Brought to you by:

Delinea

Privileged Access Management (PAM)

for dummies®

A Wiley Brand

Thwart privilege-based attacks

Get started with Privileged Access Management

Develop a step-by-step PAM roadmap

2nd Delinea Special Edition

Joseph Carson, CISSP, OSCP

About Delinea

Delinea is a pioneer in securing identities through centralized authorization, making organizations more secure by seamlessly governing their interactions across the modern enterprise. Delinea allows organizations to apply context and intelligence throughout the identity life cycle across cloud and traditional infrastructure, data, and SaaS applications to eliminate identity-related threats. With intelligent authorization, Delinea provides the only platform that enables you to discover all identities, assign appropriate access levels, detect irregularities, and immediately respond to identity threats in real time. Delinea accelerates your teams' adoption by deploying in weeks, not months, and makes them more productive by requiring 90 percent fewer resources to manage than the nearest competitor. With a guaranteed 99.99 percent uptime, the Delinea Platform is the most reliable identity security solution available.

Learn more about Delinea at delinea.com and on social media at

 www.linkedin.com/company/delinea

 x.com/delineainc

 www.youtube.com/c/Delinea

Privileged Access Management (PAM)

2nd Delinea Special Edition

by Joseph Carson, CISSP, OSCP

for dummies®
A Wiley Brand

Privileged Access Management (PAM) For Dummies®, 2nd Delinea Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN: 978-1-394-29092-5 (pbk); ISBN: 978-1-394-29093-2 (ebk); 978-1-394-29094-9 (ePub).
Some blank pages in the print version may not be included in the ePDF version.

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Manager and Developmental Editor: Carrie Burchfield-Leighton

Sr. Managing Editor: Rev Mengle

Acquisitions Editor: Traci Martin

Sr. Client Account Manager: Matt Cox

Table of Contents

Introduction

Today's IT perimeter extends well beyond the physical boundaries of the office or network. People and machines can connect to sensitive data and systems through diverse and changing access points. After they're inside your environment, users perform operations such as updating software, making configuration changes, and executing transactions. With sufficient privileges, users can cause unintentional or intentional damage, shutting down systems and disrupting business operations if the damage is left unmonitored.

Unfortunately, traditional security measures, such as firewalls and virus protection, don't provide sufficient protection when identities move in and out of a porous perimeter.

But Privileged Access Management (PAM) establishes an authorization trust model so you always know what identities are operating in your environment and what they can access. PAM replaces the need for manual password management and static access control with seamless automation, stronger security, and continuous oversight.

With PAM, you can employ consistent, policy-based controls to manage privileged identity behavior. PAM policies determine which systems authenticated identities are authorized to access and what they can do with that access.

About This Book

This book is for IT and security professionals who are building a PAM program for the first time, as well as those looking to update existing programs with the latest PAM practices. You discover how the definition of PAM has evolved and how PAM solutions have expanded their capabilities to combat the rise in privilege-based attacks.

Within these pages, you also find easy-to-understand explanations to help you save time in creating your own step-by-step roadmap. You can also share this content with others in your organization to

- Increase awareness about the importance of PAM.
- Gain buy-in and budget for your program.
- Drive the adoption of cybersecurity best practices.

Icons Used in This Book

This book uses the following icons to indicate special content.

REMEMBER

You don't want to forget this information. It's essential to gain a basic understanding of PAM processes.

TECHNICAL STUFF

This icon indicates more technical information that's of most interest to IT and system administrators — or just you techie types.

TIP

The Tip icon points out practical advice that saves you time and effort in putting together your own privileged account password security strategy.

WARNING

Watch out! Pay close attention to these details. They focus on serious issues that have a major impact on you and your organization's security.

Beyond the Book

PAM doesn't have to be an insurmountable challenge. If you're interested in learning more about PAM and how it fits into a comprehensive identity security strategy, visit the Delinea website at `www.delinea.com`. Free educational resources include original research on privilege and identity-based attacks, assessment tools to discover vulnerabilities and benchmark your PAM practices, and how-to guides, templates, and checklists to accelerate your PAM journey.

Further resources you can check out include the following:

- **Explore Delinea Secret Server, the easy-to-use PAM solution, at your own pace.** Start a free, 30-day trial by visiting `delinea.com/products/secret-server`.
- **Build and apply context across all identities with intelligent authorization.** Explore the Delinea Platform at `delinea.com/products`.
- **Benchmark your authorization maturity.** See where you place today by visiting `delinea.com/solutions/privileged-access-management-maturity-model`.

IN THIS CHAPTER

- Explaining identity
- Comparing privileged and non-privileged identities

Chapter 1
Getting to Know Privileged Access Management

Privileged identities are everywhere in the IT environment. They're the building blocks for managing infrastructure, databases, applications, and services that power your business. Yet, for most people, they're invisible.

This chapter gives you the basics of Privileged Access Management (PAM), starting with understanding privileged identities and how they gain privileged access.

Defining Identity as Part of PAM

In an IT environment, privileged identities can be human or non-human. PAM incorporates both types.

Looking at human identities

Human identities include employees as well as third parties, such as contractors, vendors, and partners. Typically, human identities are initially created in identity providers (IdP) such as Microsoft

Entra ID, Ping, or through federation with third-party Identity and Access Management (IAM) solutions.

Human identities that have a high level of privileged access include IT administrators with varying and, at times, overlapping access controls, as seen by the following:

- *Domain administrators* have the highest level of permissions, with unrestricted access to create accounts, modify system files, install software, and make changes to systems across the entire IT infrastructure. Sometimes referred to as a *god-like access admin,* they're the most risky due to the potential for misuse.
- *Superusers,* such as admins for Windows servers, have significant management rights over an IT resource but restricted access to domain accounts. Depending on the operating system (OS), the actual name of a superuser account may be root, administrator, admin, or power users.

Outside of administrators, human users with risky access also need to be monitored and controlled. This includes

- Developers that have access to test and production systems, cloud platforms, as well as software that's used in the development toolchain
- Contractors, vendors, or other third parties that access IT systems for outsourced troubleshooting and support
- Business users that can access privileged data and execute transactions via financial, accounting, or human resources systems and applications
- Business users that have local administrative accounts on workstations, which allow them to do things like download and install applications, change settings and configurations, and execute other commands

Understanding non-human identities

Non-human identities, also known as *machine identities*, are digital entities that run and manage applications, services, and scheduled tasks, IIS application pools (.NET applications), and networking equipment such as firewalls, routers, and switches. Machine identities come in two varieties:

EVERY IDENTITY MATTERS

In the past, only a small group of trusted IT users, typically domain or system administrators, were considered privileged. You knew who these people were and trusted what they were doing. Today, however, virtually every user has some level of privilege, especially when you consider the wide range of access that business users, developers, and cloud administrators have to view, manipulate, and share sensitive data. Oversight is much more difficult.

- **Workloads,** which include virtual Windows, Linux, and Unix machines, applications, containers, code, application programming interfaces (APIs) and AI agents
- **Devices,** which include user workstations, mobile devices, and operational technology

Non-human identities are increasing rapidly, largely due to new technologies, including virtual machines, containerization, APIs, and artificial intelligence (AI) algorithms that create more machine workloads. They represent a substantial and often unmanaged portion of your identity attack surface.

WARNING

In the typical enterprise, anywhere from 45 machine identities exist for every human identity. The proliferation of machine identities has drawn the attention of bad actors who've found creative ways to compromise them, requiring focused effort to prevent, detect, and respond to machine identity-related threats.

What Makes "You" So Special? Privileged versus Non-Privileged Identities

A *non-privileged identity*, or *standard user*, only has enough privileges to perform basic functions that carry little risk to the organization. Privileged access means identities have more permissions. They not only gain initial access to systems but also adjust permissions, configure settings, and change, delete, and extract sensitive, private data. The more privileges an identity has, the more risk it presents to your organization.

Privileged identities, managed by PAM, gain access to systems and resources through two related but distinct processes: authentication and authorization. Access begins with authentication to determine who you are. The user supplies credentials, such as an ID and password, which the system uses to verify the user's identity.

After the user is authenticated, a PAM system evaluates the user's permissions and determines what actions they're allowed to perform or what resources they can access based on predefined rules, roles, or policies. This is called *authorization.*

As part of PAM, organizations may implement one or more of a wide range of access controls. The most common are the following four:

- **Role-based access control:** Determines the authorization for an identity based on pre-defined roles, typically related to job title, organizational structure, or seniority level
- **Policy-based access control:** Access based on defined policies that can incorporate roles, attributes, and other conditions
- **Rule-based access control:** Rules based on conditions such as time, IP address, or other specific criteria
- **Context-based access control:** Considers the context of the access request, such as the user's location, time of access, and the device being used

After the identity is authorized, anyone with privileged access can gain entry to your IT environment. The greater the access they have, the greater the potential blast radius if those privileges are compromised.

REMEMBER

Managing authorization for all the identities in your organization is extremely difficult and time-consuming without some level of automation to support your efforts. Roles aren't static, particularly in matrixed organizations. Access requirements change frequently, and it's impossible for IT teams to keep pace.

In Chapter 2, you dive deeper into the risks of unmanaged privileged access, including the most common challenges that organizations face.

IN THIS CHAPTER

- Listing the attack stages
- Recognizing scenarios that increase your risk of attack

Chapter 2
Understanding the Risks of Compromised Privileged Access

Roughly 80 percent of companies worldwide experience a credential-based attack each year, and 93 percent of victims suffer measurable losses. With numbers like these, clearly, the stakes are high.

Understanding how these types of attacks work can help you prevent a cyber incident from becoming a catastrophe. In this chapter, I explain the attack surface and the stages of an attack that are focused on Privileged Access Management (PAM).

Looking at the Stages of an Attack

The most common cyberattacks progress in stages along what's known as the Identity Attack Chain. Adversaries leverage identities with privileged access to gain entry to your environment. Imagine someone breaking into your house by using your key. After they're inside, things can go from bad to worse.

This section covers those stages.

Stage 1: Credential compromise

In the initial stage of an identity or privilege-based attack, attackers obtain valid credentials (in most cases, a username and password combination) to gain an initial foothold in your organization.

WARNING

Threat actors commonly obtain credentials by conducting reconnaissance on employees, allowing them to find or guess usernames and weak passwords. Social engineering techniques like phishing emails entice employees to enter their credentials into fake websites or click on links that download malware. Attackers may also harvest credentials from code repositories or buy them from access brokers on the Dark Web.

Stage 2: Foothold to deliver payload

In Stage 2, the criminal seeks to escalate. Credentials helped them gain initial access. Now, they need to establish a foothold from which to operate. Commonly, cybercriminals deploy malware that executes code to give them more visibility and more access.

TECHNICAL STUFF

For example, after cybercriminals gain a foothold on a workstation or server, they may download a toolkit like HashCat and attempt an exploit like Pass-the-Hash, which allows them to move around the network and access additional resources. If there are any hashes in memory, say from a help desk admin who has logged in within the last 30 days, the hash of their credential can be captured. Attackers exploit that hash to escalate privileges.

After they're able, attackers commonly deliver a weaponized payload that executes their malicious campaign, such as malware to encrypt data for ransom. The attacker can then control actions remotely on their timetable.

Stage 3: Lateral movement and privilege escalation

Ultimately, adversaries steadily increase access levels through ongoing lateral movement and privilege elevation until they own access to do whatever they desire.

REMEMBER

Attackers want to retain their elevated position in your environment so they can come and go as they please and act on their objectives whenever they want. Because they have elevated privileges, threat actors can operate under the radar and cover their tracks.

Reviewing Scenarios that Increase Your Risk of a Privilege-Based Attack

Many factors can increase the likelihood and impact of a cyberattack. Most of these behaviors happen for convenience, in the name of productivity. People are simply trying to get things done in the fastest way possible, and they bypass cybersecurity best practices as a result.

WARNING

Instances that increase your risk of a privilege-based attack include the following:

- **Exposing passwords:** Cybercriminals celebrate when they find an Excel spreadsheet named Important Passwords stored in a user's files or when they find passwords stored insecurely in browsers.
- **Re-using passwords:** Many people use the same password for multiple devices, applications, and other IT systems. That means that if their password is compromised, a cybercriminal can use it to unlock multiple systems, move laterally, and increase the blast radius of their attack.
- **Overprivileged identities:** When granting access to identities, IT teams often default to what's easiest — a generic role or group. As a result, many identities operating in your environment have more privileges than they require. Not only can a malicious insider cause damage, but also an external attacker can with those privileged credentials.
- **Access creep:** When privileges are granted outside of standard security processes — for example, by application owners — identities may gain more access over time without visibility.
- **Standing access:** Too often, privileges aren't revoked in a timely fashion when a project ends or an employee leaves the organization. That access is left unmanaged and

unsecured. People with a grudge against the company could use their access for nefarious gain. Or, they could simply be a victim themselves and expose credentials that allow entry into your organization.

- **Backdoor accounts:** Knowledgeable insiders such as developers or server administrators may create accounts that allow them rapid access to resources by bypassing usual authentication procedures. If a threat agent finds a backdoor, you would have no way to detect their behavior.
- **Storing credentials:** Developers sometimes store credentials used by machine identities within code, inside applications, or in code repositories. Cybercriminals can find these and use them to gain access.
- **Never changing passwords:** If you don't know exactly what services depend on machine identities, you may be afraid to rotate credentials or reduce privileges for fear of breaking business-critical processes. As a result, many service accounts sit unmanaged, waiting for an attacker to exploit.
- **The dynamic cloud environment:** Most organizations today have a mix of on-premises and cloud resources, often spread across data centers and multiple cloud service providers (CSPs), as well as cloud-based applications.

  
  TECHNICAL STUFF

  In a multi-cloud environment, privileged access becomes much more complex to manage, for a few reasons:

  - A mix of different identity providers, federated apps and services, and local CSPs limit understanding of privileged behavior.
  - Modern cloud environments have intricate permission models with thousands of possible permissions across numerous services.
  - Cloud environments experience rapid shifts with new identities (especially machine identities) created constantly and entitlements provisioned and removed at breakneck speed.

- **Stringent regulatory and insurance environment:** Just as the risk of cyberattacks is increasing so are security controls required by regulators and cyber insurance companies. Compliance frameworks emphasize the need for strong password management, access control, monitoring, and reporting.

REMEMBER

These challenges aren't insurmountable. Any organization can secure privileged access and make an attacker's job more difficult. In Chapter 3, you discover how PAM lowers your risk of privileged-based attacks.

EXAMPLES OF HIGH-PROFILE PRIVILEGE-BASED ATTACKS

You have many reasons to protect privileged access, but take a look at these real-world examples:

- Cybercriminals used a set of stolen credentials to remotely access a large healthcare's systems that weren't protected by multifactor authentication (MFA) and successfully stole a vast amount of private healthcare data. The attack cost the company almost $900 million and had massive repercussions for healthcare providers and patients.
- The breach of a large data storage and analytics platform impacted multiple companies due to shared databases. Attackers used stolen login information to remotely access the company's customer accounts and subsequently breached several other organizations, including a large event ticket sales provider, exposing information for over 500 million users.
- A non-profit media organization was breached after threat actors stole exposed authentication tokens. Because the tokens hadn't been rotated, attackers could use them to gain privileged access.

IN THIS CHAPTER

- Looking at the various PAM approaches
- Getting started with PAM
- Adopting PAM for business productivity

Chapter 3
Developing a Strong PAM Strategy

This chapter helps you develop a comprehensive Privileged Access Management (PAM) strategy to lower your risk of privilege-based attacks. You discover how you can achieve defense-in-depth with multi-layered PAM to tighten your entire attack surface everywhere privileged identities exist in your organization.

You discover the different approaches to PAM and see how you can detect and respond rapidly — even automatically — if a successful attack occurs. Plus, you learn important usability and integration considerations for PAM solutions so you can improve efficiency and productivity.

THE PRINCIPLE OF LEAST PRIVILEGE

The Principle of Least Privilege is foundational to PAM. It means that all identities should have access *only* to the resources, systems, and data they need when they need it. Any additional access is considered excessive and unnecessarily increases your risk. PAM helps you ensure least privilege access. It doesn't just secure the keys to the front door; it also determines exactly what those keys unlock once someone is inside.

Detailing the Three Types of PAM Approaches

The PAM stool has three legs, and each takes a different approach to managing privileged access. The combination of these approaches in a comprehensive, modern PAM solution provides layered defenses for different privileged access scenarios and risk factors.

Privileged account and session management (PASM)

Most organizations launch their PAM program with PASM. In this approach, privileged access is managed via a secure, centralized PAM vault, which discovers, creates, stores, and protects secrets (passwords, keys, certificates) tied to privileged accounts. Privileged users must check out secrets from the vault to gain access to IT resources.

Most organizations begin by vaulting shared privileged accounts and credentials used by their most privileged users (domain admins, server admins, and so on) and then move to other parts of the organization and manage access for all privileged identities, including developers, third parties, and business users, that carry risk.

A PAM vault also manages the life cycle of non-human, machine identities and service accounts and secures their credentials,

such as application programming interfaces (APIs), Secure Shell (SSH) keys, tokens, and certificates. It automatically creates unique, complex privileged credentials, rotates them, and expires them when they're no longer needed.

In addition, PASM enables privileged session management and recording at the vault and gateway level to monitor and report on the use of privileged accounts. In this way, PASM is key to early detection of identity and privilege-based attacks, as well as post-event forensics, auditing, and reporting. PASM allows you to identify the moment in a session recording in which unusual behavior occurs, so you don't need to waste time searching through reams of data in activity logs, hunting for a needle in a haystack.

Privileged elevation and delegation management (PEDM)

In the PEDM approach to PAM, host-level controls on endpoints (including both servers and workstations) stop lateral movement or unwanted privilege elevation. That way, you can block and contain an attack, even if a threat agent or malicious insider steals valid credentials or circumvents your PAM vault.

With PEDM, all users (including domain admins and system admins) operate with standard privileges until they require a higher level of access. When necessary, privilege elevation policies grant just-in-time, just-enough privileges, meaning privileges that exist only for a limited time, under limited circumstances.

PEDM is essential for managing privileged access to Windows and Unix and Linux servers consistently, reducing the power of superusers, and eliminating the potential to create backdoor admin accounts. In addition, it helps you defend against ransomware by limiting local privileges on workstations so users can't install applications or execute commands unless they're part of a pre-approved allow list.

The PEDM approach reduces privilege sprawl by eliminating shared and duplicate privileged accounts, standing access, and excessive privileges. Because privilege elevation policies are tied to unique privileged identities instead of shared privileged accounts, you have more granular oversight of privileged behavior. Additional host-level identity security controls that support the PEDM approach to PAM include multifactor

authentication (MFA), multi-directory brokering and federation, and identity-specific privileged session recording.

Remote privileged access management (RPAM)

RPAM handles access management for external privileged users, including employees who are working remotely and third parties such as vendors and contractors who are part of your extended team. With RPAM, you can register identities outside of your identity stores, grant granular, limited access for those identities, and track and audit identity behavior for fine-grained visibility and central, consistent oversight.

RPAM is a significantly more secure method of granting remote access than traditional VPN software, which typically grants broad access and is complex for users to navigate. Instead, remote users can easily connect to your central PAM vault via a browser. With RPAM, you can manage privileged access for remote users just as you do for on-site employees, with consistent policies, session monitoring, and consolidated reporting.

Asking Questions When Getting Started with PAM

Like any IT security measure, PAM requires both an initial plan to get started and an ongoing program for continuous improvement. As you progress through the process of implementing a PAM technology solution, you should address the key questions in this section.

Who already has privileged access?

You can't manage what you don't know. With PAM, you can find out the status of your attack surface by discovering all the privileged accounts and identities that operate in your environment and their level of access. You may be surprised to find orphaned accounts, default passwords, hard-coded credentials, identities that should've been de-provisioned or removed long ago, unexpected cloud access, and more.

REMEMBER

Understanding what you have and who has access to business-critical assets is a paramount first step to building a PAM strategy.

Who actually needs privileged access?

Collaboration among IT, security, and business teams is necessary to determine which employees, vendors, and machines in your environment truly need privileged access to an organization's business-critical systems, data, and resources. This access could include teams like system administrators, developers, and security teams as well as third-party vendors and leadership who may need limited access and for a specific period of time.

When do they need that access?

How long is a privileged user expected to stay on a sensitive project? How long do you expect a third party to require access for troubleshooting? For machine identities, backup systems typically run at scheduled times, so standing access is unnecessary. Integrity validation and vulnerability scanning, for example, probably follow a scheduled penetration test. After you know these answers, you can set timelines and automatic expiration dates for privileged access.

Who is the human owner of each non-human identity?

To avoid falling off the radar, each non-human or machine identity should have a designated human owner. That person should know all dependencies related to the account and be responsible for removing access when it's no longer needed. All dependencies and ownership should be documented, and that information should be easily accessible to PAM administrators for central reporting and oversight.

Do you have to meet regulatory compliance or cyber insurance requirements?

PAM best practices are prioritized in government and industry regulations such as the following:

- The National Institute of Standards and Technology (NIST)

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- The Payment Card Industry (PCI)
- The Sarbanes-Oxley Act of 2002 (SOX)

These regulations are required for public companies in the United States to meet Securities and Exchange Commission (SEC) requirements to demonstrate effective cybersecurity practices. Even if you're not bound by regulatory requirements, chances are that your cyber insurance provider will investigate your access management practices when determining whether to grant you a policy and determine how much to charge you for it.

TIP

Check specific requirements for password management, access controls, application controls, and behavior monitoring and reporting to be sure your PAM policies and controls align with any rules you must follow. To demonstrate compliance, continuous monitoring, periodic reviews, and the use of automated tools provide immutable audit logs and reports you can share with auditors and insurers.

What is the risk if access is compromised?

Some systems within your organization represent greater technical and business risk than others. Access to systems that hold protected data or run critical business processes requires tighter control and more granular oversight.

REMEMBER

Understand your risk exposure so you can determine the appropriate level of preventive, mitigating, and detective PAM controls. With PAM, you can classify levels of access based on a risk ranking system. Consider not only the risk of an identity having access to each system individually, but also the *combined* risk of access across all systems — known as an *identity's effective access.*

How will you spot unusual privileged behavior?

Understanding privileged behavior allows you to identify possible access abuse or misuse. PAM solutions can determine a baseline for privileged behavior and let you know where there are anomalies outside the expected parameters by sending contextual alerts

when suspicious activities arise. For example, you may want to know if privileged users are attempting to log in unsuccessfully, if they're attempting to gain access for the first time in months, if they're using a different IP address, or if they're logging in at unusual hours. Any of these things can be signs of an attack in progress.

REMEMBER

If a breach does occur, monitoring privilege use helps you take immediate action to reduce dwell time. Post-attack digital forensics help you identify the root cause of the breach and identify critical controls that reduce your risk in the future.

How will you keep up with changes that impact your risk?

If there's one thing you can always count on, it's change! Your attack surface is constantly changing with new people joining, changing roles, or leaving the organization, new business processes, new systems connected, and — especially in a cloud world — new machine identities being created all the time.

With PAM, continuous discovery helps you stay on top of all the identities and privileges in your environment so you can ensure they're under centralized control.

TIP

Choose a PAM solution that can scale as your organization grows, whether you manage hundreds or hundreds of thousands of privileged credentials, secrets, workstations, and servers.

How will you measure and communicate results?

Consider how you plan to demonstrate effective management of privileged access to your stakeholders. Some of your stakeholders may want to see granular reports while others may want a high-level understanding. To measure progress and demonstrate compliance with auditors, you must be able to create and share reports. You should be able to immediately report on your system health, user activity, and priority issues with clear visualizations and ad hoc queries so everyone understands the information and shares a single source of truth.

Accelerating PAM Adoption and Ensuring Business Productivity

You've probably heard the old cybersecurity adage that people are the weakest link. Well, yes, many privilege security risks do indeed come down to poor password and identity hygiene. The fact is, when security is too complex to use, people find ways around it.

Instead of blaming the user for security failures, PAM takes the responsibility off their shoulders. It empowers people to do the right thing while staying productive. Today's PAM works automatically and intelligently behind the scenes, based on policies you define and control centrally. That way, users don't have to interrupt their workflows to access the resources they need to do their jobs. In fact, they don't need to remember or even see passwords.

TIP

At the same time, building awareness of the importance of PAM is crucial. Make sure you provide access security training to all privileged users. For example, write a formal PAM policy including how access is determined and why, and share it widely. Make sure you get buy-in and support from your executive team by educating them as well.

Understanding the key integrations for operational efficiency

For your IT and security teams, integrating PAM within your overall identity security program and IT stack saves time and money. Namely, integrations with identity stores like Active Directory and other identity providers, Identity and Access Management (IAM) solutions and MFA solutions streamline governance throughout the entire identity life cycle.

In addition, integrations with ticketing and incident response systems make it easier to identify privilege-based attacks and respond to contain the damage. If you suspect an identity or privilege-based attack is underway, you can automatically enforce additional MFA, require more layers of approval, or even remove privileged access pending investigation.

Who's responsible for PAM?

Traditionally, PAM and other identity security processes and controls have been managed in organizational silos with separate workflows and tools that don't share data. This fragmentation has led to inefficiency, duplication of spend, and wasted time.

For example, teams responsible for authorization have relied on PAM solutions. Meanwhile, those responsible for identity provisioning typically manage authentication using a variety of tools for IAM, MFA, federated identities, and Single-Sign-On (SSO). Incident response teams and security operations centers have their own tools and processes and often don't understand the full context of alerts they receive.

In many organizations, these teams are starting to work together more closely and so are the technology solutions that support them. When you bring authorization and authentication together you can realize the benefits of defense-in-depth to provide stronger identity security for your organization. The key is ensuring your solutions are fully integrated and interoperable so they share information back and forth and are always up to date.

IN THIS CHAPTER

- Rolling out your capabilities in stages
- Making sure you have high availability
- Measuring results
- Preparing and being ready for change
- Choosing a good PAM partner

Chapter 4
Ten Best Practices for a Successful PAM Journey

By taking a proactive approach to Privileged Access Management (PAM), you can be better prepared to secure your attack surface and protect critical assets in the coming years with less complexity, cost, and operational overhead. Part of a proactive approach is following tried and true best practices for your success.

Face Facts

Discovery helps you build a realistic picture of your security posture and identify vulnerabilities. After you know the risks associated with privileged access, you can prioritize your PAM implementation accordingly.

Roll Out PAM Capabilities in Stages

You don't need to boil the ocean. Simply getting started with an automated, enterprise-ready PAM solution has an immediate impact on your organization by eliminating manual password and access control practices that are dangerous and inefficient.


TIP

Begin by addressing aspects of your business that carry the greatest risk. Many organizations start with one team or set of IT resources and then move to others.

Balance Security and Productivity

You'll have greater adoption if you put the mechanics of PAM behind the scenes and allow all users to do their jobs without friction. Your IT operations, security, and audit teams will also be more excited about a PAM program if you show them how much time they can save by eliminating tedious, manual work.

Prioritize High Availability

If you can't get to your PAM vault, you can't access business-critical resources.


TIP

Make sure any PAM vault you choose provides redundancy and options for break-glass scenarios, so you can ensure business continuity.

Reinforce PAM with Other Identity Security Practices

Enhance your PAM program with additional layers of identity protection, such as multifactor authentication (MFA), which can be required at initial login and privilege elevation, depending on the level of risk.

Decide How You'll Measure Results

Consider the types of reports you want to create and share with your executive team, auditors, and insurers. Make sure you're collecting the information you need to set goals and show results.

Prepare for Change with Dynamic Policies

As the IT environment becomes even more distributed and complex, static controls won't be able to keep pace. In the future, organizations will only be able to achieve scalable, risk-based PAM with intelligent, dynamic policies.

Unlike traditional static methods, in which access control decisions are based on predefined roles and permissions, dynamic authorization adds security context to the access request, such as the user's location, device, time of access, and current threat levels. Dynamic authorization has an inherent, risk-based model for making decisions. As risk scores change, so do access requirements.

Leverage AI

REMEMBER

AI-enhanced solutions play a critical role in the PAM landscape and are a vital strategy for cyber resilience. When you leverage AI, you can support repeatable workflows, early detection, and automated threat remediation.

Even today, emerging AI capabilities are bringing together the skills and knowledge of multiple experts — PAM teams, security analysts, detection engineers, incident response experts, your own privileged session history, and patterns across the industry — to do much more than any organization's internal team can.

Build on a Solid Foundation

Select a PAM solution with modular capabilities and a common platform so you can grow at your own pace without having to redo any work you've already put in. As attackers get more sophisticated, PAM is adapting fast, and you need to be ready.

Choose a Trusted Partner

You don't have to go it alone. Partner with a PAM provider with an easy-to-use solution that can be deployed quickly for a fast time to value. After you get started and prove the case, you can grow your PAM program, reduce risk, and demonstrate measurable results.

FREE Privileged Access Management (PAM) Resources from Delinea

Free educational resources include original research on privilege and identity-based attacks, assessment tools to discover vulnerabilities and benchmark your PAM practices, as well as how-to guides, templates, and checklists to accelerate your PAM journey.

Explore Delinea's easy-to-use PAM solution at your own pace

See how Delinea Secret Server secures, identifies, manages, monitors, and audits privileged accounts and identities.

Start a free, 30-day trial.

Build and apply context across all identities with intelligent authorization

Discover the first cloud-native identity security solution that delivers intelligent, centralized authorization to reduce risk, ensure compliance, and enhance productivity.

Explore the Delinea Platform

Benchmark your authorization maturity

Learn the stages of maturity and chart your progress as you embed PAM best practices in your cybersecurity strategy.

See where you place today

delinea.com

Protect your organization from cyber threats

PAM replaces the need for manual password management and static access control with seamless automation, stronger security, and continuous oversight. With PAM, you can employ consistent, policy-based controls to manage privileged identity behavior. PAM policies determine what systems authenticated identities are authorized to access and what they can do with that access.

Inside...

- How the definition of PAM has evolved
- How to combat privilege-based attacks
- Steps to implement your PAM program
- Advice to gain buy-in and drive adoption
- Learn about privileged identities

Delinea

Joseph Carson is a multi-award-winning cybersecurity professional and author with 25+ years' experience in enterprise security. Joe's an active member of the cybersecurity community frequently speaking globally at cybersecurity conferences, often being quoted and contributing to global cybersecurity publications.

ISBN: 978-1-394-29092-5
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.