Definitive Guide™

to

Securing Privileged Access

Secure Your Vulnerable Apps, Devices and Cloud Data Through Least Privilege Access

John Pinson

FOREWORD BY:
Joseph Carson

Compliments of:

thycotic

About Thycotic

Thycotic is a global leader in Privileged Access Management, a critical layer of IT security that protects an organization's data, devices and code across cloud, on-premises and hybrid environments. Recognized as a leader by every major industry analyst group, our modern cloud-ready PAM solutions dramatically reduce the complexity and cost of securing privileged access, providing more value and higher adoption than any alternative. Thycotic is trusted by over 12,500 leading organizations around the globe including 25% of the Fortune 100. Headquartered in Washington, DC, Thycotic operates worldwide with offices in the UK and Australia. For more information, please visit www.thycotic.com.

Definitive Guide™
to
Securing Privileged Access

Secure Your Vulnerable Apps, Devices and Cloud Data through Least Privilege Access

John Pinson
Foreword by Joseph Carson

CYBEREDGE
PRESS

Definitive Guide™ to Securing Privileged Access

Published by:
CyberEdge Group, LLC
1997 Annapolis Exchange Parkway
Suite 300
Annapolis, MD 21401
(800) 327-8711
www.cyber-edge.com

ISBN: 978-1-948939-20-1 (eBook)

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgements

CyberEdge Group thanks the following individuals for their respective contributions:

Editor: Susan Shuttleworth
Graphic Design: Debbi Stocco
Special Help from Thycotic: Jordan True, Barbara Hoffman, Sara Shuman, Joseph Carson, Nate Otiker, John Ortbal, Nick Hunter, Richard Wang

Table of Contents

Foreword

With many applications and services now hosted in the cloud, we live in a world where the traditional cyber security perimeter has dissolved. Remote access from multiple devices has become the rule rather than the exception. In this always-on, Internet-connected universe, every user potentially has access to privileged or sensitive information. Consequently, the compromise of a single user's credentials can all too easily be exploited by cyber criminals to escalate privileges and gain access across your entire network, undetected.

Thus, all users may be considered "privileged." However, when it comes to securing access to both non-human and human privileged accounts—the proverbial "Keys to the Kingdom"—not all users are created equal. For instance, accessing work email may require a password or multi-factor authentication. Accessing customer information, in contrast, should require a higher level of authorization or security control, such as prior permission from an established, in-house authority based on an explanation for the request, as well as a time limit imposed if/when access is granted.

Our job as cyber security professionals is to help our organization's users (including IT staff, business employees, and third-party providers) gain access to a multitude of apps and services (mostly in the cloud) to do their jobs as safely and securely as possible. The key to making this work for everyone is to develop a comprehensive and continuous risk assessment of how data throughout the organization is accessed. You can then apply security controls and policy enforcement with automated management tools to manage the risk.

Based on my 25 years of experience in the cyber security industry, I believe there are three components needed to support a comprehensive approach to managing risk while balancing cyber security requirements with user productivity and experience. These three elements are essential to an intelligent, adaptive, and highly usable cyber security framework:

Interoperability – A traditional siloed approach to deploying "best of breed" security solutions is no longer acceptable. That doesn't mean one size fits all, where granular control is sacrificed for the sake of convenience. It does mean evaluating the integration and interoperability of multiple layers of defense.

Automation – Cyber security solutions that slow down or impede the user are doomed to remain shelf-ware or be circumvented, rendering them irrelevant. Managing secure access—including authentication, authorization, monitoring, and more—should be as frictionless as possible, with controls guided by automated policies running in the background.

Orchestration – Getting multiple cyber security solutions working together like a symphony orchestra requires a conductor to keep everyone moving in sync and harmony. Privileged access management software tools serve as the conductor, enabling the security team to coordinate and fine-tune a multifaceted defense that places a premium on seamless, secure access appropriate to the risk involved.

Understood in the context of interoperability, automation, and orchestration, securing privileged access for many diverse users is a challenging but achievable goal for organizations today. But it requires a shift in mindset and a willingness to change your frame of reference from building static walls to creating a cyber security ecosystem that ensures discipline and enforcement while remaining flexible and adaptive. This Definitive Guide to Securing Privileged Access provides a detailed roadmap to the principles and practices you'll want and need to protect your business.

Joseph Carson
Chief Security Scientist
Thycotic

Introduction

Cyber security priorities, practices, and technologies have gone through a dramatic evolution in recent years. Driven by a singular convergence of emerging trends—remote and at-home workers, device proliferation, the Internet of Things, accelerated adoption of cloud computing—organizations find that old tools and methods no longer work. The increased risks of traditional application security approaches, such as perimeter defense, user authentication access authorization, and data confidentiality, can be exposed as never before.

In this guide, we set out a new strategy crafted explicitly to secure privileged access to applications while aligning to modern IT security objectives. This strategy builds on proven privileged access management (PAM) precepts and secure vault technologies to extend security across the borderless enterprise that now extends into the cloud.

A whole new realm of security capabilities emerges through the integration of PAM with cloud access and remote access solutions. It becomes possible to gain granular control over web applications and web-based cloud management platforms. It also becomes feasible to secure access and enforce a zero trust strategy with least privilege enforcement for remote workers, third-party service providers, and vendors.

Cybercrime is a daily reality, and security professionals need to be equipped with more-effective tools and solutions. Please read on to learn more about securing privileged access within the perimeter-less digital enterprise.

Chapters at a Glance

Chapter 1, "Securing Privileged Access," lays out the basics of PAM and the changing nature of privilege today.

Chapter 2, "Understanding the Risks of Compromised Privileges," explains the risks associated with malicious and benign actors, and the growing role of regulation.

Chapter 3, "The Evolving World of Privileged Access," details the profound changes and new risks introduced through the cloud revolution.

Chapter 4, "Aligning Privileged Access to Security Priorities," describes why a secure password vault is still essential for securing privileged access to applications.

Chapter 5, "Essentials for Orchestrating Privileged Access," specifies essential capabilities such as APIs, RBAC, session monitoring, alerts, logging, and more.

Chapter 6, "Getting Started," provides next steps for securing privileged access in hybrid cloud and multi-cloud architectures serving dispersed teams.

Chapter 7, "Selecting the Right Solution to Secure Privileged Access," highlights what to look for in a solution—not just capabilities but also crucial value-adds to make your deployment a success.

Helpful Icons

Tips provide practical advice that you can apply in your own organization.

When you see this icon, take note as the related content contains key information that you won't want to forget.

Proceed with caution because if you don't it may prove costly to you and your organization.

Content associated with this icon is more technical in nature and is intended for IT practitioners.

Want to learn more? Follow the corresponding URL to discover additional content available on the Web.

Chapter 1

Securing Privileged Access

In this chapter

- Learn how the concept of privileged access has evolved
- Understand why conventional PAM no longer works

The Changing Nature of Privilege

As IT professionals we find ourselves facing fundamental changes in the way we think about cybersecurity and in particular how we regard "privileged access." That's because the very nature of what's considered privilege has evolved.

"Privilege" no longer refers only to IT users. Today, users of all types can—and should—be provisioned with some form of privileged access. In fact, the dramatically increased level of complexity in managing privileged access to applications and data, especially in the cloud, is creating demand for a new generation of solutions.

New priorities drive change

As more companies mature in their privileged access security programs, they have an increasing need to extend the benefits of PAM to different end users and groups. Additionally, what is considered "privileged" has evolved. The concept of privilege is no longer synonymous with IT users.

For example, would you not consider your CFO, who has access to the most sensitive information about your company's financials, a privileged user? Or how about a member of your engineering team, who has access to your product's codebase?

This evolution has increased demand for PAM solutions that offer automated features that are highly interoperable with

existing IT infrastructure. The ability to orchestrate privileged access from a single pane of glass has become an essential capability within many organizations.

Identity & access management

Privileged access has traditionally been categorized under the umbrella of *Identity and access management (IAM)*. IAM is evolving and until recently conventional approaches revolved around a username/digital identifier such as an email address, device, or date of birth, and then passwords for verification. In our increasingly cloud-oriented digital environment, the old ways become less effective. Indeed, the username/ password combos that provided security and privacy just a few short years ago are useless in many cloud environments.

Secure vaulting and access are critical

For these reasons, IAM and PAM best practices have evolved to a point where security professionals prioritize *secure vaulting* of credentials for privileged accounts (objects) and secure access to privileged data, systems, infrastructure and applications (targets). This dynamic now holds true for all user scenarios and any operational eventuality.

Conventional PAM models focused on IT teams: users, accounts, and systems that reside at the heart of the enterprise. And, of course, IT-centric privileged accounts—like domain admin accounts—are still prime targets for malicious cyber actors.

Why conventional approaches are no longer effective

Traditional access control models, while still very critical, are insufficient for today's IT architectures. Infrastructure architectures from five years ago are unable to keep up with the requirements of today's access control models. Heavy cloud workloads and remote work have become the norm, and these changes impact all aspects of the employee identity lifecycle.

- ☑ Cloud and mobile computing blurs the traditional perimeter
- ☑ You can't be 100% sure your fence is working
- ☑ 77% of cloud breaches involve stolen and compromised credentials.[1]

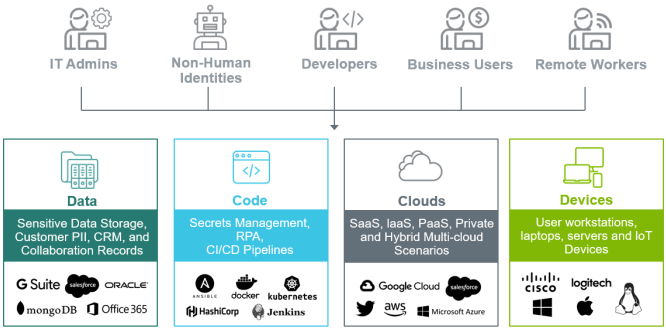

Figure 1-1: Conventional perimeter defense and privileged access tactics have become less effective in the cloud era.

Where Privileged Access Comes into Play

Managing privileges to secure data, applications, cloud, and devices has become exponentially more complicated in recent years. As complexity has increased, the scope of privileged access security has expanded from conventional *secrets vaulting* capabilities to monitoring and controlling access to shared secrets and *non-human admin accounts*.

Meeting these expanding priorities is difficult to achieve without impacting the end users' ability to leverage the applications they need to do their jobs. But today's advanced privileged access security solutions do make it possible to monitor, report on, and respond to real-time privileged access activity. These capabilities solve one of the key challenges associated with privileged account proliferation: real-time visibility into privileged user activity.

Privileged Access for All Data and Applications

Securing privileged access for data and applications has become a key focus within the wider discipline of Privileged Access Management (PAM) for a very important reason. As more organizations move to cloud-based applications and services, it becomes critical that cyber security strategies not only determine who or what can access a privileged account, but what actions can be performed once a user has logged in. Thus, securing privileged access must encompass more than getting to an application or service, but what is allowed once access is granted. This guide will help explain the evolution of PAM in the context of IT infrastructures including cloud, on premise and hybrid IT environments.

Applications are the engines of commerce in the digital age, driving revenue and growth for countless organizations. However, the critical role they play in the success of so many businesses also makes them prime targets for cybercriminals. This is why securing applications, and the access privileges to them, has become such a high priority.

Types of accounts

User accounts: A user account typically represents a human identity (such as an Active Directory user account) and has an associated password to protect information and prevent anyone from accessing it without permission. There is usually a single account password per user.

Privileged accounts: Privileged accounts provide administrative or specialized levels of access to enterprise systems and sensitive data based on higher levels of permissions. A privileged account can be associated with a human identity, non-human identity or machine identity, and *privileged administrator accounts* are omnipresent for IT resources such as servers, applications, databases, routers, etc.

Organizations often have exponentially more privileged accounts than employees. In most organizations, IT staff have one account with standard-level permissions and another for operations that require elevated permissions.

Chapter 2

Understanding the Risks of Compromised Privileges

In this chapter

- Understand how vulnerabilities arise and are exploited
- Learn the true costs of breaches and cyber incidents
- Explore how regulatory compliance adds complexity

The Doorway to Your Most Valuable Applications and Data

Industry analysts estimate that up to 80% of all security breaches today involve privileged accounts' compromise.[2] This number shouldn't surprise us—privileged credentials are the doorway to the applications and data organizations rely on to drive revenues and growth.

Despite their well-known shortcomings, countless organizations still rely on traditional methods of identifying and managing privileged accounts. Even in the most sophisticated IT environments, security practices are often characterized by continued adoption of shared passwords across multiple systems, unmonitored sharing of credentials, and use of default passwords seldomly or 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.

In many cases, personal accounts on end user devices are hacked initially through social engineering techniques; attacks are then escalated to compromise accounts with higher privileges, often using the same credentials to move laterally to other systems.

Applications and Data at Risk

Virtually all organizations have some unknown or unmanaged privileged accounts, increasing the risk of compromise. This can happen for various reasons:

- ☑ Access is never disabled for employees who have left the organization.
- ☑ An account is used infrequently and becomes obsolete or is abandoned.
- ☑ Default accounts for new devices are never disabled, and passwords remain unchanged.

Every unknown or unmanaged privileged account increases your organization's vulnerability and presents an opportunity for an intrusion. An employee may access a privileged account to perform unauthorized tasks, intentionally or unintentionally breaking compliance regulations and increasing your liability. A disgruntled ex-employee who retains privileged access can cause harm. A cybercriminal can access the account and penetrate your organization, steal information, and wreak untold havoc.

It is not unusual to find organizations where a single *privileged account* accessed through a shared password is used to run many services and applications. If that single account is breached, your risk increases dramatically.

It takes only a single compromised privileged account for an attacker to gain access to virtually any critical data and information in your organization.

How the cloud exacerbates vulnerabilities

The vulnerabilities created through the compromise of privileged accounts are becoming frighteningly widespread

as organizations across all verticals continue to migrate to the cloud. Why? Because cloud infrastructure expands the diversity of privileged access management use cases.

In a cloud model, managing privileged access to workloads, services, and applications remains your responsibility, not that of the cloud provider. It's also your responsibility to make certain data from the cloud (via web browsers, email, file exchanges such as SFTP, APIs, SaaS products, and streaming protocols) are adequately secured.

The vulnerabilities cited in the prior section are endemic to the cloud. Consider: when an organization initially sets up a cloud account, the root account provides complete access to the all-powerful cloud management console. If a bad actor gains unauthorized privileged access to this management console, directly or through an API, they could essentially have complete control over all your cloud assets and operations. Data extraction or even a ransomware-powered shutdown of your environment could easily ensue.

Techniques for compromising privileged accounts

The path to compromising a privileged account often follows a variation of this pattern:

Compromise a local account. Criminal hackers use malware or social engineering/email phishing to access desktops, laptops, or servers. Employees can be fooled by phishing scams that appear as legitimate requests from a manager, company executive, or another trusted source. They may unknowingly click on a malicious link, download a piece of software with malware hidden inside, or enter their credentials into fake websites.

Capture a privileged account. An attacker's primary goal is to obtain a privileged account (such as an Active Directory domain administrator account) that will enable them to move around the network. After capturing an employee's password, the perpetrator can log onto a network and bypass many traditional IT security controls because they appear as a user with legitimate credentials. Common techniques to elevate privileges include *Man-in-the-Middle* and *Pass-the-Hash* attacks.

Hide and observe. After attackers establish a breach, they typically use compromised privileged accounts to perform reconnaissance and learn about the IT department's everyday routines. The process may include observing regular schedules, security measures, and network traffic flow. They use these observations to blend in and make sure they don't trigger any network security alarms. Eventually, they can get an accurate picture of the entire network and its operations.

Impersonate employees. An attacker with access to a privileged account can impersonate a trusted employee or system and thereby carry out the malicious activity for weeks or months at a time without being detected as an intruder. 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 this type of breach is eventually detected.

Establish ongoing access. An attacker's next step is often to establish continuous access by installing remote access tools, which enable them to return anytime they wish and perform malicious activities without being detected. Alternatively, they could create backdoor accounts or their own privileged accounts with free access to your data and systems. Another common trend is the attackers who gained initial access sell it to other cybercriminals who will abuse that access to deploy nasty ransomware.

Consequences—what to expect when the unthinkable occurs

Depending on their motives, attackers can use privileged accounts to cause lasting harm in a variety of ways:

- ☑ Damaging system functions or disabling access by an IT administrator
- ☑ Stealing sensitive data for fraud, financial gain, or reputation damage
- ☑ Injecting bad code
- ☑ Poisoning data

Generally speaking, the most significant harm from cyber attackers falls into two categories:

Intellectual property theft: While ransomware attacks are more prevalent than ever—costs from these attacks reached a new annual high of approximately $20 billion for 2020[3]—economic losses from theft of intellectual property are orders of magnitude greater.

- ☑ Theft of American trade secrets by China costs the US $300 billion to $600 billion a year.[4]
- ☑ A report by the US Intellectual Property Commission estimates losses to American firms is between 0.87% and 2.61% of annual US GDP.[5]
- ☑ With US GDP for 2019 at $21.43 trillion, total losses could be as high as $500 billion annually.

Operational downtime: While ransomware is covered elsewhere, it bears repeating: ransomware attacks have risen sharply during the COVID-19 pandemic. With an enormous chunk of the global workforce forced to go remote and work from home, attack surfaces expanded rapidly for organizations across all sectors. Headlines on ransomware attacks often focus on the exorbitant monetary demands involved. The larger and more lasting damage from ransomware attacks is inflicted when critical applications, services, and operations must be taken offline.

- ☑ The cost of downtime from ransomware attacks in 2020 was 50 times greater than the ransom amounts demanded by cybercriminals.[6]
- ☑ The average cost of downtime for 2020 was 94% greater than in 2019.[7]
- ☑ Estimates peg total ransomware costs to the United States in 2019 at more than $7.5 billion.[8]

Threat actors—outsiders, yes, but insiders too

The malicious hacker's image is pretty well fixed in the public mind and mostly misleading: a lone guy wearing a hoodie in his parents' basement, wreaking havoc willy-nilly on unsuspecting IT teams. Alas, the bad guys are far more likely to be highly coordinated teams of cybercriminals, often overseas organized crime outfits or nation-states. Far more dangerous than any single cybercriminal could be, these types of professional criminals are responsible for the vast majority of cyber security incidents today.

The public perception of threats from inside the organization is off base. Sure, disgruntled ex-employees exist. The more common and more serious threat comes from well-meaning insiders—IT admins who are just doing their jobs but might bypass a vital security procedure for convenience, only to leave open a critical vulnerability. Studies show most significant insider threats stem from accidental actions. Typically, misconfigurations in the assignment of privileges are to blame. Today, insider threats represent the primary vector for 60% of breaches.[9]

How Regulation Becomes a Force Multiplier

Virtually every organization that handles data must abide by security compliance requirements. If you handle any type of personal, financial, or health information, you must be able to demonstrate compliance or face significant financial penalties and public embarrassment. If you are seeking government contracts, you must receive a stamp of approval from security auditors to be successful.

The ultimate objective with compliance is effective security against rising cyber threats. The costs of non-compliance have proven to be far higher than the costs of compliance. Yes, there are upfront costs to managing compliance and audit processes. But the costs of doing it wrong, or not doing it at all, can increase the downside considerably. The costs of a breach covered earlier can be compounded by regulatory fines, bad publicity and damage to your brand.

Chapter 3

The Evolving World of Privileged Access

In this chapter

- Learn how the cloud is changing security requirements
- See why typical authentication isn't enough
- Review how the concept of the "user" is evolving

The Great Cloud Migration

In recent decades, the tech industry has brought great change to daily life through a series of breakthroughs. The web browser and the dawn of the commercial internet in the 1990s. Web 2.0 and the rise of social media in the early 2000s. The mobile/smartphone revolution, which got fully underway with the arrival of the first iPhone in 2007. The latest breakthrough has been more subtle and has largely taken place off the typical consumer's radar. Its long-term ramifications could arguably be as profound as those of any of its predecessors. I speak, of course, of the cloud.

AWS, Azure, and the other major cloud platforms

Many of us are still using the single word, cloud, as if it refers to only one thing, but the cloud is anything but an individual entity. Software as a service (SaaS). Infrastructure as a service (IaaS). Platform as a service (PaaS). Google Docs. Dropbox. Salesforce. Facebook. All of these are the cloud, yet each is a unique concept or offering. However, when it comes to privileged access security, the discussion centers primarily on

IaaS and PaaS web services providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform.

What makes cloud computing distinct

These enterprise-grade cloud platforms are where corporate America—and companies worldwide—are increasingly turning to host core applications and services. Famously, some large brands have completely migrated over their IT operations to cloud platforms, Netflix to AWS being the most prominent. Today, most startups are completely cloud-first entities, developing their businesses, solutions, and services in the cloud from the get-go.

This last trend points to the corporate data center's imminent demise, a long-tail effect of the great cloud migration that is of potentially greater significance than other tech waves. Netflix is the exception, for now; the vast majority of global enterprise brands still maintain significant on-premises computing resources. For many of these brands, especially in financial services, managing critical operations within their own secure data center will continue to make business sense. But even they will move to a hybrid model, and overall the trend toward cloud is clear.

Digital transformation

For the generation of companies that have started up since the mid-2010s, the born-in-the-cloud ethos likely means they'll never make large investments in on-premises capabilities. Keep in mind that established sector leaders across nearly every vertical industry have spent staggering sums on *digital transformation* journeys in recent years. In many cases, digital transformation was a mandate to get the company on a more competitive footing and help stave off nimbler players. Examples include big financial services providers looking to stay ahead of challenger banks and established players in style, apparel, and homewares looking to adapt their retail operating models to become future-ready.

For these organizations, moving to the cloud was a major part of the digital transformation process. In the case of companies born in the cloud, digital transformation is not something they need to think about or spend money on. They're cloud-

native! They are digital to the core and can quickly spin up or orchestrate new business services using automation tools and APIs. The tensions at work here between the old guard reliant on traditional data centers and born-in-the-cloud startups will shape many business sectors' future.

Why conventional authentication isn't enough for cloud applications

While the cloud's financial business benefits are apparent, numerous technological drivers need to be considered. First, ensuring the security of applications, data, and workloads is essential in any scenario. Established organizations have long worked to protect their information with traditional security perimeter tools, such as firewalls, anti-virus, and intrusion detection solutions. But with fast-evolving cloud, mobile, and virtualization technologies, building a fence or moat around critical assets is no longer sufficient. In fact, it's impossible.

The "Perimeter-less" Enterprise

In the digital workplace, people share information and are exposed to social engineering and targeted spear-phishing attacks to steal passwords and credentials. When attackers compromise identities, they can easily bypass the traditional security perimeter undetected and escalate privileged accounts' exploitation.

This is why conventional approaches to authentication haven't worked as well with cloud applications. Hacking privileged credentials can mean the difference between a simple breach and one that could lead to a cyber catastrophe. Therefore, the "new cyber security perimeter" must focus on protecting the *access rights* of employees, contractors, third-party partners, services, and cloud systems.

Changing nature of the user

I won't recount the seismic changes brought about by the COVID-19 pandemic here, other than to note that the five-day-in-the-office work week is very likely gone for good in many white-collar sectors. A parallel development that we do need to consider is the increasing reliance on third parties—especially in the context of the cloud.

Restricting access privileges to a time window is an effective way to contain and limit the potential damage caused by a malicious user, or force the attacker into taking more risks, thereby increasing the possibility of detection.

More and more, entities outside the core organization require access to sensitive data and systems. In manufacturing, a parts supplier might need to enter order and tracking data into your supply chain system of record. In retail, a marketing services provider might need to access sensitive information on customers to personalize offers.

Auditors might need to access information on security systems and data-handling practices to document compliance with privacy statutes in financial services. These types of exchanges are far easier to carry out in a cloud environment where the vendor can simply be granted privileges to the data source in question.

Device proliferation and the IoT

We always think of PCs and smartphones when we hear "device proliferation," but it's a phenomenon that goes far beyond the number of laptops or iOS and Android phones your IT department needs to maintain. The internet of things (IoT) and emerging technologies like software-defined wide area networks (SD-WAN) are radically transforming industries from healthcare and manufacturing to retail, transportation, logistics, and beyond. Today, conventional servers are being replaced by lightweight commodity appliances or virtual appliances in many enterprise networks.

Worldwide, the number of IoT-connected devices is projected to increase to 43 billion by 2023,[10] an almost threefold increase from 2018. How privileges are handled for accessing and managing these devices—and the applications running on them—has become a central PAM challenge that will only grow in the years ahead.

Chapter 4

Aligning Privileged Access to Security Priorities

In this chapter

- Learn why an encrypted password vault is foundational to securing privileged access
- Understand how to manage secrets and delegate access in real-world scenarios

Establishing a Secure Vault

To this point, we've shown the importance of privileged accounts and application security, documented how privileged accounts can be compromised, and looked at the complications presented by the rise of the cloud. Now, we begin to consider how best to execute on privileged access security priorities.

Regardless of the use case, an aggressive, effective privileged account security posture will always depend on your ability to store and manage privileged credentials. Years of best practice development in the cyber security space show that this goal is best accomplished via an encrypted, centralized vault. Encrypted storage empowers your security and IT ops teams to secure and manage all types of privileged accounts quickly and easily. It also underpins proactive protection measures such as automated password change policies, security status monitoring, and configurable policies. These capabilities set the stage for the full range of processes that are essential to a successful PAM program.

Privileged Access Management Lifecycle

A significant part of the audit process for organizations in financial services and healthcare, and increasingly in retail and many other industries, is documenting the use of compliant security practices. Auditors want to see proof that you're securely managing privileged credentials before they'll sign off on your organization as fully compliant.

Priveleged Discovery

What if an audit turned up evidence that specific privileged account passwords had not—contrary to best practices—been changed in years? Not good, especially if you lack privilege discovery capabilities. Discovery is so vitally important because it provides clear visibility. With strong discovery capabilities, you can quickly identify all service, application, administrator, and root accounts to curb sprawl and gain a complete view of your privileged access landscape.

Managing secrets

Healthcare organizations, in particular, are highly susceptible to ransomware attacks, with more than 560 ransomware incidents in the United States alone in 2020—a substantial year-to-year leap from 2019[11]. Penetration testing has shown that the methods some hospitals use to connect to and log into systems open the door to *Pass-the-Hash* attacks. In this scenario, administrators can sometimes leave password hashes behind on remote endpoints. Attackers can then scrape system memory or use other techniques to obtain those passwords and gain entry to a large IT environments as a privileged user.

Here is why the ability to provision and de-provision accounts, rotate credentials, and ensure password complexity is important. With advanced secrets management, passwords can be rotated automatically without any interruption to services or workflow. Two-factor authentication and checkout features provide extra layers of protection for privileged accounts.

Case Study: Achieving High Marks on Compliance Audits

As one of the leading steel suppliers in the United Kingdom began deploying more a virtual infrastructure with AWS, its IT team realized they needed a security solution to protect data both in a traditional data center and within cloud-based solutions. To keep pace with increasing regulation, the company needed to move from its legacy access management system to a more robust and fully functional PAM system.

Solution

Deploying Thycotic Secret Server gave the company a much more granular view of what was happening with all of its data and who had access to it—all from a single pane of glass. Secret Server is now supporting:

- Full auditing of corporate data, down to something as simple as someone opening and viewing a piece of data.
- Health checking of data integrity to ensure no one has changed it and to establish full audit trails.
- Management of the PAM lifecycle, such as end-to-end management of the complete password and access cycle.

"Of all of the changes we've made within our environments over the past five years, implementing Secret Server for PAM and auditing is probably one of the most important."

– Head of IT Operations and CISO

Delegating access

The mass adoption of work-from-home policies during the COVID-19 pandemic provided many organizations with a crash course in the importance of PAM and access delegation policies. Especially in companies or sectors where work-from-home was rare—think government, healthcare, telecom—the dangers and drawbacks came to light quickly. Employees accustomed to working in office settings, with secured internal networks managed by professional IT staff right in the building, suddenly found themselves logging into the corporate network through home Wi-Fi connections, often via outdated, unpatched routers. They expected the same access to systems they had while in the office. The IT and security teams, however, had little visibility into workers' devices, or control over where employees might wander online.

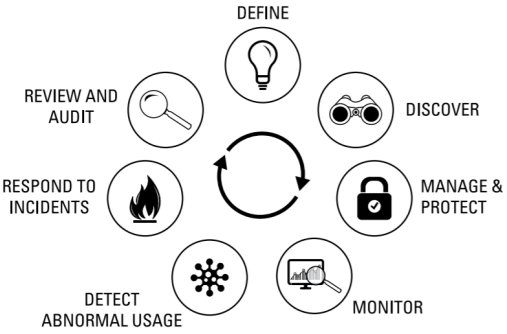

Figure 4-1: The PAM Lifecycle approach provides a framework to help PAM experts manage privileged access as a continuous process rather than a one-and-done project.

Because ensuring employee productivity and security in a work-from-anywhere environment requires a much different approach, it's critical to have advanced delegation and privilege controls among your PAM capabilities. Some access delegation considerations to keep in mind:

- ☑ *Role-based access controls (RBAC)* enable you to configure baseline and default access for each remote worker to internal and web applications. You want to determine and control what actions users can take, such as which button can be clicked, which text can be read, which form can be filled, and much more.
- ☑ We have already established the importance of a secure password vault. For added oversight, it's critical to track when administrators check credentials in and out, and to set time limits for temporary access when necessary. Session management controls such as workflow approval, dual control, keystroke logging, and session recording add an extra layer of control.
- ☑ Through the use of automated launchers, connection management provides access to secured resources without ever revealing the password to the user through the use of injected credentials. This approach helps move passwords into the background, mitigating employee password fatigue

and vastly reducing the security risk of someone selling or handing off a password. Connection management is vital for auditing because it tells us with 100% certainty "who was behind the keyboard" at the specific time a shared account was used.

- ☑ Remote employees and third parties may use their own workstations, including laptops and mobile devices, in different situations. You want to create a unified identity for each employee across all operating systems and environments, both on premise and in the cloud. That way, you'll know who they are when they access privileged accounts, regardless of the device they use.
- ☑ With today's enterprise-grade PAM solutions, users don't need to remember passwords. In fact, they don't need to see them at all. A high-quality PAM solution generates complex passwords, rotates them automatically, and uses proxies to connect systems, taking the human element out of the equation.

Least privilege for cloud apps

When users or applications operate with administrative privileges, they can access sensitive data, operating systems, and powerful controls. In scenarios where cloud applications, IaaS platforms, or developer tools come into play, admin privileges can pose a particularly dire risk. In contrast, under a least privilege model, administrative accounts with elevated privileges are given only to people who really need them, and only *when* they need them. All others operate as general, everyday users with an appropriate set of privileges.

Usage tracking

It's also critical to be able to track and alert on service account behavior. With up to 80% of breaches involving a compromised user or privileged account, gaining insights into service account access is a top priority. Visibility into your service accounts' access activity in real time will help you spot suspected account compromises and potential abuse—for example, monitoring when a service account has been used to log onto a system. Automating the process of privileged account discovery and management will help protect against

attackers or rogue insiders creating additional privileged accounts for their own use.

Session monitoring

Ideally, you want to make it simple for IT teams to configure and secure remote *sessions*, especially when your workforce is remote. Read on to learn why it's essential to provide your IT team with tools to navigate different connection protocols such as RDP and SSH, inject credentials, and interact with privileged sessions from start to finish.

Your PAM solution should be able to monitor and record service account activity. These capabilities will help enforce proper behavior and avoid mistakes by employees and other users because they know their activities are being monitored. Essential capabilities include:

- ☑ Remote access: Launch and configure sessions across multiple environments
- ☑ Session management: Automatically inject credentials into sessions as needed
- ☑ Centralized control: Access a single interface to manage and interact with sessions
- ☑ Session recording: Create an end-to-end record of privileged user access

Auditing

Successful application control demands a complete, real-time understanding of the status and activity of all endpoints. Your solution for securing privileged access should provide a unified reporting dashboard so you can quickly evaluate the status of endpoints, review activity logs and event data, and access a comprehensive library of reports. Look for a responsive, configurable solution that enables you to quickly drill down into reports across any dimension (time, geo/region, OS, status) to evaluate activities and trends. You should also be able to set up automated alerts to stay informed of potential problems and automated remediation to address policy violations.

Chapter 5

Essentials for Orchestrating Privileged Access

In this chapter

- Learn the core authentication standards and technologies underpinning privileged access
- Review the techniques organizations use to orchestrate the service account lifecycle

In Chapter 4, we walked through two use cases showing where privileged access principles should be applied in real-world business situations. The primacy of basing all PAM operations around a secure vault should be apparent by now, but what of the other key technology elements? Let's take a look at what comprises a full-featured PAM solution for securing access and the kinds of productivity enhancements that integrate application privilege management into existing workflows or tools. For instance, mobile apps can secure access from anywhere, or a browser extension can provide seamless injection of credentials. In this chapter, we'll walk through how these diverse capabilities come into play through the PAM lifecycle.

APIs & SDKs Enabling Interoperability

As the central hub for securing applications, any effective PAM solution must integrate with current and future technologies inside and outside the IT environment. Thus, a PAM

solution needs to provide application programming interfaces (APIs) and a wide range of integrations across multiple vendors and their technologies. The solution should have APIs to provide administrative workflows, incident response tools, and a central evidence repository. Endowed with these features and capabilities, the PAM solution helps deliver automated privilege orchestration to a business like a symphonic conductor, enabling privileged access between interoperable solutions.

Here's an example of how APIs would be invoked. A PAM solution can establish automatic connections between people and systems without exposing credentials to users. An advanced PAM solution can serve as a proxy through which an administrative session is performed and automatically relay the privileged account password from its vault to the target device or application. A smart IT department will identify and remove embedded/hard-coded passwords and replace them with API calls that inject passwords into workflows as they are needed.

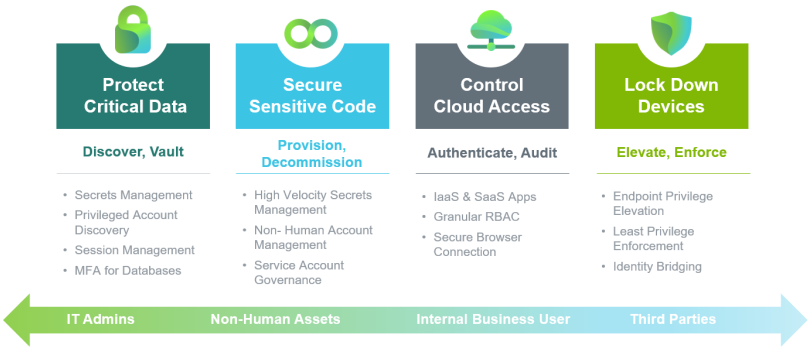

Figure 5-1: PAM solutions portfolio.

Similarly, a software development kit (SDK) provides security professionals with a set of capabilities that support advanced DevOps operations. Specifically, an SDK is usually made available for securing and streamlining DevOps processes involving operations running on the secure vault. Capabilities to look for include a command-line interface (CLI) that allows you to more efficiently engage the vault without compromising security or securely retrieve credentials from and track access to the vault.

Authentication—MFA, SAML, & OIDC

Unlike consumer password vaults that store credentials at rest, enterprise credentials move throughout the organization—in memory or in a token—and need to authenticate with other people and systems. To do so securely, you should encrypt privileged credentials and use multi-factor authentication (MFA). You also need to monitor credentials when they are in use during a privileged session or an API call.

Privileged user accounts are typically located in a central authentication system running in Active Directory (Windows) or in another central identity and authentication system that manages accounts, groups, and permissions for employees. Password changes can be challenging in one system; when you attempt to keep multiple systems in sync, there's a very high chance that errors will occur.

It's essential that your privilege access solution supports a second layer of authentication, either MFA or two-factor authentication (2FA), for added security. Basic email 2FA capabilities are standard in commercial PAM offerings. Still, it's far more preferable to integrate commercial, enterprise-grade 2FA and MFA offerings into your privilege management program.

FIDO2/YubiKey is one such MFA offering. It is based on an open authentication standard (Fast Identity Online, second edition) that uses physical devices for authentication. Integrated with a secure vault, FIDO2 would provide a second authentication after a standard password entry—any FIDO2-enabled user attempting access to a vault account must have a FIDO2 device in hand. The device eliminates many password-related issues, such as phishing and Man-in-the-Middle attacks. It also speeds up the login process compared to requesting a 2FA code via callback or text.

Security Assertion Markup Language (SAML) allows single sign-on (SSO) to applications and websites. Because SAML is an open standard, PAM solutions can integrate with it to offer greater flexibility in authentication and segregation of authorization. For instance, users can configure the solution as a service provider and link it to their SAML identity provider. This makes it easier for them to log into the solution because

once the identity provider authorizes them, they won't be prompted for their credentials. Similarly, OpenID Connect (OIDC) enables SSO and 2FA.

Active Directory

Roles and permissions processes are tightly integrated with the vault's directory (name) services architecture. Most enterprise-grade privilege management solutions use Active Directory to handle mapping the names of network resources to their network addresses. Their shared information infrastructure locates, manages, and organizes network resources, including volumes, folders, files, users, groups, devices, and much more.

Role-based access controls & permissions

Privilege management requires a method of regulating permission to access systems in which each user and group must be assigned a role. The industry-standard approach to restricting system access to authorized users is role-based access control (RBAC). A typical RBAC hierarchy is based on three roles: administrator, user and read-only user, and each role contains various permission levels to match the job function of the user. RBAC makes it possible to assign multiple permissions to a role. For example, you could assign Administer Users, Edit Secret, Own Secret, and View Active Directory permissions to the same role. That role can then be assigned to a user or group.

Here's an example of how using RBAC with a PAM solution would control privileges in a typical business scenario. Your monitoring team needs to configure event alerts or view usage reports, but they shouldn't have access to the privileged passwords. Within the RBAC and PAM solution you can grant granular access to those users, so they only have access to the information they actually need. Later, you can quickly and easily revoke that access, or even set the privileges to expire at a given time.

RBAC for a Complex Enterprise

Role-based access controls are the antidote to piecemeal user and permission management. RBAC provides a mechanism for system administrators to set policies and apply them as appropriate.

While RBAC has been around for many years, implementing it consistently has become increasingly challenging due to the complexity of modern use cases. With the growth of cloud services and third-party software, a unified approach to RBAC is critical to reducing risk and meeting compliance requirements.

Import & discovery

IT departments are seldom starting from scratch when they implement a PAM program. Users are already storing passwords in spreadsheets, personal password managers, and text files. You must ensure those passwords are not overlooked and get all users onboard quickly by importing existing passwords from other apps. An effective import solution can simplify integration with current and legacy systems and allow users to easily add large numbers of secrets, or passwords, from a CSV or XML file. Alternatively, discovering accounts and automatically updating their passwords ensures that any passwords left lying around in files or on sticky notes are no longer valid and do not present an ongoing risk.

You'll need a discovery capability that allows administrators to overwrite existing passwords using a privileged account. Admins will also need to determine which applications are in use and require rights to run, including hidden or hard-coded admin privileges. The most powerful applications installed on endpoints require administrator credentials or root privileges to run. You'll want to develop a clear snapshot of how these applications are used before implementing any changes. Ideally, you will have discovery policies to target any new application action that requires administrator or root access, so no privileged action goes unnoticed.

The service account lifecycle

Service accounts provide access to critical applications and data but fly under the radar of IT. Historically, they've been very time-consuming to discover and control, and are prone to human error when managed manually. Often the original purpose of a service account has been forgotten, but organizations cannot risk removing it because doing so may cause unpredictable system failures. Because of this lack of governance, we've seen almost all medium-to-large organizations suffer from extreme service account sprawl, perpetuating the unmanaged, uncontrolled expansion of their privileged account attack surface.

An effective service account lifecycle management solution should allow for the automation and interoperability of user access. IT teams get full visibility into user access and role assignments as well as ongoing user and role changes. Better interoperability and visibility improves governance and security across the organization, streamlines the delivery of privileged access to improve both end user and IT productivity, and optimizes PAM across the enterprise.

Session management & recording

Particularly important for organizations that allow third-party access to privileged accounts are monitoring and recording privileged session activity, which should be included in advanced PAM programs. They must also incorporate workflows that allow for multiple levels of approvals to grant or deny exceptional access to sensitive data or critical systems.

Session monitoring increases oversight of privileged account use and permits in-depth analysis of privileged session activity in real time or after the fact. With modern PAM software featuring "four eyes" capabilities, session policies can be set requiring two people to sign off on any significant action.

Credential management

The core of PAM, access security, includes vaulting, delegation, and elevation of privileged credentials, following a least privilege model. This group of capabilities enables the secure usage of privileged accounts. Privileged passwords,

certificates, and keys are stored and managed in a secure vault with very restrictive permissions, ideally requiring MFA to access. When users or systems "check out" secrets, PAM establishes user accountability for a specific period of time. PAM can establish automatic connections between people and systems without exposing credentials to users. An advanced PAM solution can serve as a proxy through which an administrative session is performed and automatically relay the privileged account password from its vault to the target device or application.

Automation (event pipelines)

Core IT security systems are notorious for generating large numbers of alerts that can overwhelm staff, creating "alert fatigue" that can lead admins to overlook essential warnings. Here, PAM solutions can play an important role with automated event pipeline capabilities—or "if/then" automation. Common trigger events can initiate a series of automated actions, weeding out minor events and escalating more-serious threats in the warning pipeline to save staff time so they can focus on alerts that need more investigation or a complex response. For example, if a privileged credential's heartbeat fails, indicating a password has been changed outside of the central PAM vault, a triggered action can rotate that password automatically and bring control back into the solution.

Intelligence & real-time alerting

Logging, analytics, and reporting capabilities are most often associated with audit and compliance processes. Yet privileged behavior analytics are also highly valuable for uncovering any warning signs of privileged account abuse and initiating action to mitigate risk or prevent damage. Based on the analytics you set up, a comprehensive solution can trigger alerts or perform automatic responses. For example, administrators may wish to lock down accounts, rotate credentials immediately, or suspend or terminate sessions when alerted of suspicious behavior. Once the event is investigated and cleared, administrators can reset to baseline. These actions can be associated with events including:

- ☑ A sudden increase in privileged account access by specific users or systems
- ☑ Aberrant or atypical access of the most privileged accounts or secrets
- ☑ A large number of privileged accounts accessed all at once
- ☑ Accounts accessed at unusual times of the day or from unusual locations

Logging & reporting

Advanced PAM programs include logging privileged activities with an immutable audit log that allows playback for reporting, auditing, and event forensics. Require employees to enter a comment in your log as to why they need access to a privileged account or link the access to an existing work item ticket. Set up alerts or emails to managers, team leads, or InfoSec when the domain admin membership group and other privileged groups change. Automate and share reports to increase visibility and continuously improve your PAM program.

Just-in-time access

Privileged access control solutions should simplify and automate managing remote workers' access to IT resources they need to be productive and secure. Look for a platform that centralizes session authentication, recording, and auditing of both RDP and SSH connections and implements just-in-time privileged access controls within a centralized user portal. These features are especially valuable for providing secure access to third-party vendors and contractors, and remote workers.

Chapter 6

Getting Started

In this chapter

- Understand why security experts are counseling IT Ops leaders to plan for the perimeter-less enterprise
- Review how a firm in the freight logistics management sector is securing access for remote teams and third parties
- Learn to manage secure access in multi-user environments

Conventional approaches to privilege management treat on-premises applications and cloud applications as entirely different animals, leading to multiple conflicts and repetitive processes. Today, the smarter way to go is with solutions that allow you to easily integrate your existing authentication solutions with any web application, without writing any additional code. The best solutions apply granular RBAC policies to enforce and employ least privilege and zero trust initiatives even to custom and legacy web applications.

Privileges at a Granular Level

Especially when it comes to today's cloud and virtualized environments, you need the ability to secure accounts on cloud servers like AWS and Rackspace, containers like Docker, and web applications like Salesforce and Office 365. All this cloud infrastructure requires tight integration with Active Directory and other directory services. The essential capabilities in this approach include:

Least Privilege for Cloud Apps
Specify what an individual employee is allowed to read or modify within any web application.

Access and Rights
Grant, manage, and revoke access to cloud applications. Specify who gets access to what at a granular level.

Usage Tracking
Track usage of each and every cloud application, including clientless session recording without agents.

Building for The Perimeter-less Enterprise

Organizations—especially manufacturers and retailers with long supply chains—often use third-party contractors to carry out specific tasks or supplement their internal teams. The resulting workflows can be manually intensive and create security and compliance risks. Common challenges include creating accounts for contractors, granting the appropriate level of access, managing rights, and off-boarding contractors when their jobs are finished.

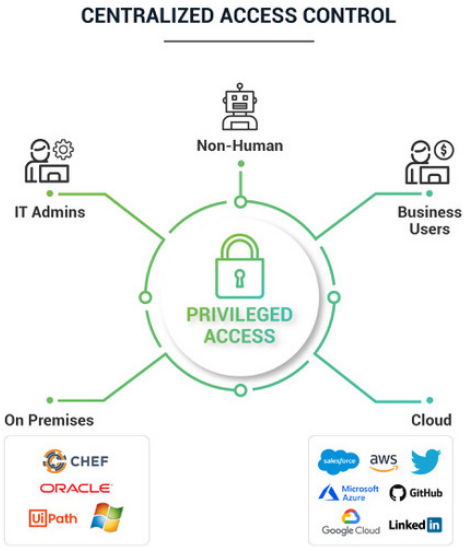

Figure 6-1: Hybrid and multi-cloud architectures require a least privilege approach backed by strong access rights and usage tracking.

Freight Logistics Software Provider Ensures Regulatory Compliance with Thycotic

This company's cloud software and data analytics platform connects all parties involved in global trade transactions. More than 10,000 organizations use the platform for ocean, air, truck, and rail freight, drayage and cartage, warehousing, customs brokerage, financing, and insurance. The company relies on remote third parties for data entry, logging, and other tasks related to sensitive information and high-risk business activities to augment internal engineering resources.

- Remote teams and third parties need access to a custom application, GitHub repositories, and CI/CD tools, as well as project management systems for ticketing queues.
- Multiple groups require specialized roles to access a variety of projects.

Solution

- The company selected Thycotic's Access Controller products, and was quickly
- able to validate uptime and low latency sessions between globally dispersed workers and the servers they needed to access, which was very important to the engineering team.
- The company now has internal oversight and evidence collection to demonstrate compliance to an auditor.
- If a breach occurs, the security team now has access to auditable activity recordings to recover and understand the root cause.
- The team also introduced session recording to improve oversight and ensure compliance.

"Now we enable access for our remote teams by handling everything virtually. They can log into a portal from any laptop and only access locked down resources without even knowing the credentials."

– Senior Technical Program Manager

Meeting the collective challenges above can be characterized as enforcing a zero-trust strategy for remote workers and third parties. Because your vendors require access to applications and data, you need to arrange your organization as a perimeter-less enterprise. To do so, the ability to enforce policies—including the use of MFA and session recording—becomes crucial. The essential capabilities for such a solution must include:

Remote Access
Record, review, and audit all RDP and SSH remote access sessions for Windows and Unix-based servers and containers.

Third-party Access
Grant remote workers access to accounts, web apps, and servers on the corporate network in line with third-party policies.

Frictionless Adoption
Enable vendors to opt into the solution without the need to deploy agents or install software on any endpoints or servers.

Hybrid & multi-cloud architectures

The exponential rate of hybrid cloud and multi-cloud adoption continues to stress-test existing security models and conventional application security and PAM approaches. With organizations migrating workloads to AWS, Azure, and GCP at record speeds, security teams need to do everything they can to limit the risk associated with secrets proliferation. Because DevOps teams often prioritize speed over security, what's needed are cloud-based vault solutions that balance the organization's security needs with the velocity that developer teams require.

Accommodating DevOps tools

Look for a solution that enables your organization to adopt enterprise-class secrets management for DevOps CI/CD pipelines. The complexity and variety of tools within these pipelines require centralized management of privileged access to maintain security, unify privileged access management, and control costs. Rapid deployment and elastic scalability are crucial attributes, as is the ability to handle the high-speed secrets management needs of the most dynamic DevOps environments. Requisite to any effective solution would be the ability to handle all the different types of secrets commonly used by DevOps teams:

- ☑ **Usernames/passwords** – CI/CD solution-to-solution authentication/integration
- ☑ **X.509 certificates** – Additional layer of MFA
- ☑ **SSH keys** – Access Linux/Unix systems
- ☑ **API keys** – Access credentials from scripts/code

Multi-user environments

Risky DevOps practices open the door for privileged account attacks. To access systems, developers may embed hard-coded keys or credentials within an application. During testing, they may store credentials in a repository such as GitHub, forget about them, and then commit them to production, where an external threat agent may find them.

Some DevOps teams share private keys and credentials with other users for immediate access to secure accounts, which increases the risk of insider threats, either malicious or accidental. DevOps teams may be distracted from core product development tasks if they use vaults for secrets management by building their own. Organizations may end up with multiple vault instances that aren't connected, centrally managed, or auditable.

Critical Elements & Capabilities

To mitigate the threats inherent in multi-user environments, today's fast-moving, cloud-oriented organizations need powerful capabilities in all of the following areas:

Cloud access control

Today's environment call for granular control over web applications and web-based cloud management platforms. With RBAC and the ability to carry out least privilege best practices, you should strive to manage shared accounts efficiently. Additionally, the ability to log, record, and audit user activities allows you to intelligently block unauthorized access based on security policies, and control what web application functions a user is allowed to use.

Remote access control

Providing secure access for remote workers and vendors requires the ability to enforce zero trust principles supported by MFA. Because revoking access the moment it's no longer needed is a key capability with remote users, you'll also want to have just-in-time privileged access controls and strong activity auditing functionality.

Database access control

Increasingly, organizations rely on cloud databases from AWS (RDS), Google, Azure, and Oracle to support critical business priorities. With much of your most valuable information now stored essentially outside of the establishment, extra access controls become necessary. Look for solutions that offer the ability to monitor and manage privileged users, verify identities, and layer MFA onto connections to the database.

Least privilege, everywhere

Least privilege access is a foundational principle in cybersecurity, but how exactly would it play out across your organization? Some basics:

- ☑ Grant privileges only at the required level on every device, every server, every OS, every database, and every application.
- ☑ Cloud portals are no exception. Never allow users to freely interact with IaaS platforms that, if misconfigured or attacked, could bring an organization to its knees.
- ☑ Within Linux/Unix systems, SSH key rotation should be enabled on demand or on a schedule.
- ☑ Every user must be secured: IT admins, developers, remote workers, business users, and even non-human identities.

Chapter 7

Selecting the Right Solution to Secure Privileged Access

In this chapter

- Recap the essentials for securing privileged access
- Understand the "must-haves" and what to avoid

As discussed throughout this book, securing privileged access to critical data, applications and accounts has become a central focus for IT security professionals in recent years due to a convergence of evolving technology trends. With businesses increasingly embracing cloud computing and new methodologies in areas like DevOps to craft new business services, the vulnerabilities inherent in conventional approaches are exposed as never before.

A substantial majority of global breach incidents are conducted through stolen credentials. Like the old bank robber joke, "*Why do you rob banks? Because that's where the money is!"* privileged credentials are where cyber criminals concentrate their efforts because that's where they can extract the greatest value. This reality has been driven home as the historic shift to at-home work has opened up a host of new vulnerabilities over the past year.

Defining Characteristics of an Effective Solution

Throughout this guide, I've made the case for specific principles, capabilities, and technologies that are indispensable for secure privileged access. I've also highlighted how organizations around the world are effectively implementing

these precepts through short case studies. The core attributes should be clear at this point. Still, ancillary attributes and collateral issues need to be considered when selecting a secure privileged access solution. Let's dive in.

Protect passwords

The core of securing privileged access includes vaulting, delegation, and elevation of privileged credentials, ideally in accordance with a least privilege model. This approach enables the secure usage of privileged accounts and helps move passwords into the background. Privileged passwords, certificates, and keys must be stored and managed in a secure repository—an encrypted vault—with very restrictive permissions and access requiring MFA.

Hybrid solutions

Many new organizations are building out their operations based on a cloud-first or "born in the cloud" ethos. But the overwhelming majority of organizations today still keep most of their IT infrastructure on-premises. To be fully effective, a secure privileged access solution must function both in corporate data centers and in the cloud or support a hybrid solution.

Capabilities of on-premises privileged access management deployments must include:

- ☑ Control over end-to-end systems and infrastructure
- ☑ Deployment of software in your on-prem data center
- ☑ Compliance with legal and regulatory obligations

Privileged access management in the cloud must include:

- ☑ SaaS model that allows fast sign-up and rollout
- ☑ No/minimal hardware or costs with PAM in the cloud
- ☑ No/minimal provisioning, patching, or maintenance overhead
- ☑ Elastic scalability as you grow
- ☑ Controls and redundancy with high uptime SLAs

The solution should be able to establish automatic connections between people and systems without exposing credentials to users. You want an advanced solution that can serve as a proxy through which an administrative session can be performed and that automatically relays the privileged account password from its vault to the target device or application. Advanced privileged access programs identify and remove embedded/hard-coded passwords and replace them with API calls that directly inject passwords.

Internal threats

Insider threats represent the primary vector for 60% of data breaches today.[12] Studies show the biggest insider threat stems from accidental actions, typically misconfigurations in the assignment of privileges. A critical capability for addressing insider threats is rapid scanning of your environment to discover which accounts may be overprivileged and, therefore, vulnerable to insider threats and malware attacks.

Real-time session management

As discussed in Chapter 5, session monitoring enables you to increase oversight of privileged account use and perform in-depth analysis of privileged session activity in real time or after the fact. Selecting a solution with real-time monitoring capabilities ensures that you can tune in live to watch sessions, oversee remote connections, modify privileges, or even terminate connections.

Rapid deployment & scalability

You're never going to find a software vendor that will admit its solutions are difficult and time-consuming to implement. "Get up and running fast!" is the standard claim, but how can you tell if this is really the case? Vendors with proven solutions that can be deployed quickly share these qualities and characteristics:

- ☑ Free Trials and PoC: Look for an intuitive user interface. This leads to higher user adoption and greater confidence using the tool. Take it for a test drive to get a feel for how successful you will be.

- ☑ Extensive documentation: Detailed instructional content that clearly lays out how to get the solution operating and performing to spec is vital. Also, assess how much your team can handle versus what requires (sometimes very pricy) professional services.
- ☑ Customer testimonials: Case studies and videos from customers—especially IT security pros—are a strong indicator that you're dealing with a proven vendor.
- ☑ Support: A professionally run vendor will provide a customer success team to work with you on implementation to achieve ROI as fast as possible.

Try to Avoid...

Beware of niche tool vendors that operate in a single vertical industry or use case. This vendor might meet your immediate needs but may not scale with your business.

Beware also of any solution or vendor that requires a major investment in professionals services as the price of implementation. Be sure to ask where and when such professional services are required: Customizations? Regular release updates? This can have a substantial impact on your overall cost of ownership, adoption and flexibility.

Conclusion

As organizations transition to the perimeter-less enterprise, traditional approaches to PAM have not always protected critical applications, accounts, and data. We live in a digital environment of expanding attack surfaces and fast-evolving cyber threats. Never before has the need to effectively secure privileged access been so great. Yet, the good news is that today's most advanced solutions for securing privileged access are up to the challenge. In seeking out the right solution for your organization, keep in mind that it must serve the needs of IT admins and developers and remote workers, business users, and non-human identities. Your solution must protect data, code, cloud resources, and the full range of devices within the enterprise. And it must effectively execute all these priorities on premise and in the cloud.

Glossary

API: Application programming interface. A defined set of functions that can be called from external software or scripts to retrieve data or perform actions within a software product or system.

CI/CD: Continuous integration and continuous delivery. The practice of merging development and operations activities into a combined and often automated workflow.

Cloud computing: Umbrella term for Internet-based computing capabilities that provide access to data, storage, applications, and developer tools online. Subcategories include software as a service (SaaS), infrastructure as a service (IaaS), and platform as a service (PaaS).

Device proliferation: The rising number and diversification of digital devices that is closely associated with the growth of mobile technologies and the Internet of Things (IoT). Worldwide, the number of IoT-connected devices is projected to increase to 43 billion by 2023, an almost threefold increase from 2018.[13]

DevOps: The combination of system development and operations functions. The aim is shortening the time between development and deployment of software and tools. See also CI/CD.

Least privilege: In cyber security, the concept of limiting access to privileged accounts by users, applications, and services to only what is required for productivity. These limits are imposed through various controls and tools.

Non-human identity: An account used to run services or applications that are not actively managed by a human administrator.

Password vault: An application that stores, encrypts, and manages passwords and other credentials to access applications, accounts, and services.

Perimeter-less enterprise: Organization characterized by a large number of employees and users located outside

the office/firewall. With fast-evolving cloud, mobile, and virtualization technologies, building a fence or moat around critical assets is no longer possible. A perimeterless enterprise requires advanced privileged access technologies to achieve security objectives.

Privileged access management (PAM): Cyber security strategy for exerting control over elevated access and permissions for users, accounts, and processes. PAM determines not only which people and systems can access a privileged account but also what actions they can perform once logged in.

Privileged account: An account that provides administrative or specialized levels of access to enterprise systems and sensitive data, based on higher levels of permissions. A privileged account can be associated with a human being or an IT system.

Role-based access controls & permissions (RBAC): An approach that enables security admins to configure baseline and default access for each remote worker on internal and web applications. RBAC is a technique for managing permissions to determine and control what actions users can take, such as which button can be clicked, which text can be read, which form can be filled, etc.

Secrets vault: An application that stores, encrypts and manages credentials used to access applications, accounts, and services. Credentials protected by a secrets vault may include passwords, certificates, SSH keys, and access tokens.

Session monitoring: A technique to increase oversight of privileged account use and allow in-depth analysis of privileged session activity in real time or after the fact.

Zero trust: An approach to cyber security that assumes all endpoints, applications, and users are compromised and therefore must be authenticated and managed at all times as if they were malicious.

Endnotes

Chapter 1

1. Anastasios Arampatzis, "Verizon DBIR 2020: Cloud Apps, Stolen Credentials, and Errors," in The State of Security, 2020.

Chapter 2

2. Joseph Carson, "Dissecting the Make-Up of a Privileged Account Hack," in SecureWorld, 2017.
3. Casey Crane, "20 Ransomware Statistics You're Powerless to Resist Reading," in The SLL Store, 2020.
4. Reuters, "China theft of technology is biggest law enforcement threat to US, FBI says," in The Guardian, 2020.
5. "Insider Threats Are Becoming More Frequent and More Costly," in ID Watchdog, 2020.
6. Joseph W. Sullivan, "From the Chartroom: The Cost of China's Intellectual-Property Theft," in National Review, 2020.
7. Edward Gately, "Cost of Downtime from Ransomware Nearly Doubles this Year" in Channel Futures, 2020.
8. Filip Truta, "Ransomware Downtime Costs Doubled Since 2019, MSPs Report," in Bitdefender Business Insights Blog, 2020.
9. Patrick Howell O'Neill, "Ransomware may have cost the US more than $7.5 billion in 2019," in MIT Technology Review, 2020.

Chapter 3

10. Dahlqvist, Patel, Rajko and Shulman, "Growing opportunities in the Internet of Things," in McKinsey & Company Our Insights, 2019.

Chapter 4

11. Jessica Davis, "560 Healthcare Providers Fell Victim to Ransomware Attacks in 2020," in Health IT Security, 2021.

Chapter 7

12. "Insider Threats Are Becoming More Frequent and More Costly," in ID Watchdog, 2020.

Glossary

13. Dahlqvist, Patel, Rajko and Shulman, "Growing opportunities in the Internet of Things," in McKinsey & Company Our Insights, 2019.

thycotic

Your path to secure privileged access starts here

Free Secret Server 30-Day Trial

Protect your privileged accounts with Thycotic Secret Server, an enterprise-grade Privileged Access Management (PAM) solution trusted by more than 12,000 companies worldwide available both on-premises and in the cloud.

- Establish Secure Vault
- Discover Privileges
- Manage Secrets
- Delegate Access
- Control Sessions

Get your free
SECRET SERVER
30-Day Trial
https://thycotic.com/secretserver

Discover how critical applications, deployed in traditional infrastructures and in the cloud can be securely accessed by local remote users.

Securing critical business applications, cloud assets, and remote teams in the perimeter-less enterprise with conventional PAM tools is no longer tenable. Today's cyberthreats are simply too diverse and unrelenting. CISOs need to deploy advanced privileged access to gain secure control over web-based cloud management platforms and enforce least privileged access for remote workers.

- Explore the basics—learn why managing privileges has become more complex
- Uncover how secrets and privileges become compromised—discover the risks confronting organizations from malicious and benign actors
- Understand how application access is evolving—explore the profound changes and new risks of the cloud evolution
- Align privileged access to security priorities—understand why a secrets vault is essential for securing privileged access
- Review privileged access toolbox essentials—discover why APIs, RBACs, alerts, and logging are critical
- Get started—identify the next steps for securing privileged access in hybrid and multi-cloud environments

About the Author

John Pinson is a veteran technology executive, content creator, strategist, and journalist. He's headed content for brands such as ForgeRock and SparkPost, and frequently authors white papers, ebooks, blog posts, and web content for brands including Infoblox, Mitratech, ClimateWorks Foundation, and many others. John's bylines have appeared in Computerworld, eWeek, CNET, and other IT publications.

CYBEREDGE PRESS

Not for resale

ISBN 978-1-948939-20-1