2020 STATE OF PRIVILEGED ACCESS MANAGEMENT (PAM) MATURITY REPORT

of organizations fail to meet even basic PAM security hygiene

PAM Maturity Assessment survey reveals more than four out of five not automating key privileged access capabilities

thycotic

Executive Summary

With up to 80% of breaches due to compromised credentials according to leading analysts, more organizations than ever are prioritizing privileged account protection. As Privileged Access Management (PAM) becomes top of mind, C-level, IT and cyber security professionals are seeking a framework in which they can properly assess, manage, and minimize risks to privileged credentials.

Thycotic's free, online PAM Maturity Assessment helps organizations determine progress along their journey to lower privileged access risk, increase business agility, and improve operational efficiency. Based on security industry best practices and deep experience with more than 10,000 PAM customers worldwide, the PAM Maturity Assessment asks questions that determine how far an organization has progressed through the four phases of PAM maturity described below.

PHASE 1

Analog

Organizations in the Analog phase of PAM maturity face a high degree of risk. Securing their privileged access is limited and minimal. Privileged credentials are managed mostly manually and may be tracked with spreadsheets. As a result, these organizations often provide excess privileges to people who don't need them, share privileges among multiple administrators, and neglect to remove privileges when users leave the organization or change roles.

Service accounts are created "in the wild," leading to poor documentation, poor mapping to applications or core services, and "re-usage," where a single account is used repeatedly for numerous services. Security and operations teams are typically unaware of the breadth of web applications in use and allow users to make independent decisions regarding privileged access and permissions.

How to Define Privileged Access Management (PAM)

Privileged access must be defined around the specific situation of each organization. We recommend you perform a Data Impact Assessment to determine which privileged accounts are being used to access your most sensitive data, including intellectual property. You can then audit and confirm who should have access rights to view and manage this sensitive data. Privileged accounts are everywhere in your IT environment and can be human or non-human. Some privileged accounts are associated with individuals such as local administrators or network administrators, while others are service accounts used to run databases, appplications and other systems and aren't associated with a person's unique identity.

PHASE 2

Basic

Organizations transition from Analog to the Basic phase of PAM maturity by adopting PAM security software and automating time-consuming, manual processes. They have implemented a password vault to store privileges but are typically implementing password management tools more appropriate for consumers than enterprises.

They focus on privileged accounts managed by domain administrators and other IT users and as a result they have a limited view of the privileged account attack surface.

Organizations in this stage must make periodic pushes to discover and rediscover new accounts across the network. Occasionally business-critical applications experience downtime because new usages of service accounts have not been onboarded and associated with the corresponding service account managed in the PAM solution. This sometimes leads to an atmosphere of mistrust between teams, making full adoption of a PAM solution difficult.

PHASE 3

Advanced

Organizations in the Advanced phase of PAM maturity have moved from a reactive to a proactive privilege security strategy. PAM becomes a top cyber security priority, with a commitment to continuous improvement of privileged security practices.

As organizations move from a reactive to a proactive strategy they enter the Advanced phase of PAM maturity, they broaden their definition of privileged account management and expand their PAM policies to actively manage service accounts, as well as web and SaaS applications managed by developers and business users.

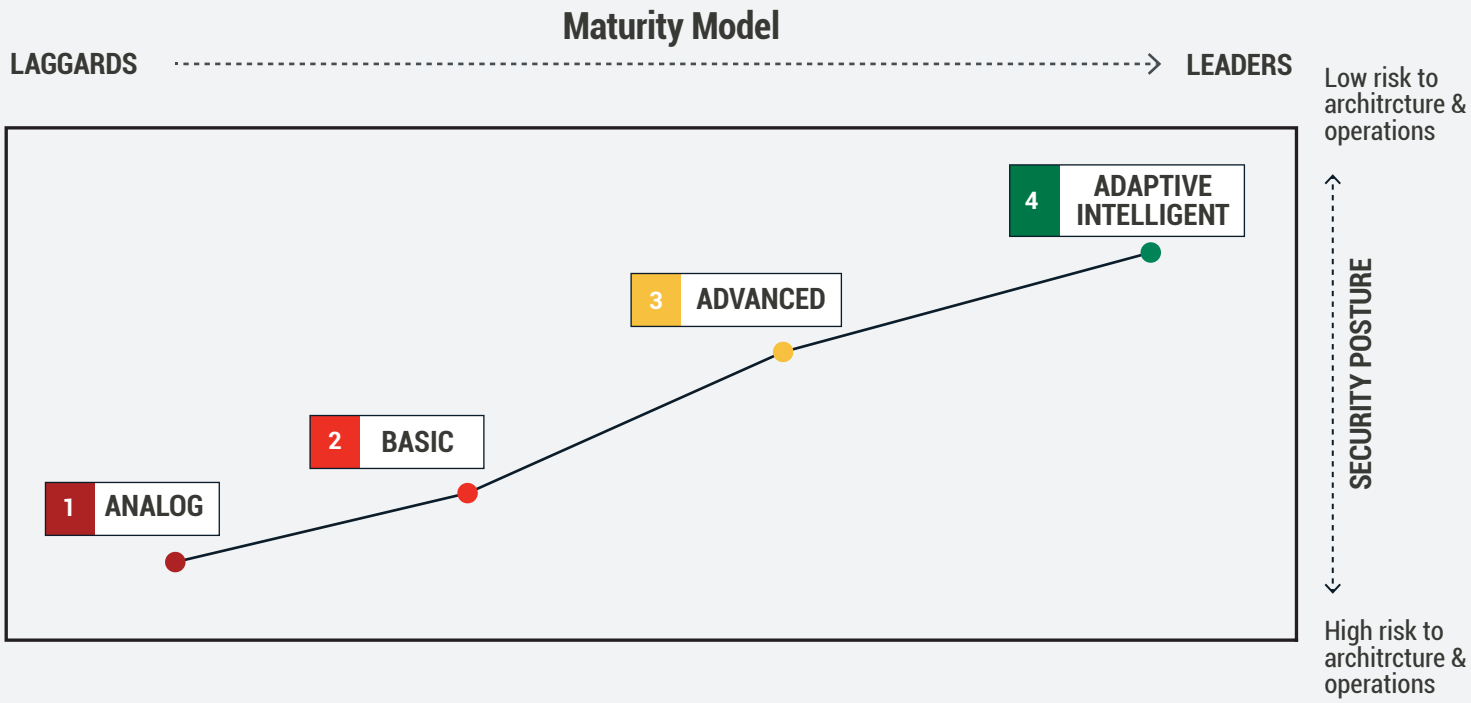
PHASE 4

Adaptive Intelligent

As the ultimate stage of PAM maturity, organizations in the Adaptive Intelligent phase take continuous improvement to a higher level, integrating leading technologies such as artificial intelligence and machine learning to collect information and adapt system rules. These organizations fully automate and manage the entire lifecycle of privileged accounts, from provisioning to rotation to deprovisioning and reporting.

They consider every account a privileged account and have a consolidated view of all accounts, credentials, access and user permissions, for all types of privileged accounts throughout the organization.

Privileged Access Management Maturity Model



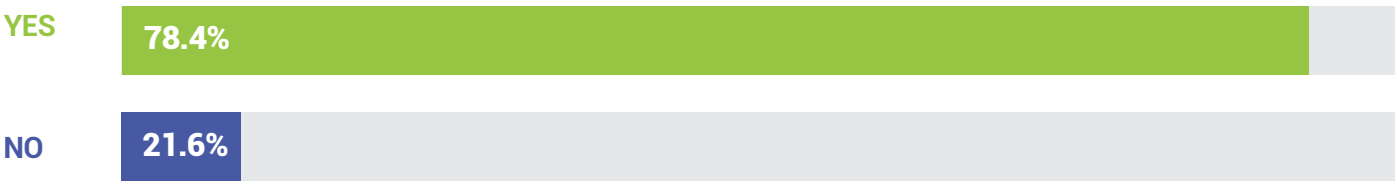
86%

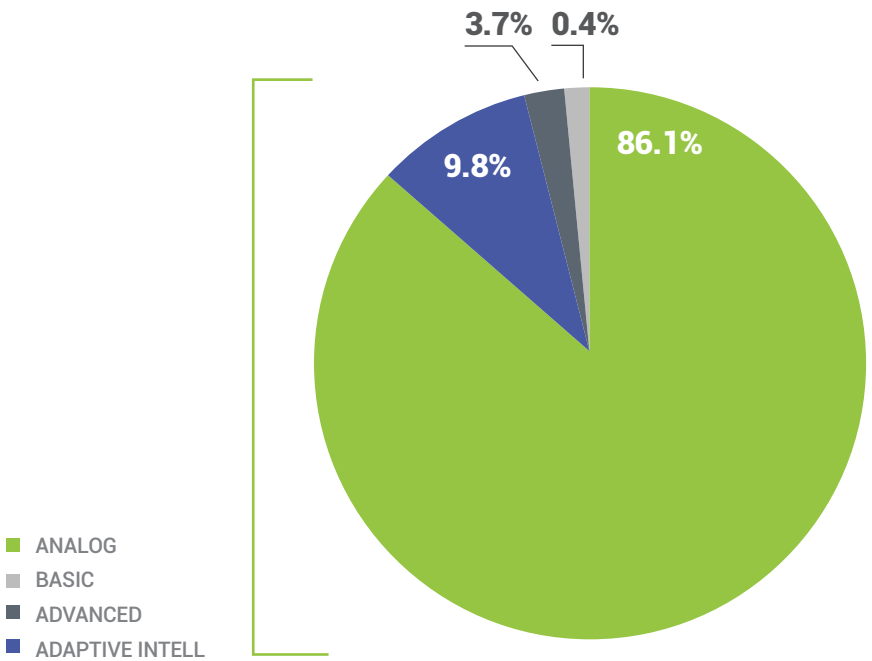
of organizations fail to meet even a basic PAM maturity level.

This report summarizes findings based on 568 completed surveys.

The results are far worse than you might think—and may go a long way to explaining why four out of five breaches are related to compromised credentials.

Are you including privileged accounts in your broader IT cyber security policy?





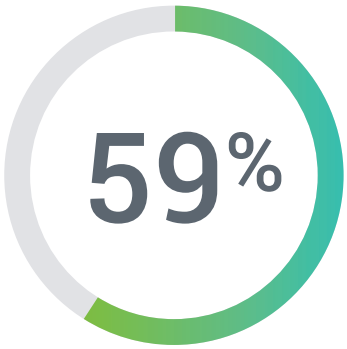
4 in 5

organizations include privileged credential protection as part of their cyber security strategy, their PAM security practices are woefully lacking and even worse than you might expect. This means organizations have acknowledged the problem but are failing to put the necessary security controls in place to reduce risks.

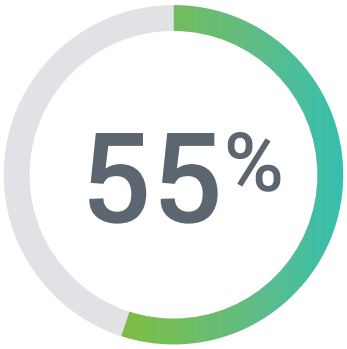
86%

of respondents are still struggling to get beyond the Analog phase of Privileged Access Management (PAM) maturity!

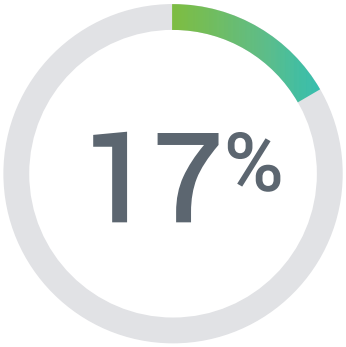
Among those failing to reach even a basic level of maturity:



of organizations have no idea how many privileged accounts they have or where they're located.



of organizations' privileged accounts never expire or get deprovisioned.



of organizations are storing all their privileged accounts in a secure privileged access management vault or password manager.

If a survey respondent answered "no" to any of four critical questions, they were designated to the "Analog" phase of maturity. In other words, if they weren't including PAM in their cyber security strategy, weren't discovering privileged accounts, weren't deprovisioning privileged credentials or weren't storing credentials in a secure vault, they haven't achieved even the Basic level of PAM maturity.

In sharing the assessment results in this report, Thycotic encourages organizations across the globe to examine their own PAM practices and target specific areas for improvement. We've highlighted three key takeaways in this report along with specific recommendations and suggested resources for further learning and action steps.

Our goal is help you apply lessons from the PAM Maturity Model to your own cyber security strategy regardless of the size of your company, your industry or the number and type of privileged accounts you need to

Key Takeaways

KEY TAKEAWAY #1

You can't protect what you can't see. Your first step must be to automate discovery of privileged accounts.

Most disturbing of all the PAM Maturity Assessment results is the lack of visibility into how many privileged accounts exist in an organization and where they are located. More than half (55%) of survey respondents aren't automatically discovering privileged accounts. Because privileged accounts such as local admin and service accounts exist everywhere in multiple places throughout an organization, trying to manually discover and manage them is virtually impossible. Your first step should be to automate privileged account discovery so that you can see what you need to protect. Then, apply basic PAM security controls to use complex passwords and rotate passwords on a regular basis.

KEY TAKEAWAY #2

Basic PAM hygiene won't improve without stopping bad habits while adopting and automating better ones.

It's clear from those taking the PAM Maturity Assessment that ingrained bad habits continue to hamper efforts in securing privileged access. Less than one in five organizations are using a password vault and most still don't require Two-Factor Authentication. If you aren't already using one, you need to implement a password vault manager as soon as possible. Then, establish and automate specific security policies that promote proper PAM security hygiene, especially for deprovisioning privileged credentials. Multi-Factor Authentication should be standard for all privileged accounts and an audit trail of privileged account usage should be instituted to meet policy and compliance mandates.

KEY TAKEAWAY #3

Only with greater PAM maturity can you gain critical insight to reduce cyber risk.

Once you achieve basic PAM security practices, you're ready to go to the next level of maturity, and become more sophisticated in your knowledge, insights, and actions. Most organizations are unable to monitor for suspicious privileged account behavior and only one in eight has implemented a least privilege policy for account access with application control. Fully one third (34%) of respondents don't apply Privileged Access Security with their DevOps teams. You should begin evaluating PAM solutions for privileged behavior analytics and a implement a least privilege strategy to ensure your organization can realize the full benefits of advanced and agile PAM.

KEY TAKEAWAY #1

You can't protect what you can't see. Your first step must be to automate the continuous discovery of privileged accounts.

Once you've been able to identify all your privileged accounts you can begin to implement basic PAM security polices, such as automating password creation and rotation for accessing privileged accounts.

SURVEY RESULTS

If you can't see it, you can't protect it.

59% of organizations taking the assessment aren't discovering privileged accounts with automated tools, meaning they likely don't know how many privileged accounts they have or where they're located.

QUESTION #2

Are you discovering privileged accounts automatically in your organization?

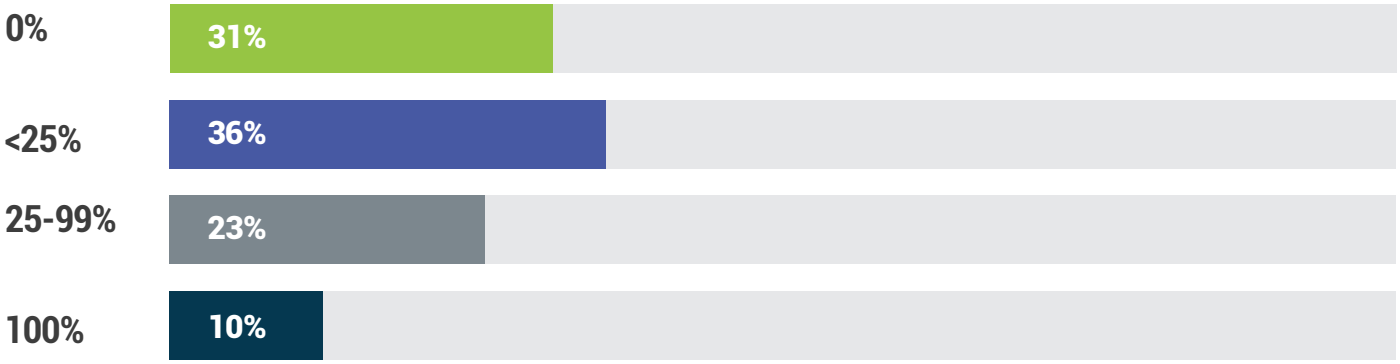
Without an automated process for identifying privileged accounts it's nearly impossible to keep track of them manually, if at all. This means 55% of organizations likely have no idea how many privileged accounts they have or if they might have been compromised. With hundreds and sometimes thousands of privileged accounts throughout an IT environment, organizations face serious risks from both internal abuse and external threats.

Creating passwords manually and never changing them invites disaster.

10% of organizations are generating complex passwords for all privileged accounts and rotating them on a schedule

QUESTION #3

How many of your privileged accounts utilize automatically generated complex passwords and are rotated on a timeframe?



9 of 10

organizations rely on human-created passwords for privileged accounts—and these passwords may never have been changed over a period of months or even years.

33%

of organizations have instituted complex password generation and regular rotation of their privileged accounts passwords.

31%

of organizations don't address the issue at all.

"I've got to write it down, so I don't forget."

57%

of organizations allow passwords to be viewed by any user.

10%

of organizations fully rotate passwords on a schedule.

QUESTION #5

Are you using any tools to prevent passwords from being disclosed during usage?

Allowing employees to see passwords for privileged accounts poses the risk that those passwords will be written down for reference in a spreadsheet or Post-it note, easily shared with colleagues, or used to access systems by skirting security controls. Automated tools exist to help ensure that no employee needs to see a password to gain access, especially for privileged credentials.

Recommendations

Lack of visibility into how many privileged accounts exist in an organization and where they are located is an enormous risk for organizations. Because privileged accounts, such as local admin and service accounts, exist everywhere throughout an organization, trying to manually discover and manage them is virtually impossible. Your first step should be automating privileged account discovery on a continuous basis so you can see what you need to protect. Then, apply basic PAM cyber security strategies to identify weak passwords and remediate them using complex passwords and regular password rotation.

- **Conduct a complete discovery of all privileged accounts across the enterprise**
- **Identify weak passwords on privileged accounts and remediate them**
- **Establish a password rotation protocol for all privileged accounts**

Free Resources

Windows Privileged Account Discovery Tool

thycotic.com/freediscoverytool/

At the click of a mouse, Thycotic's Free Privileged Account Discovery Tool discovers your Windows privileged accounts and generates immediate, detailed reports.

Service Account Discovery Tool

thycotic.com/solutions/free-it-tools/service-account-discovery-tool/

The Service Account Discovery Tool measures the state of privileged access entitlements in your Active Directory service account

Privileged Account Management for Dummies eBook

thycotic.com/PAMforDummies/

This free eBook is written for IT teams and systems administrators along with security professionals responsible for protecting an organization from security threats.

KEY TAKEAWAY #2

Basic PAM hygiene won't improve without stopping bad habits while adopting and automating better ones.

To stop ingrained bad habits when accessing privileged accounts, you need to make processes easier as well as more secure. That means automating password management through a secure vault to store credentials, implementing Multi-Factor Authentication, and keeping a record of usage.

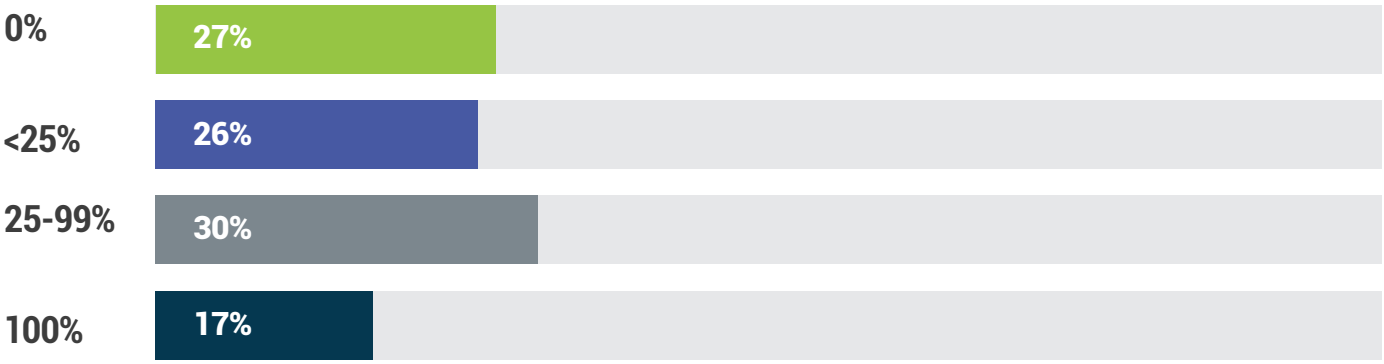
SURVEY RESULTS

Who, what, when, where...?

17% of organizations are storing all privileged accounts in a secure Privileged Access Management vault or password manager. Twenty-eight percent of organizations are doing nothing to protect them, likely using spreadsheets or putting them on paper.

QUESTION #4

How many of your privileged accounts are being stored in a secure vault?



The risks of not storing passwords in a secure vault are clear. Organizations have no visibility into when passwords are used, no insight into what security controls are applied to privileged accounts, and no idea who is using them or who has access. This situation makes it difficult to demonstrate compliance with ISO standards, mandates such as PCI, and many other regulations and compliance requirements.

A single password can't fully protect a privileged account.

57% of respondents aren't using Two-Factor Authentication or Multi-Factor Authentication with privileged accounts. That leaves a single password as the only obstacle between a cyber criminal and privileged access.

QUESTION #6

Do you enforce 2 factor authentication or Multi-Factor Authentication to be used with privileged accounts?

Most compliance policies and legal regulations require that privileged accounts be safeguarded with at least Two-Factor Authentication for good reason. A password should never be the only security control protecting a privileged account as it's too easily compromised. Privileged account access should always be established with security controls that verify identity and build trust. Combining Two-Factor Authentication with Privileged Access Management, for example, enables an organization to adapt a zero-trust approach for access to sensitive systems or data, ensuring every access request is continuously verified.

Who used this privileged account last, and when?

58% of respondents fail to maintain an audit trail of privileged account activity.

QUESTION #7

Do you maintain an immutable audit trail of privileged accounts activity?

Lack of an audit trail for privileged access is especially important in responding to data breaches. Without an audit trail, the only way to fully remediate a domain administrator account breach, for example, would be to rebuild the entire account activity from scratch since there would no way of knowing exactly what a cyber criminal might have modified. No organization wants to find itself in such a position, when quickly responding and remediating a breach can be the difference between a minor incident and a major disaster.

The never-ending story of privileged account risk.

55% of organizations have privileged accounts that never expire or get deprovisioned. This is a major risk when organizations focus only on provisioning privileged accounts but never remove them.

QUESTION #9

Do you automatically retire privileged accounts no longer in use?

Organizations face a very high risk of compromised privileged accounts if they fail to remove them once they are no longer required. Cyber criminals enjoy going after low-level privileged accounts that are left dormant, keeping a low profile while waiting for the right moment to abuse them.

Recommendations

Unfortunately, ingrained bad habits continue to hamper efforts to properly secure privileged access. Far too many organizations fail to use a password vault manager and most still don't require Two-Factor Authentication. If you haven't already, you need to implement a password vault manager as soon as possible. Then, establish and automate specific security policies that promote proper PAM security hygiene, especially for deprovisioning privileged credentials. Multi-Factor Authentication should be standard for all privileged accounts and an audit trail of privileged account usage should be instituted to meet policy and compliance mandates.

- **Discover and minimize all domain admin and service accounts**
- **Vault all passwords for privileged accounts with password management software**
- **Institute Multi-Factor Authentication for all privileged accounts**
- **Conduct session monitoring and recording for privileged access**
- **Establish PAM security policies to safeguard systems and meet compliance mandates**

Free Resources

Security Policies Template for Privileged Passwords

https://thycotic.com/solutions/free-it-tools/free-privileged-access-management-pam-policy-template/

Privileged account credentials are a prime target of hackers, so it's critical that you put password protection policies in place to prevent unauthorized access and demonstrate security compliance.

Privileged Access Management Policy Template

thycotic.com/policy-template/

The free Privileged Access Management Policy Template saves you hours of effort defining clear and consistent policies that everyone who uses and manages privileged accounts understands and accepts. It contains 40+ pre-written policy statements, based on requirements outlined by CIS, NIST, PCI and HIPAA.

KEY TAKEAWAY #3

Only with greater PAM maturity can you gain critical insight to reduce cyber risk.

As organizations move from Analog to Basic PAM security hygiene they can implement more sophisticated measures to protect their networks and endpoints with automated software tools. These measures include behavioral analytics along with a least privilege strategy with application control to secure endpoints without impacting pro-

SURVEY RESULTS

Just because you don't see it doesn't mean it's not there.

61% **of organizations taking the assessment aren't checking automatically for suspicious activity with privileged access, meaning they're likely already a victim of cyber crime and just haven't discovered it yet.**

QUESTION #8

Do you have a way to automatically detect and respond to anomalous privileged activity?

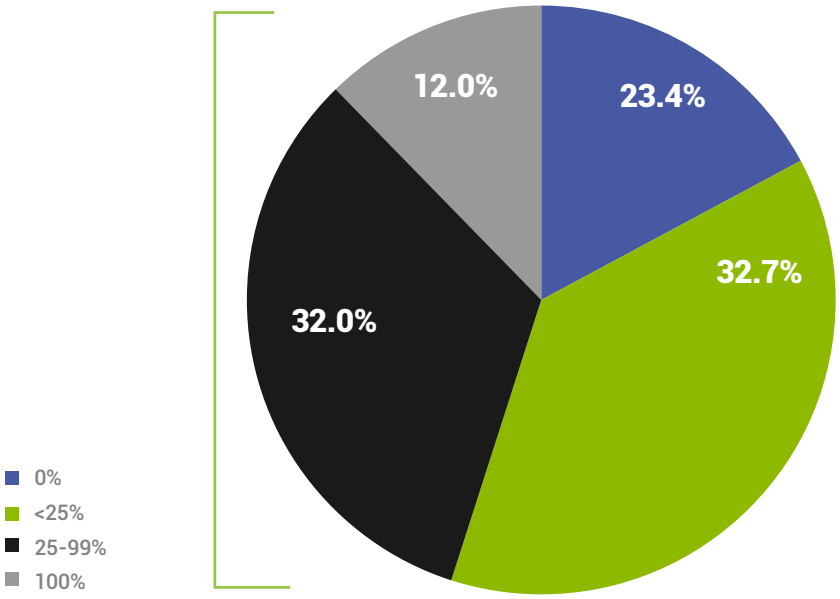
Unfortunately, it's probably not a question of if you're going to be a victim of cybercrime, but rather when it's going to happen. Given the limited staff resources of most organizations, an automated tool to detect suspicious activity should be put in place along with a formal incident response plan to manage security incidents that occur. Those organizations not automatically checking for suspicious activity regarding privileged accounts are likely already a victim of cybercrime.

You've got to rein in overprivileged users.

12% **of organizations have implemented both Privileged Access Management and application control on their endpoints to enable a least privilege strategy.**

QUESTION #11

What percentage of endpoints are protected by privilege management and application control?



A least privilege strategy is becoming recognized as essential to protecting both human and non-human privileged accounts. Cyber security regulations are evolving globally, aimed at ensuring employees are not overprivileged with access. Several countries have significant financial penalties for failure to comply. Yet, four out five respondents—86%—are exposed to the extremely high risk of compromise from overprivileged users. Only one of those overprivileged user accounts needs to be compromised for attackers to gain access to an organization's entire network.

Ignore DevOps security at your peril.

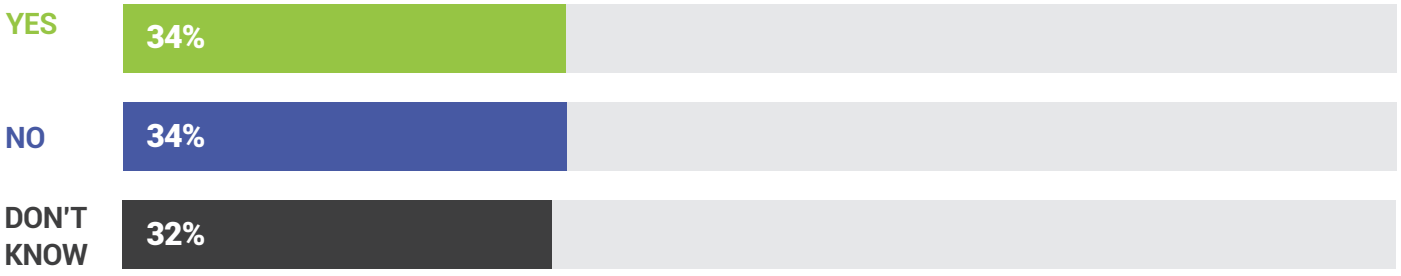
34%
of organizations have adopted a DevSecOps approach to integrate cyber security into the development process.

34%
of organizations still have not introduced security into DevOps.

32%
of organizations don't have the security team involved in the development process.

QUESTION #10

Do you utilize a credentials management tool during your software development processes?



Organizations that have moved to using DevOps for continuous delivery and continuous integration have benefited from being able to quickly deploy new updates and features in near real-time, greatly improving efficiency. The need to include security into DevOps has introduced a concept known as DevSecOps—building security into the development process and lifecycle. Those organizations that have adopted DevSecOps can realize significant savings over those that try to "bolt on" security measures at the end of the development cycle.

Recommendations

Once you achieve basic PAM security practices, you're ready to go to the next level of maturity. That means implementing a least privilege strategy, monitoring for suspicious behavior with privileged accounts, and preparing and testing an incident response plan. You should evaluate automated PAM solutions that enable behavior analytics and least privilege strategy with application control to ensure your organization can realize the full benefits of advanced and agile PAM.

- **Implement privileged behavior analytics to help detect suspicious activity**
- **Plan a least privilege strategy for privileged credentials with application control**
- **Develop and test an incidence response plan**
- **Centralize control over privileged access in a single interface to better manage often overlooked accounts such as DevOps, service accounts and cloud resources**

Bottom Line

The key to improving cyber security with Privileged Access Management stems from an understanding and implementation of a PAM lifecycle approach. Only a comprehensive solution can ensure that your "keys to the kingdom" are properly protected from hackers and malicious insider threats. And, it will ensure access controls meet regulatory requirements for compliance mandates in your industry and geography.

For more information about Thycotic and the PAM solutions we provide, visit our website at www.thycotic.com.

Free Resources

Least Privilege for Dummies book

thycotic.com/least-privilege-dummies/

This free eBook is the perfect starting point for you and your staff to understand the basic concepts of least privilege and key steps to planning your least privilege strategy, including how to apply least privilege with application control.

Windows Least Privilege Discovery Tool

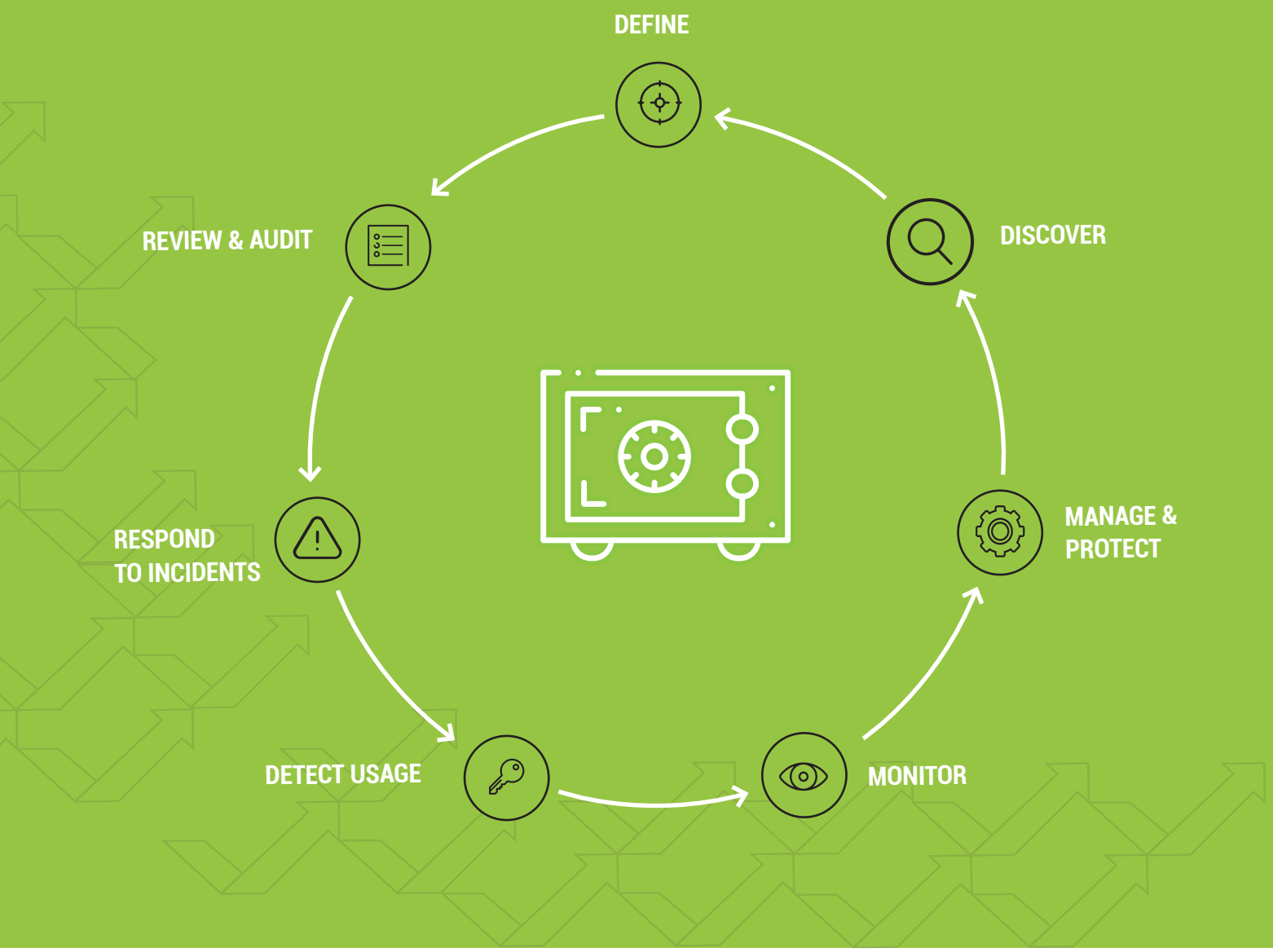
thycotic.com/least-privilege-tool/

With this tool you can discover local admin accounts, service accounts, and applications in use on endpoints.

Incident Response Plan Template

thycotic.com/incident-response-template/

The template provides a checklist of roles, responsibilities, and actionable steps to measure the extent of an privileged account cyber incident and contain it before it damages critical systems. The template is customizable to match your incident response policies, regulatory requirements, and organizational structure.



CONCLUSION

Achieve more mature practices with a PAM Lifecycle Model.

The 2020 State of Privileged Access Management (PAM) Maturity Report is a wakeup call for organizations worldwide to immediately assess their PAM practices with a goal of moving beyond dangerous habits to implementing a PAM Lifecycle Model. A PAM lifecycle approach provides a framework for any organization to manage its privileged accounts and access as a continuous program rather than a one-off project.

Define

Start by defining what 'privileged access' means and identify what a privileged account is for your organization. It's different for every company so it's crucial you map out what important business functions rely on data, systems and access. Gain a working understanding of who has privileged account access and when those accounts are used.

Discover

Identify your privileged accounts and implement continuous discovery to curb sprawl, identify potential insider abuse, and reveal external threats. This helps ensure ongoing visibility of your privileged account landscape crucial to combating cyber security threats.

Manage and protect

Proactively manage and control privileged account access, schedule password rotation, audit, analyze, and manage individual privileged session activity. For IT administrators and privileged account users, control access and implement superuser privilege management to prevent attackers from running malicious applications, remote access tools, and commands. Least privilege and application control solutions enable seamless elevation of whitelisted applications while minimizing the risk of running unauthorized applications. Secure access to systems and services that reside on-premise and in the cloud, including IaaS, PaaS, and SaaS.

Monitor

Monitor and record privileged account activity. This will help enforce proper behavior and avoid mistakes. If a breach does occur, monitoring privileged account use also helps digital forensics identify the root cause and identify critical controls that can be improved to reduce your risk of future cyber security threats.

Detect

Ensuring visibility into the access and activity of your privileged accounts in real time will help spot suspected account compromise and potential user abuse. Behavioral analytics focuses on key data points to establish individual user baselines, including user activity, password access, similar user behavior, and time of access to identify and alert you of unusual or abnormal activity.

Respond

When a privileged account is breached, simply changing the password or disabling the account isn't enough. While inside, hackers could have installed malware and even created their own privileged accounts. If a domain administrator account gets compromised, for example, you should assume that your entire Active Directory is impacted and investigate and make changes so the attacker can't easily return.

Review and Audit

Continuously observing how privileged accounts are being used through audits and reports will help identify unusual behaviors that may indicate a breach or misuse. Automated reports help track the cause of security incidents as well as demonstrate compliance with policies and regulations. Auditing privileged accounts will also give you metrics that provide executives with vital information to make more informed business decisions

PAM Maturity Index Scoring Methodology

The chart below shows the scores assigned to each question in the Index.

Question #	Question	Response Options	Response Score	Cumulative Score Considerations
Question 1	Are you including privileged accounts in your broader IT cyber security policy?	A-Yes B-No	A-100 B-0	If B, then automatic cumulative assessment of ANALOG
Question 2	Are you discovering privileged accounts automatically in your organization?	A-Yes B-No	A-100 B-0	If B, then automatic cumulative assessment of ANALOG
Question 3	How many of your privileged accounts utilize automatically generated complex passwords and are rotated on a timeframe?		A-0 B-33 C-66 D-100	If A or B, then automatic cumulative assessment of ANALOG
Question 4	How many of your privileged accounts are being stored in a secure vault?		A-0 B-33 C-66 D-100	If A or B, then automatic cumulative assessment of ANALOG
Question 5	Are you using any tools to prevent passwords from being disclosed during usage?		A-100 B-0	
Question 6	Do you enforce 2fA or MfA to be used with privileged accounts?		A-100 B-0	
Question 7	Do you mantian an immutable audit trail of privileged activity?		A-100 B-0	
Question 8	D you have a way to automativally detect and respond to anomalous privileged activity?		A-100 B-0	
Question 9	Do you automatically retire privileged accounts no longer in use?		A-100 B-0	
Question 10	Do you utilize a credentials management tool during your software development processes?		A-100 B-0	
Question 11	What percentage of endpoints are covered by privilege management and application control?		A-0 B-33 C-66 D-100	

After the survey is completed, the chart below is used to assign the final Maturity Level.

Note: Any score of zero for any of questions 1-5 will automatically result in a “Analog” assessment for the organization.

Cumulative Point Score	Maturity Level Determination
0-275	1- Analog
276-550	2- Basic
551-825	3- Advanced
826-1100	4- Adaptive Intelligent

About Thycotic

Thycotic is the leading provider of cloud-ready privilege management solutions. Thycotic's security tools empower over 10,000 organizations, from small businesses to the Fortune 500, to limit privileged account risk, implement least privilege policies, control applications, and demonstrate compliance. Thycotic makes enterprise-level privilege management accessible for everyone by eliminating dependency on overly complex security tools and prioritizing productivity, flexibility and control. Headquartered in Washington, D.C., Thycotic operates worldwide with offices in the UK and Australia. For more information, please visit www.thycotic.com.

For more information, please visit www.thycotic.com

thycotic