts constantly

#4 Enforce strong password policies for end users

With only 11% of organizations fully implementing a commercial PAM security solution and another 20% partially implementing security controls, nearly 70% of organizations have not implemented a solution or are using a homegrown solution. Homegrown solutions are typically manual operations that can be difficult to keep updated and/or used to demonstrate compliance with regulatory requirements. In a survey Thycotic conducted last year, 94% of hackers find privileged credentials in unprotected files such as spreadsheets, meaning that manual or home grown solutions represent a significant risk of compromise.

FIGURE 5

Does your organization have a commercial privileged account management platform in place that allows you to control passwords, create checkout policies, integrate with access to critical systems, and provide sound audit trails for all credential use?



If you don't have good privileged account management, attackers can take your credentials and start acting like a trusted user."

- Cybersecurity expert Dave Shackleford of IANS

PART 4:
IDENTIFYING MAJOR SECURITY GAPS IN PAM SECURITY PRACTICES

20% of organizations have never changed their default passwords on privileged accounts

30% of organizations allow accounts and passwords to be shared

40% of organizations use the same security for Privileged Accounts as Standard Accounts

70% of organizations do not require approval for creating new Privileged Accounts

50% of organizations do not audit privileged account activity

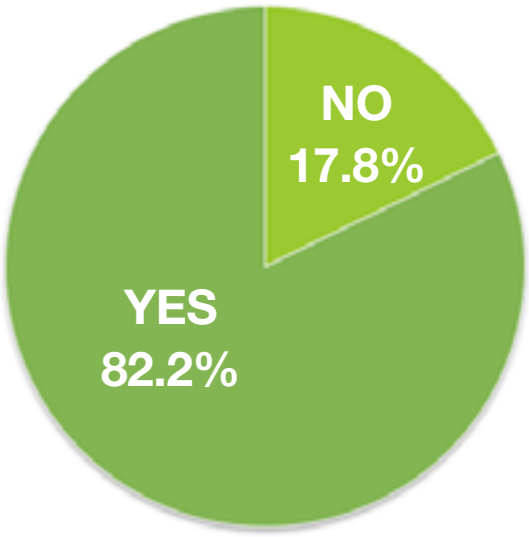
1 OUT 5 ORGANIZATIONS STILL DO NOT CHANGE DEFAULT VENDOR PASSWORDS

While many respondents are changing the default credentials of vendor-supplied accounts, almost 20% are still exposed to threats. This indicates that attackers have a 20% chance that publically available vendor passwords can be easily hacked to gain access to sensitive, proprietary data.

It only takes access to one privileged account for an attacker to perform malicious activity and go virtually undetected.

FIGURE 6

Are all vendor-supplied default passwords changed before any computer or communications system is used in production?



3 OUT OF 10 ORGANIZATIONS LACK FORMAL PASSWORD CONTROLS

Survey results show that 3 out of 10 organizations have no formal password controls in place. This poses a major security risk knowing that end users continue to use simple dictionary word passwords as well as using the same password for multiple accounts. It also means organizations are vulnerable if user passwords are compromised through personal use or duplicated in the workplace.

FIGURE 7

Top 500 Passwords

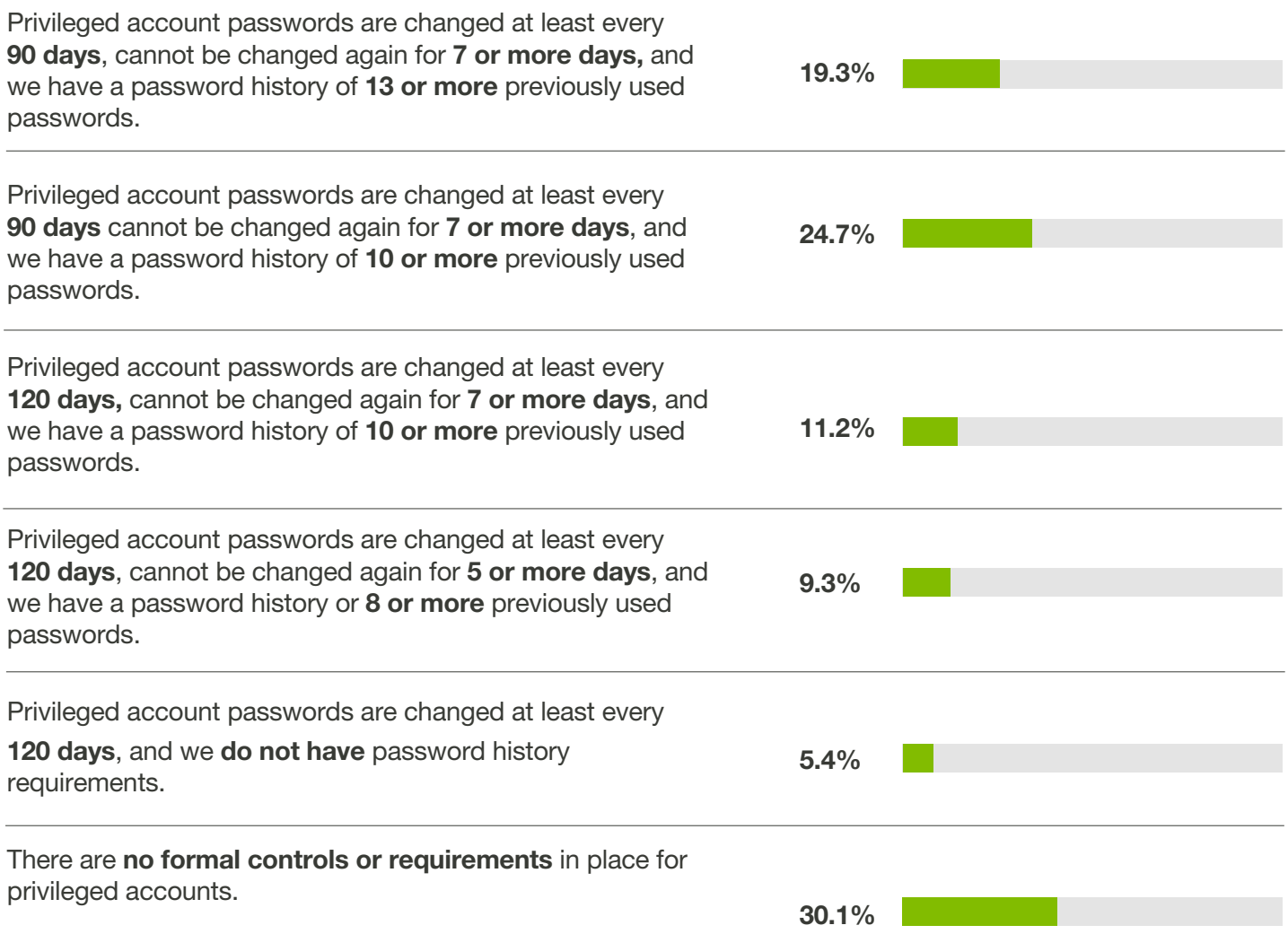
Source: http://www.informationisbeautiful.net/visualizations/top-500-passwords-visualized/

3 OUT OF 10 ORGANIZATIONS LACK FORMAL PASSWORD CONTROLS

cont'd

FIGURE 8

Please select the most appropriate set of controls you have in place regarding password changes and change history:



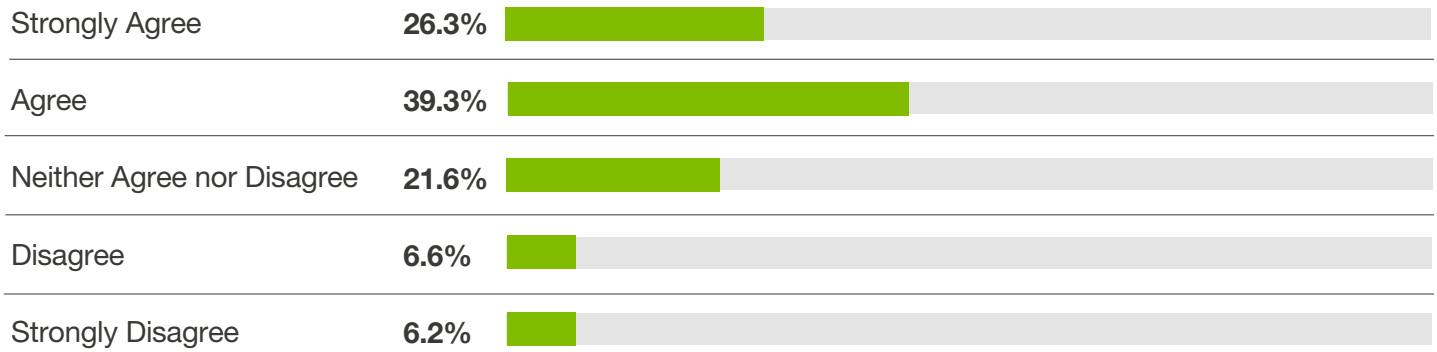
3 OUT OF 10 ORGANIZATIONS ALLOW ACCOUNTS AND PASSWORDS TO BE SHARED

About 35% of organizations do not enforce or restrict the sharing of privileged accounts. Because passwords are shared, auditing activity cannot be considered non-reputable since organizations can't identify the unique account or user initiating actions using the account. This lack of control and enforcement means the accountability of accounts is significantly reduced, and employees will be less likely to adhere to corporate IT security policies.

User passwords should not be shared in any organization. However, privileged user accounts can be shared with the proper controls in place to determine which user is actively using the account. Proper tracking and control ensures a full audit trail.

FIGURE 9

User passwords are not permitted to be shared in our organization.

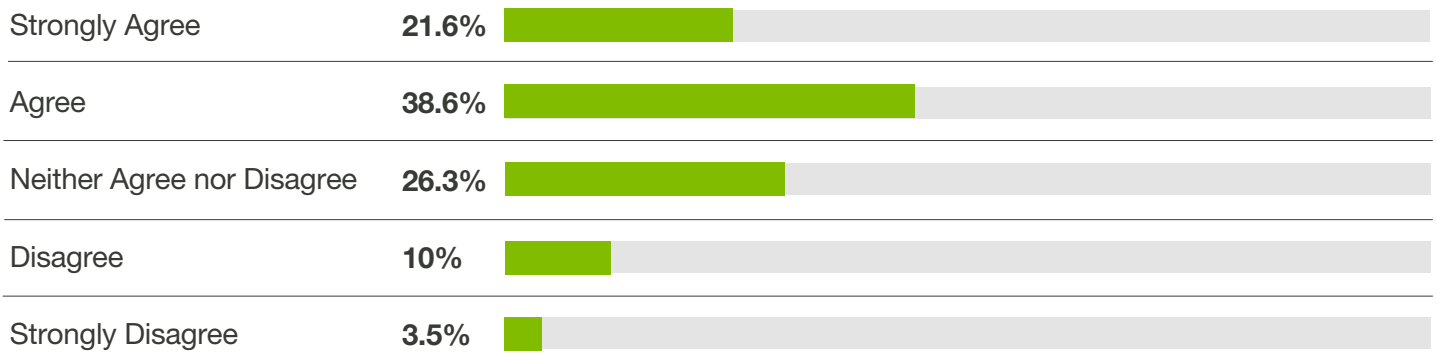


4 OUT OF 10 COMPANIES USE THE SAME SECURITY FOR PRIVILEGED ACCOUNTS AS STANDARD ACCOUNTS

It is particularly disturbing that 40% of organizations treat privileged accounts the same as standard accounts, and no additional security controls are used to manage and protect privileged accounts. This means that attackers can use the same methods used to compromise standard accounts to exploit privileged accounts.

FIGURE 10

Privileged accounts in our environment employ greater security than non-privileged accounts, including longer, more secure passwords and greater audit accountability.



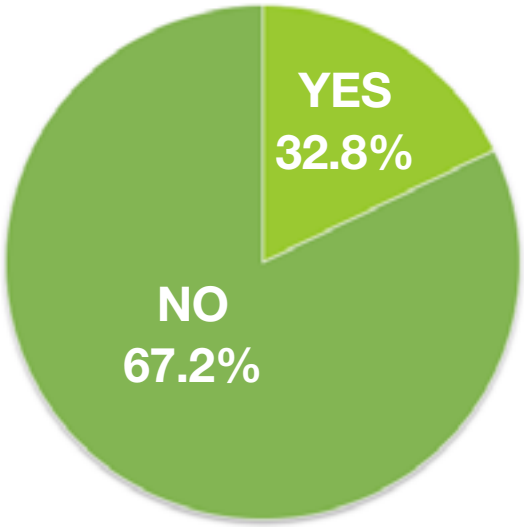
7 OUT OF 10 ORGANIZATIONS DO NOT REQUIRE APPROVAL FOR CREATING NEW PRIVILEGED ACCOUNTS

Without requiring approval for creating new privileged accounts, many organizations will continue to experience rogue privileged accounts. In many cases, organizations are unaware of hundreds or even thousands of privileged accounts throughout their network. These unknown privileged accounts include: local administrator, root accounts, domain administrator, and service accounts to name a few.

By properly discovering these accounts on a scheduled basis and automatically bringing them into a secure, encrypted vault, organizations can create an active inventory of their usage, properly vault credentials, and manage who has access to these sensitive accounts. Continuous discovery of privileged accounts should be conducted as a basic security measure if no approval process exists for organizations. This allows organizations to at least identify rogue-privileged accounts and determine if they are not required or pose a security risk.

FIGURE 11

Does your organization require multiple approvers for creation of a new privileged account?

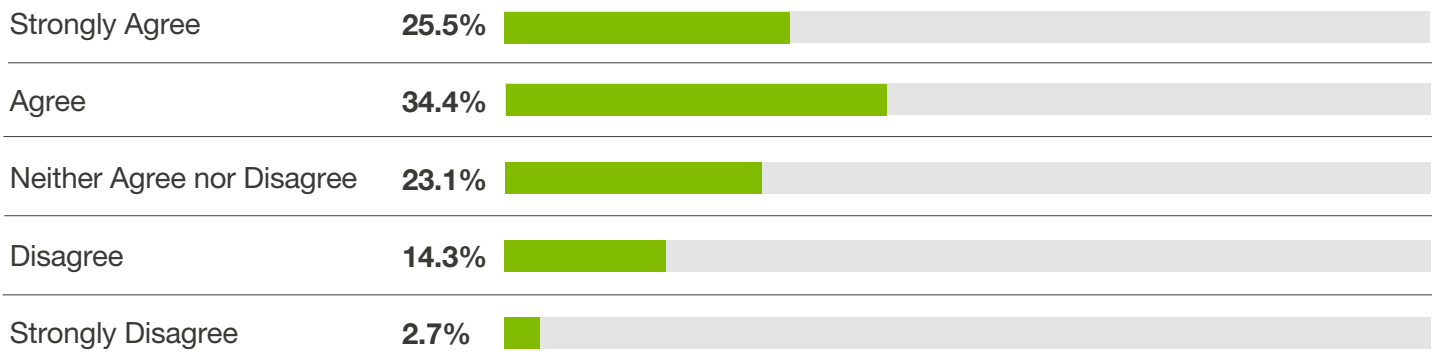


4 OUT OF 10 OF ORGANIZATIONS DON'T CHANGE GENERIC DEFAULT IDs

Unfortunately, a large percentage of companies do not modify the default generic ID's of privileged accounts. That gives any attackers 50% of the information they need to compromise an account—an unacceptable risk that can easily be remedied. Generic user IDs should never be allowed, and all user IDs should be unique and tied to a specific individual.

FIGURE 12

Generic user IDs are never allowed, and all user IDs are unique and tied to a specific individual at our organization.

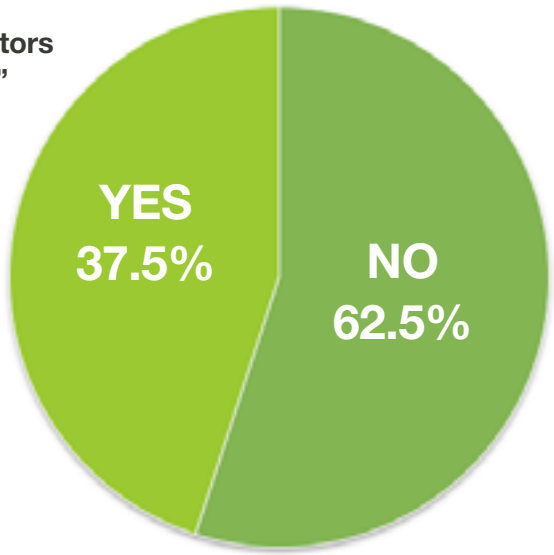


4 OUT OF 10 COMPANIES ALLOW ADMINISTRATORS TO USE THEIR PRIVILEGED ACCOUNTS TO LOG INTO ANY DEVICE, RATHER THAN LIMITING THEM TO USING A STANDARD ACCOUNT

This is an enormous but often overlooked cybersecurity risk. By not enforcing any controls over privileged accounts, organizations are exposed to much higher risk of compromise. Recent variants of malware specifically seek to exploit and compromise the privileged accounts of administrators using them for day-to-day operations. Organizations should make sure they manage and protect privileged accounts by allowing them only to be used when they are required.

FIGURE 13

Does your organization require that all administrators and other privileged users log in with a "standard" user ID for day-to-day activities, and only use a privileged account when required?

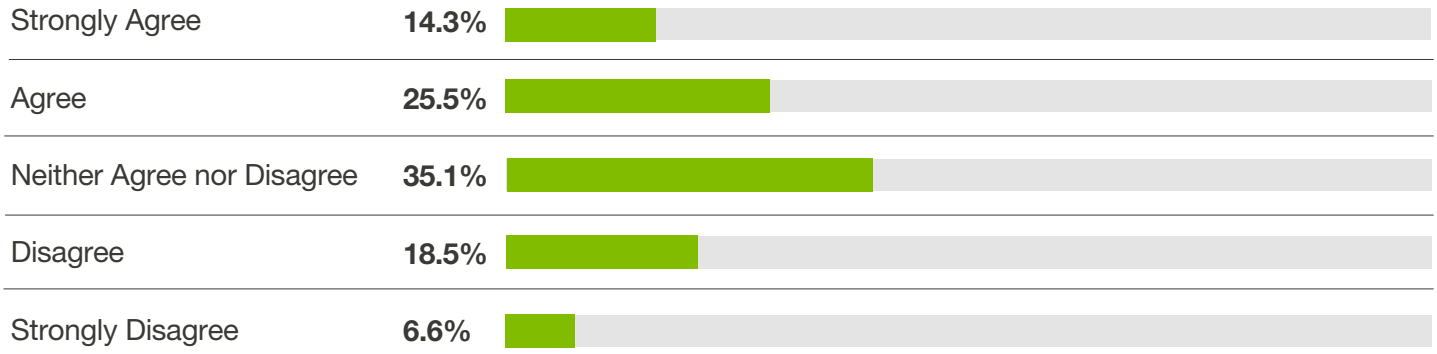


6 OUT OF 10 ORGANIZATIONS DO NOT EXPIRE THIRD-PARTY PRIVILEGED ACCOUNTS WITHIN 30 DAYS

Failing to expire privileged accounts that have been assigned to or used by third-party providers represents a substantial and wholly unnecessary risk for any organization. Many of the high profile breaches in the past few years were from compromised credentials of third-party vendors associated with major corporations. Privileged account users or applications should always be assigned an expiration date.

FIGURE 14

Third-party privileged accounts for users or applications should always be assigned an expiration date, with a default of 30 days or less if the expiration date is unknown.



HALF OF ORGANIZATIONS DO NOT AUDIT PRIVILEGED ACCOUNTS ACTIVITY

If you don't audit privileged account activity you are assuming they are never compromised and therefore don't pose any risk. That's because compromised privileged credentials can take up to 205 days before they are detected. Not recording and logging privileged account activity means you won't be able to determine normal privileged account behavior. By auditing and logging activity you have the necessary information to help detect cybersecurity breaches. Additionally if/when a breach occurs, audited activity provides vital forensic data to identify which systems an attacker may have accessed.

FIGURE 15

Do you log all privileged account activity on all systems and applications in your environment?

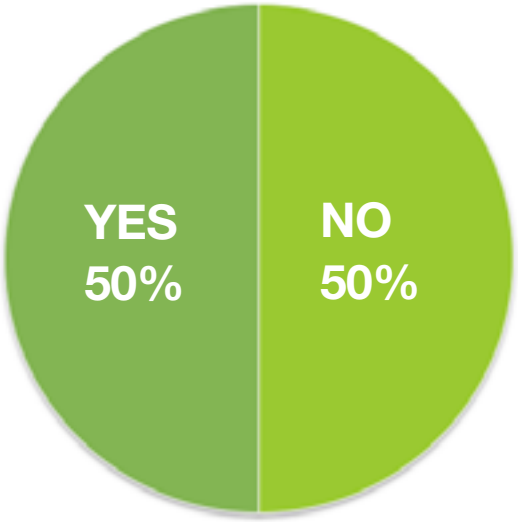
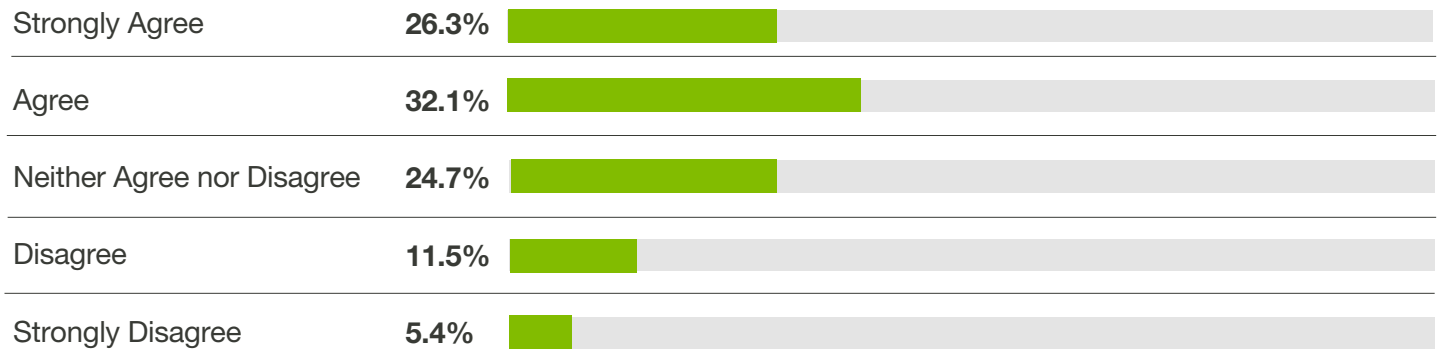


FIGURE 16

All user ID creation, deletion, and privilege change activity performed by Systems Administrators and others with privileged user IDs is securely logged in our environment.



PART 5:
TAKING ACTION
BASED ON BEST PRACTICE RECOMMENDATIONS

The 2016 State of PAM Report provides several recommended actions to help secure privileged credentials throughout the enterprise. These recommendations represent a cross section of best practices for PAM security generally accepted by experts and analysts in the industry.

Educate Key Stakeholders About Privileged Account Management Security

Educate key stakeholders in your organization about the urgency and value of Privileged Account and Access Management Security. You can use the 2016 State of PAM report executive summary as a starting point to get their attention. There are other sources at the **SANS Institute** as well as the new **Verizon 2016 Data Breach Report** which has just added a category for protecting privileged credentials. Be sure to take the **Privileged Password Vulnerability Benchmark survey** yourself to see how your current PAM practices compare with others, and share the results, and get specific recommendations to address issues you've identified within your organization.

Discover Where Your Privileged Accounts Are Located

Discover where your privileged accounts are located across your entire enterprise environment. You can't protect what you don't know exists, so it makes sense that one of your first steps to implementing better privileged credential security would be to find where all of your privileged accounts are located across your enterprise. There are free tools you can use to discover where your privileged accounts are located for both **Windows** and **Unix** environments.

Automate The Management And Security of Privileged Account Passwords

Automate the management and security of privileged account passwords. It's shocking that 6 out of 10 organizations, according to the report, still use manual methods such as spreadsheets and lists to keep track of privileged account passwords. It's nearly impossible in this day and age to handle the vast numbers and complexity of tracking and managing privileged account passwords by manual means. There is no reason any organization should not automate password management when there are affordable PAM solutions available for any size organization. Learn more about the top five privileged account password tasks you can automate in this **free eBook.**

Adopt And Implement Security Policies to Help Ensure Least Privilege Access

Adopt and implement security policies to help ensure least privilege strategy for account access. Too many accounts have been granted broad and deep privileges, and if only one of these accounts is compromised, it can quickly be used by an attacker to exploit your entire IT infrastructure. You should explore employing **software tools to limit privilege access** without impacting user productivity. It's a policy highly recommended by the SANS Institute and other cybersecurity organizations.

Provide Greater CISO Visibility and Demonstrate Compliance

Provide greater visibility into PAM for CISO, while helping to ensure you can demonstrate compliance with audits and policies affecting privileged account credentials. Implementing a PAM security program will give your executive stakeholders a more accurate and reassuring picture of your security posture while helping to spend less time and effort in demonstrating compliance with password policies for auditors. You can get a **free template for best practice privileged account security policies** as well as **free PAM software** to help automate and enforce those policies, improve security, and satisfy audit requirements.

PART 6: CONCLUSION

Given the results of the Privileged Password Vulnerability Benchmark Survey, we will likely continue to see major cyber breaches since such a significant portion of organizations appear to be failing to secure and manage privileged credentials.

Once accessed, these privileged credentials or "keys to the kingdom," provide an ideal channel for cyber criminals and others to find and extract critical information.

While progress has been made, and more organizations and security professionals are aware of the risks and vulnerabilities associated with Privileged Account Management (PAM), we still have a long way to go in implementing best practices to secure them. These security gaps in PAM are all the more remarkable when one considers that protecting privileged account passwords and access can mean the difference between a simple perimeter breach and a major cybersecurity disaster.

Our hope is that this report will encourage organizations and individuals worldwide to take a much closer look at automated PAM solutions and see how they can help implement practical and affordable PAM security controls. There is literally no excuse for leaving privileged credentials undiscovered and unprotected given the variety of PAM software solutions available.

About the report sponsors:

Thycotic

Thycotic is a global leader in IT security, and the fastest growing provider of Privilege Management solutions that protect an organization's most valuable assets from cyber-attacks and insider threats. Thycotic secures privileged account access for more than 7,500 organizations worldwide, including Fortune 500 enterprises. Thycotic's award winning Privilege Management Security solutions minimize privileged credential risk, limits user privileges and controls applications on endpoints and servers. Thycotic was founded in 1996 with corporate headquarters in Washington, D.C. and global offices in the U.K. and Australia.

For more information visit
www.thycotic.com

Cybersecurity Ventures

Cybersecurity Ventures is a research and market intelligence firm focused on the Cybersecurity industry. The firm's Cybersecurity Market Report forecasts worldwide cybersecurity spending will eclipse $1 trillion for the 5-year period from 2017 to 2021. Cybersecurity Ventures is regularly featured, quoted, and cited as a trusted source by major newspapers and the leading business, financial, technology, and cybersecurity news media.

For more information visit
www.cybersecurityventures.com

Survey Methodology

Thycotic Privileged Password Vulnerability Benchmark Scoring Methodology

The Benchmark has a maximum of 106 points possible. Not every question is scored; for example, questions about your industry or number of employees do not carry any score. Questions about your privileged password procedures and practices do carry a score value.

Your Grade is an "A" if your score is between 94 and 106

Your organization is exhibiting numerous best practices related to privileged account management and monitoring. You likely have a strong privileged account policy in place, with sound procedures and technology in place to support careful creation, management, and monitoring of all privileged accounts in the environment. You have integrated central privileged password control tools with your systems and applications, and adhere to best practices regarding password complexity, length, history, lockout, and more.

Your Grade is a "B" if your score is between 80 and 93

Your organization is meeting many best practices related to privileged account use, but could improve some of your technical controls and processes. You likely have a sound privileged account and password policy in place, and most hardening and configuration steps related to privileged accounts, passwords, and systems are being followed. Focus on implementing a strong centrally-managed privileged user and password management system, as well as the overall password and account lifecycle for privileged users in your environment.

Your Grade is a "C" if your score is between 65 and 79

Your organization is "average" when it comes to privileged account and password management, monitoring, and control. While you may have a policy and some general best practices in place, you should focus on account approval and lifecycle, a central password and account management platform, and more rigorous procedures for auditing, logging, and controlling access to privileged accounts in your environment.

Your Grade is a "D" if your score is between 50 and 64

Your organization is missing a number of best practices regarding privileged account and password management in your environment. Focus on a privileged user, account, and password policy that specifies how privileged accounts should be created, managed, controlled, and monitored. Once a policy is in place, ensure fundamental hardening and configuration steps are being taken across all systems and applications in the environment, and consider implementing a central privileged user and account management system.

Your Grade is an "F" if your score is between 49 and 0

Your organization is not meeting a majority of best practices regarding privileged account and password management today. This may result in significant security vulnerabilities and compliance deficiencies if not remedied in the near future. Ensure you have a strong policy, look for admin and other privileged accounts in use within the environment, and ensure management understands that privileged account management and monitoring needs to be a top security priority for you. Consider a privileged account management and monitoring platform to help get this issue under control as well.

Survey Demographics

Out of the organizations surveyed the global response indicates that North America is leading the adoption of Privilege Account Management followed by Europe. The report highlights that due to the increasing amount of cyber-attacks and breaches in North America that organizations are looking to secure privileged accounts to help defend against the ever growing amount of cyber breaches. Cyber terrorism awareness must become more of a priority for businesses as the threat of a catastrophic event is becoming increasingly likely. This was also reinforced in a recent report from the US Department of Energy which indicated that privileged accounts can be the difference between simple system access and the ability to shut down critical infrastructure as we have seen recently occurring in Ukraine in which a cyber-attack cut power to more than 80,000 people.

Location of respondents to Privileged Password Vulnerability Benchmark survey

United States 76.5%

Western Europe 12%

Canada 7.3%

India 1.5%

Asia-Pacific 1.5%

Asia 1.2%

Size Of Organizations Participating in the Privileged Password Vulnerability Benchmark Survey

Global – 15%

Large – 25%

Mid-Sized – 25%

Small – 35%

The industries surveyed show that Government, Finance and Academic sectors are adopting Privilege Account Management or considering it as a higher priority. This is indicated by the higher valued targets for financial or political-based attacks, though while these are high value targets we have seen that no one is excluded from cybercrime with many SMB companies being breached.

Types Of Industries Represented by Participants in the Privileged Password Vulnerability Benchmark Survey

Financial Services/Insurance – 15%

Health care – 10%

Manufacturing – 10%

IT – 10%

Academic – 7%

Govt – 7%

Energy – 9%

Auto – 5%

Entertainment – 2%

All others – 25%

Thycotic privileged account security solutions provide organizations with several key advantages including:

- Comprehensive platform for proactive protection of privileged credentials and target assets from cyber-attacks. Our solution for privileged account security enables customers to proactively protect against and automatically detect and respond to cyber-attacks before they strike vital systems and compromise sensitive data. We enhance the effectiveness of traditional security defenses by introducing a new security layer that prevents the misuse of privileged accounts which exist in virtually every piece of technology in the organization including security products.

- Automatic identification and understanding of the scope of privileged account risk. Our solution automatically detects privileged accounts across the enterprise and helps customers visualize the resulting compliance gaps and security vulnerabilities. This automated process reduces the time-consuming and error-prone task of manually tracking and updating privileged credentials, thereby decreasing IT operational costs. This enhanced visibility significantly improves the security posture of our customers and facilitates adherence to rigorous audit and compliance standards.

- Continuous monitoring, recording and secure storage of privileged account activity. Our solution monitors, collects and records individual privileged session activity. It also provides highly secure storage of privileged session recordings and robust search capabilities allowing organizations to meet their audit and compliance requirements. Session recordings also provide a full forensics record of privileged activity to facilitate a more rapid and precise response to malicious activity.

- Purpose-built solution architected for privileged account security. Our solution is architected across products to optimize security. Our Vault, is a secure repository for privileged credentials, offers multiple layers of security including robust segregation of duties, a secure proprietary communications protocol and military-grade encryption.

- End-point security and application control for Windows and UNIX and prevents privilege escalation by removing and/or limiting privileges for business users and IT admins without impacting productivity.

- Scalable and flexible platform that enables modular deployment. Our solution is scalable and flexible to enable deployments in large-scale distributed environments.

To learn more visit our website at www.thycotic.com

SEE FOR YOURSELF!
TAKE THE SURVEY:

Take the Privileged Password Vulnerability Benchmark survey now!
https://thycotic.com/solutions/free-password-vulnerability-benchmark-tool/

FREE TOOLS & SOFTWARE

Privileged Account Discovery Tool for Windows
https://thycotic.com/solutions/free-windows-privileged-account-discovery-tool/

Privileged Account Discovery Tool for UNIX
https://thycotic.com/solutions/free-it-tools/free-unix-privileged-account-discovery-tool/

The Top 5 Tasks to Automate for Privileged Account Management and Security
https://thycotic.com/resources/it-automation-ebook/

Security Policies Template
https://thycotic.com/solutions/free-IT-tools/free-privileged-password-security-policy-template

Secret Server Free
https://thycotic.com/solutions/free-it-tools/secret-server-free/

Software Tools to Limit Privileged Access
https://thycotic.com/products/endpoint-security-remediation-suite/