Brought to you by:

Delinea

Privileged Access Management

for dummies®

A Wiley Brand

Grasp Privileged Access Management (PAM)

Develop a PAM security strategy

Top ways to protect your organization

Joseph Carson, CISSP

Delinea Special Edition

About Delinea

Delinea is a leading provider of privileged access management (PAM) solutions for the modern, hybrid enterprise and makes privileged access more accessible by eliminating complexity, enforcing Zero Trust, and seamlessly defining the boundaries of access. Delinea simplifies security, ensures compliance and reduces risk for thousands of customers, over half the Fortune 100, and the world's largest financial institutions, intelligence agencies and critical infrastructure companies. For more information, go to www.delinea.com

Privileged Access Management

Delinea Special Edition

by Joseph Carson, CISSP

for dummies®
A Wiley Brand

Privileged Access Management For Dummies®, Delinea Special Edition

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

ISBN: 978-1-119-88722-5 (pbk); ISBN: 978-1-119-88723-2 (ebk). 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:
Carrie Burchfield-Leighton

Sr. Editorial Manager: Rev Mengle

Production Editor:
Mohammed Zafar Ali

Acquisitions Editor: Ashley Coffey

Business Development Representative: Matt Cox

Introduction

The increase in sophisticated, targeted security threats by both external attackers and malicious insiders have made it extremely difficult for organizations to properly protect critical and sensitive information. The task of protecting these assets has only grown harder as IT environments have become more complex and widely distributed across geographic locations and in the cloud.

Many recent high-profile breaches have one thing in common: They were accomplished through the compromise of credentials. In many cases, end-user passwords are initially hacked through various social engineering techniques. Then permissions are escalated to gain access to more privileged accounts — the keys to the kingdom. This unauthorized access can easily go undetected for weeks or even months, allowing cybercriminals to see and steal information at their convenience.

Unfortunately, many IT users lack a full understanding of how privileged accounts function, as well as the risks associated with their compromise and misuse. That makes them and their organizations much more vulnerable to potential monetary and reputational damage from increasing threats.

About This Book

This book gives IT professionals a practical understanding of Privileged Access Management (PAM). It describes what privileged accounts are, where they reside throughout an IT environment, and how they function. Most important, this book explains the risks associated with these accounts and how to best protect them from cybercriminals and malicious insider threats.

This book has been written for IT administrators, systems administrators, and security professionals responsible for protecting their organizations from security threats. It assumes a basic level of IT expertise and experience in managing IT networks and exposure to the use of privileged accounts and passwords as part of daily tasks.

That said, this book may also be helpful in educating business users and others as to the importance of privileged account security 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

Indicates more technical information that is of most interest to IT and system administrators.


TIP

Points out practical advice that will save 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.

Where to Go from Here

IT professionals seeking more information about PAM and password security can learn more at the Delinea website: `www.delinea.com`.

Resources include several free tools for discovering password vulnerabilities on Windows and Unix platforms along with free security policies, Weak Password Finder Tool, online security training, and benchmarking tools to help measure the effectiveness of your PAM and general security practices.

IN THIS CHAPTER

- Differentiating privileged accounts from user accounts
- Understanding the types of privileged accounts
- Managing and protecting privileged account passwords

Chapter 1
Getting to Know Privileged Access Management

Privileged accounts are everywhere in the IT environment. They give IT the building blocks for managing vast networks of hardware and software that power the information-driven world. Yet for most people, they're invisible. This chapter gives you the basics of Privileged Access Management (PAM) — understanding privileged accounts, what they do, and why it's so important to protect access to them as the "keys to the kingdom" of your growing information empires.

Understanding a Privileged Account

There are two major categories of accounts. The *user account* takes on the form of an online bank or corporate account used by an employee. Every user account has a password associated with it that enables you to access that account and conduct your business. Passwords exist to protect your information from anyone else accessing your user account without your permission.

USER VERSUS PRIVILEGED ACCOUNT

A user account typically represents a human identity such as an Active Directory user account and has an associated password to restrict access to the account. There is usually a single account password per human user that needs to be memorized by the person.

A privileged account can be human or non-human and does not necessarily represent human beings. An example includes application accounts that are often shared by IT staff. Privileged account passwords should be set to very large, complex values and stored in a secure vault. When properly stored or vaulted, these accounts don't need to be memorized.

A *privileged account* can be human or non-human; they exist to allow IT professionals to manage applications, software, and server hardware. Privileged accounts provide administrative or specialized levels of access based on higher levels of permissions that are shared. Some types of non-human privileged accounts are application accounts used to run services requiring specific permissions. In many cases, user accounts can also have elevated or administrative privileges attached to them.

WARNING

Like user accounts, privileged accounts have passwords to control access. The problem with user and privileged account passwords is that many tools exist to aid cybercriminals in cracking these passwords. After a cybercriminal gets access to a password-protected system, the damage can be catastrophic. Hijacking privileged accounts gives attackers the ability to access and download an organization's most sensitive data, distribute malware, bypass existing security controls, and erase audit trails to hide their activity.

In most organizations, IT staff will have one account with standard-level permissions, then another account for performing operations that require elevated permissions. IT accounts that are different types of privileged accounts include

- Local or Domain Admin accounts that manage servers
- Domain Admin accounts that typically control Active Directory users

- SA accounts that are system admin accounts that help manage databases
- Root accounts that manage Unix/Linux platforms
- Accounts that run and manage Windows applications, services, and scheduled tasks
- IIS application pools (.NET applications)
- Networking equipment accounts that give access to firewalls, routers, and switches

An example of a type of privileged account is a service account that requires special privileges to run, schedule a task, or an application. These accounts are often used in a one-to-many situation, where a single account may be used across an entire organization to run many services or applications.

WARNING

Unfortunately, service accounts are often misused. To keep things running and avoid application downtime or insufficient privileges, they are often configured with high levels of privilege and passwords that are never changed and never expire. These common practices create a dangerous vulnerability for any organization.

Who Uses Privileged Accounts and Where They Are Located

The typical user of a privileged account is a system administrator (sysadmin) responsible for managing an environment or an IT administrator of specific software or hardware. These individuals can perform the following:

- Install system hardware/software
- Access sensitive data
- Reset passwords for others
- Log into all machines in an environment
- Use elevated privileges to make changes in IT infrastructure systems

Because privileged accounts are used by systems administrators to deploy and maintain IT systems, they exist in nearly every

connected device, server, database, and application. In addition, privileged accounts extend well beyond an organization's traditional IT infrastructure to include employee-managed corporate social media accounts.

That means organizations can typically have two to three times more privileged accounts than employees. And, in many cases, some privileged accounts within an organization may be unknown, unmanaged, and, therefore, unprotected.

Why Privileged Accounts Are Prime Targets for Cybercriminals

Industry analysts estimate that from 60 to 80 percent of all security breaches now involve the compromise of user and privileged account passwords. Yet, traditional methods of identifying and managing privileged accounts still rely on manual, time-consuming tasks performed on an infrequent or ad-hoc basis.

Even in the most sophisticated IT environments, privileged accounts are all too often managed by using common passwords across multiple systems, unauthorized sharing of credentials, and default passwords that are never changed — making them prime targets for attack.

These practices can easily compromise security because for most attackers taking over low-level user accounts is only a first step. Their real goal is to take over privileged accounts so they can escalate their access to applications, data, and key administrative functions. After they gain access to privileged account credentials, cybercriminals can easily conceal their activities in the guise of a legitimate administrative user.

In Chapter 2, you find out how the bad guys are getting their hands on user and privileged account passwords and what you can do to stop them.

IN THIS CHAPTER

- Understanding how cybercriminals get passwords to your privileged accounts
- Looking at what happens when a privileged account gets hacked
- Realizing why traditional IT security methods aren't enough

Chapter 2
Looking at the Dangers of Compromised Privileged Accounts

Privileged accounts represent the "keys to the kingdom" of any IT environment providing special access to sensitive information stored and used to run the business. It only takes one compromised privileged account for an attacker to gain access to virtually any information within an organization's IT network.

When attackers compromise a privileged account, they can perform malicious activity, steal sensitive information, commit financial fraud, and often remain undetected for weeks or months at a time. Most cybersecurity breaches go undetected for more than 200 days, a period of time known as the *dwell time*.

The danger is obvious, but it's important to understand how cybercriminals and malicious insiders can compromise any end-user or privileged account and "escalate" their privileges to steal information and damage the reputation of any organization.

How Cybercriminals Compromise Your Privileged Accounts

With up to 80 percent of breaches resulting from stolen or weak password credentials, the path to compromising privileged accounts is pretty simple. Cybercriminals' most preferred pathway to privilege exploitation is as follows:

1. **Compromise an end-user account.**

   Cybercriminals use malware or social engineering to get access to desktops, laptops, or servers. Employees are typically fooled by phishing scams that ask them to click on a link, download a piece of software with malware hidden inside, or enter their password credentials into fake websites. In many cases, these scams appear to be legitimate requests from an employee's manager, company executive, or another trusted source.

2. **Capture a privileged account.**

   Attackers need a privileged account (local Windows admin/service account) to move around. After an employee's password is captured by cybercriminals, the perpetrator can log onto a network and simply bypass many of the traditional IT security controls because they *appear* as a user with legitimate credentials. Most common hacker techniques include Man in the Middle or Pass the Hash attacks to elevate privileges.

3. **Go anywhere on the network.**

   With privileged credentials, cybercriminals can access core network services and remain undetected for weeks or months, spreading malware or stealing valuable information.

WARNING

Cybercriminals also can compromise accounts from end-users or privileged accounts that fail to modify and change default passwords. A Delinea survey, for example, indicated more than 20 percent of companies fail to change default passwords, such as "admin" and "12345."

Additionally, many organizations rely on humans to generate passwords. This results in weak passwords that are easily guessed or "cracked" by cybercriminals with automated computer tools. And, to compound the problem, many humans reuse the same password for several different accounts.

Knowing What Happens When You Get Hacked

When a privileged account gets compromised, it allows the attacker to impersonate a trusted employee or system and carry out malicious activity without being detected as an intruder. After attackers establish a breach, they typically use compromised privileged accounts to perform reconnaissance and learn about the normal routines of IT teams. This includes observing regular schedules, security measures in place, and network traffic flow. Eventually the attacker can get an accurate picture of the entire network and its operations.

As attackers learn more about the targeted network, they can blend in with normal operations, avoid detection, and make sure they don't trigger any network security alarms. They learn how to avoid detection, and then their next step is to establish ongoing access by installing remote access tools. These tools enable attackers to return anytime they wish and perform malicious activities without raising an alarm.

Depending on the motive of the attackers, they can use privileged accounts to

- Damage system functions or disable access by an IT administrator
- Steal sensitive data for fraud or reputation damage
- Poison data
- Inject bad code
- Introduce malware
- Deploy Ransomware

HIGH-PROFILE CYBERSECURITY BREACHES

Want to know the impact of a major security breach? Here are some high-profile examples:

- In 2021, Texas-based SolarWinds Corp said the sprawling breach stemming from the compromise of its flagship software product cost the company at least $18 million in the first three months.
- In 2021, REvil's $70 million ransomware price in the Kaseya cyber-attack became the largest-ever ransom demand publicly known, surpassing a $50 million ransom demand in March after REvil compromised PC giant Acer.
- In 2020, Twitter saw $1.3 billion in market value wiped out after a massive hack targeted Barack Obama, Kim Kardashian, Elon Musk, and other prominent accounts.

Because a compromised privileged account appears to be a legitimate user, it's very difficult to find the root cause or perform digital forensics when the breach is eventually detected.

WARNING

While most organizations have an incident response plan in place to handle system breaches, they haven't evaluated the risk of a privileged account being compromised. Chapter 3 explains the steps you can take to prevent privileged accounts from being compromised and exploited.

Needing More than Traditional IT Security to Stop Attacks

Until now, most organizations have protected their information with traditional security perimeter tools, such as firewalls, antivirus, and intrusion detection solutions. But in the age of fast evolving cloud, mobile, and virtualization technologies, trying to build a fence or moat around critical assets no longer works.

In the digital workplace and social society, people are constantly sharing information and being exposed to social engineering and targeted spear phishing attacks aimed at getting your user passwords and credentials. After your identities are stolen, attackers can easily bypass the traditional security perimeter undetected and escalate the exploitation of privileged accounts.

Hacking privileged credentials can mean the difference between a simple perimeter breach and one that could lead to a cybercatastrophe. Therefore, the "new cyber security perimeter" must focus on protecting the identity and access of employees, contractors, and third-party partners. As many organizations have shifted to working remotely, the perimeter is gone. Identity is the new perimeter, and access is the new security.


TIP

Effective policies and best practices with Privileged Access Management (PAM) can help your company accelerate new technology adoptions and at the same time help avoid becoming the next victim of cybercrime. Check out Chapter 3 for more information on how to protect privileged account passwords and what you can do to stop them from being compromised.

IN THIS CHAPTER

- Answering critical questions when getting started
- Developing a comprehensive PAM security strategy
- Integrating PAM with your other security and operational functions

Chapter 3
Managing and Protecting Your Privileged Accounts

This chapter helps you answer critical questions that help develop a comprehensive Privileged Access Management (PAM) solution tailored to your business needs. Be sure to include important integration considerations so you can develop a holistic security approach to secure and protect privileged accounts.

Critical Questions to Answer When Getting Started

Like any IT security measure designed to help protect critical information assets, managing and protecting privileged accounts requires both a plan and an ongoing program. You must identify which privileged accounts should be a priority in your organization, as well as ensuring that those who are using these privileged accounts are clear on their acceptable use and responsibilities. Before you can successfully implement a PAM security solution, the planning phase must answer several key questions:

- **How do you define a privileged account for your organization?** Every organization is different, so you need

to map out what important business functions rely on data, systems, and access. A useful approach can be to reuse the disaster recovery plan that typically classifies important systems, which need to be recovered first, and then you can identify the privilege accounts for those systems. Classifying privileged accounts at this stage is good practice because this helps identify and prioritize privileged accounts for the business and will make later decisions easier when it comes to applying security controls.


TIP

Because privileged accounts play such an important role in running IT, make sure to align your privileged accounts to business risk and operations. Understanding who has privileged account access, and when those accounts are used, helps define your security posture.

When you know when high-risk accounts are in use, IT security managers can tell when and where sensitive information could be exposed. Visibility into how privileged accounts are used helps organizations quickly identify security risks and exposures and make better decisions.

- **Who needs access to your privileged accounts?** Privileged accounts should be categorized as human, applications and services, systems, and infrastructure accounts. These classifications will determine the level of interaction and security controls applied to each privileged account. For example, when considering human interaction, think about if your employees ever need to know the password or if they're required to check out the password before use. For applications and systems, ask yourself how often rotating the passwords is required and if the path to the system is static so you can restrict IP addresses that can use the privileged accounts.
- **Do you rely on third-party contractors that need access?** Third-party contractors that need access to privileged accounts can be one of the highest risks because you don't have full control over how they access and manage privileged accounts. Many of the breaches in recent years resulted from stolen or hacked contractor laptops that housed data such as personal identifiable information like credit cards, home addresses, and employee health records — all of which get exposed. Some major data breaches that resulted in massive consequences include

both the SolarWinds and Kaseya breaches in 2021 that used third parties in the supply chain.

- **Do you set time windows for privileged account usage?** Accounting systems, for example, may only require access at the end of the month or quarter. Backup systems typically run at scheduled times. Integrity validation and vulnerability scanning probably will follow a scheduled penetration test. Knowing when specific privileged accounts are supposed to be used indicates normal behaviors that allow you to identify possible abuse or misuse.
- **What happens if privileged accounts are compromised by an outside attacker?** Do you have an incident response plan in case privileged accounts are compromised? Many organizations aren't prepared when an account is breached and typically default to simply changing privileged account passwords or disabling the privileged account. That's not enough.


REMEMBER

Privileged accounts are your "keys to the kingdom." So if your privileged accounts are compromised by an outside attacker, cybercriminals can install malware and even create their own privileged accounts. If a domain administrator account gets compromised, for example, you should assume that the entire active directory is vulnerable. That means restoring the entire active directory so the attacker can't easily return.

- **What's the risk of privileged accounts being exposed or abused by an insider?** Protecting privileged accounts from insider misuse or abuse should focus on your most critical systems. Most employees, for example, shouldn't be given access to *all* critical systems at the same time, including production systems, backup systems, and financial systems. And, employees changing jobs within your organization shouldn't be able to keep the same access from their previous roles.


TECHNICAL STUFF

The highly-publicized exposure of the National Security Agency's classified government information by Edward Snowden in 2013 is a prime example of how unauthorized access by an insider can be just as devastating as any attack by outside cybercriminals.

- **Do you have an IT security policy that explicitly covers privileged accounts?** While a lot of companies have a corporate IT policy in place, many still lack acceptable use and responsibilities of privileged accounts.

TIP

Treat privileged accounts separately by clearly defining a privileged account and detailing acceptable use policies. Be sure to include who's responsible and accountable for using privileged accounts.

- **Do you have to comply with government or industry regulations?** If your company must comply, then it's critical to get privileged accounts secured. Many organizations must undergo regular audits to comply with internal policies and government or industry regulations. That means demonstrating that your privileged accounts are audited, secured, and controlled because cybercriminals can access sensitive information, such as credit cards, health records, or financial information.
- **Are you actively reporting to your CISO on privileged account use and exposure?** If you can't properly observe what's going on with your privileged accounts, you increase your risk of insider abuse and letting outside attackers escalate privileges after they've gotten a user password. If a breach does occur, monitoring privileged account use helps digital forensics identify the root cause and identify critical controls that can be improved to reduce your risk of future cybersecurity threats.

Developing a Comprehensive PAM Security Strategy

After you've asked (and hopefully answered) the set of questions about PAM (see the preceding section), you're much better prepared to actually implement the security measures that will best protect your IT environment. This section gives you the steps to develop a comprehensive PAM security solution.

Build on a solid foundation

Building a solid foundation to manage and secure privileged accounts helps organizations be more scalable and flexible when adopting new technologies. It is key to protecting critical assets and ensuring only trusted and authorized employees access the right data and systems.

TIP

Two important action items in building this foundation are

- **Providing cybersecurity awareness training to those who will be using and are accountable for privileged accounts:** Your training should emphasize the critical importance of privileged account security and include IT security policies specific to your organization. Make sure you get buy in and support from your executive team by educating them as well.
- **Looking for tools that help you automate the discovery, security, and protection of privileged accounts:** Any software tools you evaluate should give you the ability to continuously discover privileged accounts, store privileged account passwords in a safe "vault," automatically rotate passwords regularly, and effectively monitor and report on privileged account activity.

Establish PAM security policies and controls

An important step in establishing PAM security is setting up some policies and controls, such as the following:

- **Change default IDs and passwords for many built-in privileged accounts.** This should be one of your very first tasks in improving PAM security. Research shows one in five organizations have never changed default passwords, such as "admin" or "12345," on privileged accounts. These default credentials are a top priority for cybercriminals because it's so easy to crack their passwords.
- **Write a formal password policy for privileged accounts to assure accountability.** Policies should be based on the categorization and classification of privileged accounts specific to your organization. You can find policy templates online so you don't have to start from scratch.
- **Don't allow privileged accounts to be directly shared.** Shared credentials among IT administrators make it very easy for an attacker to escalate permissions and gain access to sensitive information. Privileged account access should be limited by time, scope of permissions, and approvals needed.

For example, when employees go on vacation, they should be able to assign or delegate the privileged accounts for their roles to another colleague. But security controls should restrict how long and exactly what their colleagues can do with those accounts. This could even mean that the colleague may never even see the account password.

- **Monitor and record sessions for privileged account activity involving sensitive data or systems.** This helps enforce proper behavior and avoid mistakes by employees and other IT users because they know their activities are being monitored. Recorded sessions are also invaluable when discovering the cause of a breach after it's been detected.
- **Control new privileged account creation with a formal review and approval process.** Because external attackers or malicious insiders often try to create and embed new privileged accounts, you need to strictly control the process. The creation of any new privileged account should be subject to specific reviews and approvals involving a peer or supervisor review. Automated software can also run periodic discovery to identify new or unauthorized privileged accounts.
- **Evaluate your privileged accounts to set appropriate expiration dates.** This policy helps prevent what's known as *privileged access creep* where users accumulate privileges over time that may not still be required. You should review and disable privileged accounts that aren't appropriate for specific users — especially for accounts used by third-party contractors that are no longer needed.
- **Implement privileged account "on-demand" usage instead of "always-on" availability.** Privileged accounts should only get used for a specific task or purpose. On-demand privileged account access means the user can't access an account directly but must go to a change management or control point. Automated PAM software allows you to ensure that IT administrator employees will only use privileged accounts for their intended purposes.

  The on-demand process is typically known as an account checkout, approval, or least-privilege model that requires an administrator to provide a business reason for privileged account usage. Even when access is granted, it should be limited to standard account privileges that get elevated only when a specified task is necessary. This significantly reduces the risk of privileged account abuse or compromise.

Ensure ongoing improvement

This section gives you a few ways to ensure that you have ongoing improvement in auditing privileged accounts and demonstrating compliance.

Audit and analyze privilege account activity

Examine how privileged accounts are being used through audits and reports that help spot unusual behaviors that may indicate a breach or misuse. These automated reports also help track the cause of security incidents, as well as demonstrate compliance with policies and regulations.

Auditing of privileged accounts gives you cybersecurity metrics that provide executives, such as the chief information security officer (CISO), with vital information to make more informed business decisions. The combination of auditing and analytics can be a powerful tool for reducing your privileged account risks and exposure to compromise.

Demonstrate compliance with regulations

Demonstrating compliance with regulations is essential in highly regulated industries or when satisfying government mandates. PAM security is now considered an essential part of any overall cybersecurity protection strategy.

Keep discovering privileged accounts

You need a process and automated tools to continuously identify new privileged accounts and account changes made in your network. It's the only practical way to maintain the visibility and control necessary to protect your critical information assets.

Integrating PAM with Your Existing Security Controls

Like so many cybersecurity measures, PAM is but one vital component in your strategy. To function effectively, it's crucial to integrate PAM into your organization's other security controls to provide a more holistic cybersecurity blanket that protects you from evolving threats.

Integrating PAM as part of the broader category of Identity and Access Management (IAM) ensures automated control of user provisioning along with best security practices to protect all user identities. PAM security should also be integrated with Security Information and Event Management (SIEM) solutions. This provides a more inclusive picture of security events that involve privileged accounts and gives your IT security staff a better indication of security problems that need to be corrected or those that require additional analysis.

REMEMBER

PAM can also be used to improve insights into vulnerability assessments, IT network inventory scanning, virtual environment security, identity governance, and administration and behavior analytics. By paying special attention to privileged account security, you can enhance all your cybersecurity efforts, helping to safeguard your organization in the most efficient and effective way possible.

By implementing a comprehensive plan for PAM security, you can protect your organization from cyberthreats. Delinea's own survey of cybercriminals confirmed that limiting access to privileged accounts makes the cybercriminal's job much more difficult — and your organization much more secure.

WHAT'S NEXT FOR PAM?

The IT categories of PAM and IAM will likely converge over the next few years. That means users will have a digital identity that works across not only a single employer but also multiple industries and governments. Imagine a digital identity that you could conveniently use for voting, banking, traveling, unlocking doors, starting a car, riding public transportation, or accessing healthcare services. Block chain technologies within IAM are emerging now that provide nonrepudiation and integrity for users to access all these things — delivered from the cloud as a service.

PAM is also encompassing behavior analytics to help establish trust levels for employees, third-party companies, multiple applications, and network systems. PAM is a major enabler of a Zero Trust Strategy. These capabilities take identity and trust verification to a whole new level of confidence in managing cybersecurity in the near future.

IN THIS CHAPTER

- Making the cybercriminal's job more difficult
- Choosing a partner to help implement your PAM solution

Chapter 4
Top Ways to Protect Your Organization

Privileged Access Management (PAM) doesn't have to be an insurmountable challenge. Any organization can control, protect, and secure its privileged accounts (and make the cybercriminal's job more difficult) with these practical tips:

- **Steer clear of manual methods for PAM:** Too many organizations today still rely on Microsoft Excel spreadsheets to keep track of privileged account passwords and share them among employees. These manual practices are dangerous and inefficient. Automated PAM software solutions can be installed quickly and managed with minimal effort. You save time and money and greatly increase protection from malicious hackers and insiders.
- **Educate employees:** The weakest security link in most organizations is humans. As more sophisticated social engineering and phishing attacks have emerged, companies need to expand their IT security awareness programs beyond simple online tests or signoffs on security policies. As personal mobile devices are increasingly used for business purposes, educating employees on secure behaviors has become imperative.

- **Discover and automate the management of privileged accounts and SSH (Secure Shell) keys:** Use a dedicated PAM software solution and start by focusing on the most critical and sensitive privileged accounts, and implement continuous discovery to curb privileged account sprawl, identify potential insider abuse, and reveal external threats. This helps ensure full, ongoing visibility of your privileged account landscape crucial to combatting cybersecurity threats.
- **Limit IT admin access to systems:** Limit access through a *least-privilege strategy,* meaning privileges are only granted when required and approved. Enforce least privilege on end-user workstations by keeping end-users configured to a standard user profile and automatically elevating their privileges to run only approved applications. For IT administrator users, you should control access and implement super user privilege management for Windows and UNIX systems to prevent attackers from running malicious applications, remote access tools, and commands.
- **Protect privileged account passwords:** Proactively manage, monitor, and control privileged account access with password protection software. The solution should automatically discover and store privileged accounts; schedule password rotation; audit, analyze, and manage individual privileged session activity; and monitor password accounts to quickly detect and respond to malicious activity.
- **Limit privileged and unknown applications:** Application accounts need to be inventoried and undergo strict policy enforcement for password strength, account access, and password rotation. Least-privilege and application control solutions enable seamless elevation of approved, trusted, and whitelisted applications while minimizing the risk of running unauthorized applications.
- **Choose a partner for your PAM solution:** Implement a comprehensive PAM solution with a trusted partner to help you control access to systems and sensitive data, comply with policies and regulations, and ultimately make your company safer.


TIP

Look for software solutions that automate the identification and understanding of risk to your privileged accounts, along with continuous monitoring, recording, and secure storage.

Protect your organization from security threats

Sophisticated, targeted security threats by both external attackers and malicious insiders have made it extremely difficult for organizations to properly protect critical and sensitive information. The task of protecting these assets becomes harder as IT environments get more complex and widely distributed. *Privileged Access Management For Dummies,* Delinea Special Edition, helps you manage IT networks and exposure to the use of privileged accounts and passwords.

Inside...

- Types of privileged and user accounts
- Manage and protect passwords
- Head off cybercriminals
- Dangers of compromised accounts
- Integrate PAM with your security
- Choosing a PAM partner

Delinea

Joseph Carson is a cybersecurity professional with more than 25 years' experience in enterprise security specializing in endpoint security, application security, and PAM. Joseph is a CISSP and an active member of the cybercommunity, speaking at cybersecurity conferences globally. He's a cybersecurity advisor to several governments, as well as critical infrastructure, financial, and maritime industries.

ISBN: 978-1-119-88722-5
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.