LEARNING MADE EASY

CyberArk Special Edition

Privileged Access Management (PAM) as a Service

for dummies®
A Wiley Brand

Secure accounts, credentials, and secrets

Reduce risk from cyber attacks

Take action to secure privileged access

Brought to you by

CYBERARK®

Aaron Pritz

About CyberArk

CyberArk is the global leader in privileged access management (PAM), a critical layer of IT security to protect data, infrastructure, and assets across the enterprise, in the cloud, and throughout the DevOps pipeline. CyberArk delivers a complete solution to reduce risk created by privileged credentials and secrets, with flexible deployment options from Software as a Service (SaaS) to on-premises. The company is trusted by the world's leading organizations, including more than 50 percent of the Fortune 500, to protect against external attackers and malicious insiders.

A global company, CyberArk is headquartered in Petach Tikva, Israel, with United States headquarters located in Newton, Massachusetts. The company also has offices throughout the Americas, EMEA, Asia Pacific, and Japan. To learn more about CyberArk, visit **www.cyberark.com**.

Privileged Access Management (PAM) as a Service

CyberArk Special Edition

by Aaron Pritz

for dummies®
A Wiley Brand

Privileged Access Management (PAM) as a Service For Dummies®, CyberArk Special Edition

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

ISBN: 978-1-119-72157-4 (pbk); ISBN: 978-1-119-72241-0 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

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

Project Editor: Carrie Burchfield-Leighton

Sr. Managing Editor: Rev Mengle

Acquisitions Editor: Steve Hayes

Production Editor: Tamilmani Varadharaj

Business Development Representative: Molly Daugherty

Table of Contents

Introduction

Theft, disruption, and compromise throughout history have thrived the most when a thief obtained the "keys to the kingdom." It makes getting what is desired so easy. Why would a more cumbersome method (such as breaking through a castle wall) even be considered if you could obtain a key to walk in the front door?

One interesting historical example is the one and only successful (for a very short time) attempt to steal the crown jewels in London. In 1670, the jewels were kept at the Tower of London in a basement protected by a large metal grille under lock and key. Thomas Blood disguised himself as a parson and became friends with Talbot Edwards (the keeper of the crown jewels who literally had the key). He manipulated Talbot into a concocted relationship and staged a tour with his wealthy nephew. Once inside the room with the jewels, he knocked out Talbot and made off with the jewels (but didn't make it far).

In today's corporate world, the key to most companies' crown jewels is through privileged access, whether a privileged account, credential, or secret. Almost all of today's breaches tie back to an attacker stealing an admin account or credential. The attacker can "socially engineer" (or trick) his way to get privileged access similar to how Talbot Edwards was tricked. Privileged access can also be obtained through other means, such as searching for unsecure documents that contain credentials or by using more sophisticated "bad" computer programs (known as *malware*).

So if protecting privileged access is so critical to protecting a company's crown jewels, why aren't companies doing more to guard against these types of attacks? Well, the good news is you have picked up this book, so you likely have an interest in learning and doing more. By using this knowledge, you can help your company mitigate against privileged access security risks. With IT infrastructure, platforms, and software all rapidly moving to "as a service" models, we also examine how you can help your company successfully run Privileged Access Management (PAM) as a Service.

About This Book

This book is written with the expectation that anyone in your company should be able to read it, understand the content, and be able to better articulate the need to mitigate privileged access security risks. Often, cybersecurity books go into significant technical depth that's great for security engineering, software developers, and architects. You should expect this book to be conversational, with plenty of examples, analogies, and elements designed to make this security topic more approachable.

At the beginning of each chapter, a cyber attacker greets you and shares his or her perspectives, and *attempts* to dissuade you from learning about these important concepts that make their lives more difficult.

Icons Used in This Book

Throughout this book, I use special icons to call attention to important information. Here's what to expect:


REMEMBER

This icon points out information that you should let sink into your long-term memory. These bits and pieces are the highlights that allow you to talk intelligently on the privileged access security topic as it comes up at your company.


TIP

Tips are the recommendations for how much you should tip the author and editor (Venmo, PayPal, and all forms of crypto are accepted). Just kidding — these tips are small nuggets of value that are "nice to haves" when thinking about implementing these ideas.


WARNING

Nobody likes to make mistakes. Warnings are lessons learned from experience that you can avoid and save yourself time while securing your privileged access.


TECHNICAL STUFF

You won't find the biogenetic cure for world hunger in this text, but if you're looking to swoop down a couple levels into some moderate technical discussion, this icon's information is for you.

Beyond the Book

It's my hope that this book gives you a better understanding of PAM as a Service, but if you're left wanting more, visit the CyberArk website at `www.cyberark.com` where you can learn more about tools and services and how to deploy, manage, and optimize a PAM program.

IN THIS CHAPTER

- Learning about the types of privileged access
- Looking at internal and external risks
- Securing privileged access through high-level methods

Chapter 1
Defining Privileged Access and PAM as a Service

"My name is Ivan. I have been a 'freelance hacker' for the last few years. It started out as a hobby, but it quickly turned into a highly lucrative business for me. I never really liked the thought of having a boss, so I decided to use my skills to make money off others' mistakes in cyberspace as I manipulate them to get what I need from them or their company computer network. These days, I don't have to use most of my sophisticated hacking skills. *Phishing* people (enticing them to click on my links and attachments over email) is easy and quick to get results. I just cast my nets every day and pull in my nets later that evening to see all the little (and sometimes big) fish that I caught. I really get excited when someone who has a lot of super-secret IT or online system access to a company ends up in one of my 'nets.' My best days are when I get database admins, cloud console admin accounts, DevOps tool console accounts, company network admins, or the accounts of company executives. I call those execs 'whales' for a reason. I absolutely *love* how admins in

the cloud environments now are often people outside of IT, like Human Resources (HR) managers. New victims! Well, it's been nice chatting with you, and I hope not too many people read this book because the less you know about securing privileged access, the more money that flows into my pockets. Keep doing everything just like you've been doing. It. Is. Perfect!"

Privileged access management (PAM) is top of mind for today's security and IT leaders. Many folks are adopting PAM as a Service, as Software as a Service (SaaS) is increasingly becoming the norm for new software initiatives. External attackers like Ivan as well as malicious insiders (such as employees or contractors) routinely exploit privileged access to steal confidential information or disrupt business-critical applications and services.

In this chapter, you discover the basic types of privileged access, the responsibilities and impacts of managing access, and the risks. I also give you high-level tips on how to manage privileged access with PAM as a Service to avoid folks like Ivan.

Types of Privileged Access

Privileged accounts, credentials, and secrets are needed for an administrator, application, process, or device to access a system. They exist almost everywhere. They're part of systems, databases, and applications; they reside on-premises and in the cloud; and they're used by people as well as by applications, automated processes, machines and bots.

Privilege is a term used to designate special access or abilities, above and beyond that of a regular user. If you aren't personally an administrator at work, think about how at home you have to provide a password to download a new app on your iPad or smartphone, even though your whole family shares the device. You're the administrator of the iPad and have privileged access to the device. You're in control of what gets to be installed on that device (unless you've shared your password, which is another all-too-common story). In today's environment, which is quickly adopting SaaS-based technology, PAM services are also heading down a similar path of options.

You find two types of privileged access in a business setting. The first is privileged access *used by humans*, and the second is access *used by non-human* automated processes.

Privileged access used by humans

Human privileged access is when a human manages and uses an account and typically knows the password unless some advanced tools are in place. Types of privileged access used by humans, whether your own employees or third parties, includes the following:

- **Superuser type accounts:** This is a special user account that's used for system or tool administration, such as making configurations to a system or application, adding/removing users, or deleting data.

  Example: Jim, Sales Operations IT Manager, logs in and is authenticated via single sign-on (SSO), granting him access to a popular Customer Relationship Management (CRM) application. His role enables him to add and remove users who are starting or leaving the sales department. He also makes system level configuration changes as requested by the head of Sales. Note that a role with this level of access may be an IT employee or someone playing an administrative role in a functional area such as Sales.

- **Domain administrative account:** These accounts provide privileged administrative access across all workstations and servers within a network domain (for example, your company's network). While these accounts are few in number, they provide the most extensive and robust access across the network. With complete control over all domain controllers (I cover these more in Chapter 3), a compromise of these credentials is often a worst-case scenario for an organization.

  Example: Jacky is a server administrator at her company and has access to a common type of privileged administrative account that attackers target: a Windows domain controller account. If a hacker obtains the domain admin account that Jacky utilizes, he typically can access many servers and corresponding data across the network.

- **Cloud shadow admins:** Unlike other types of human privileged access, the cloud shadow admin isn't a type of

access that anyone has been delegated. Instead, it comes about due to lack of oversight of the permissions that are granted to users in cloud environments. People who are cloud shadow admins may appear to have no privileges but have the ability to create policies such as "allow all" that enables them to become full admins. This glitch is often overlooked by security teams because these permissions are managed outside of traditional directory services. When overlooked and left unsecured, the existence of cloud shadow admins can create unnecessary risk and increase an attacker's likelihood of success.

Example: Bob is a user with a single permission to manage other groups' members in AWS. If an attacker gains control of this type of user, he can modify the members of an existing admins group and add compromised users, in effect creating new full admins.

- **Local administrative accounts on workstations:** This account uses a combination of a username and password that helps people access and make changes to workstations.

  Example: Jane logs on to her computer with a user ID and password so she can get access to *her* workstation and can make changes, such as downloading applications, unless local administrative privileges have been removed from her workstation. If Jane doesn't have local admin privileges, the local administrative account can only be accessed by a system administrator.

- **Secure socket shell (SSH):** SSH is a cryptographic network protocol that largely uses SSH keys to provide direct root access to critical systems. The use of SSH is extremely common for both on-premises and cloud-based systems. Root is the username or account that by default has access to all commands and files on a Linux or other Unix-like operating system. Users can execute "sudo" to allow permitted users to execute commands as if they were superusers.

  Example: Bill, an application administrator, utilizes an SSH key to remotely and securely log in to an online tool hosted at an offshore facility.

- **Emergency accounts:** These accounts provide users with administrative access to secure systems in the case of an emergency and are sometimes referred to as *firecall* or *break*

glass accounts. While access to these accounts typically requires managerial approval for security reasons, it's usually a manual process that's inefficient and lacks any auditability.

Example: Devon has access to an emergency account that is a specific application administrative account for a third-party software package and has broad access to configure the application but is *not* needed for normal support. This account may be used in emergencies where other points of access aren't sufficient.

- **Privileged business user:** A privileged business user is someone who works outside of IT but still has access to sensitive systems. This could include someone who needs access to finance, HR, or marketing systems.

  Example: Jane, the HR admin, logs into the HR management (HRM) system. She has the ability to view and change sensitive information related to employee compensation.

Non-human privileged access

Non-human privileged access consists of automated processes that are also referred to as *machine identities.* Types of privileged access used by automated processes include the following:

- **Application accounts:** A privileged account that's specific to the application software and is typically used to administer, configure, or manage access to the application software. It basically allows two systems to talk to one another via the application account.

  Example: A data visualization tool that produces reports and diagrams connects to a data warehouse to pull the data. The application account automatically connects to the data warehouse without user intervention to allow the application to access the right data. The password for this account is often stored in the application itself or a configuration file.

- **Service accounts:** These special accounts are used by an application or service to interact with other accounts or services. Windows service accounts can be used to access and make changes to the operating system or the configuration. A Google Cloud Platform service account is a special account that can be used by services and applications to interact with other Google Cloud APIs.

Example: The accounting application needs to start a local database engine service on the local computer running SQL server without the user having to worry about it or even know it's happening.

- **Robotic Process Automation (RPA) Bot Accounts:** RPA is a form of business process automation technology based on software robots (bots) or artificial intelligence (AI) workers. Bots streamline operations by interacting with the user interfaces (UIs) of business applications. Bots require a lot of access to privileged accounts to perform their work. The secret to success is figuring out how to provide bots with extensive access but in a way that safeguards the business and information that you must protect.

  Example: Danny is setting up a new RPA system for his company so that routine tasks can be automated to save money. He personally needs to use the RPA tool admin account to get everything configured and maintained. However, he has to grant access to numerous privileged accounts to applications so the robots can perform the routine administrative work that is required.

- **SSH keys:** SSH keys can use short-lived certificates and are also used by automated processes. Functionally SSH keys resemble passwords. They grant access and control who can access what in modern cloud and other computer-dependent services. SSH keys have two parts: a public key and a private key. Private keys can match with public keys and authenticate successfully. For SSH certificates, a private key is not needed; the public key is signed by a certificate authority, which is passed and trusted to authenticate.

  Example: SSH keys are used in dynamic cloud environments that auto-scale infrastructure (adjust the size of the infra-structure needs based on the computing power needed).

- **Secrets:** The term *secrets* is most frequently used by developers development and operations (DevOps) teams. This is a catch-all term that refers to SSH keys, application program interface (API) keys, and other credentials used by DevOps teams that provide privileged access.

  Example: A DevOps development team may have secrets, to access a database or other sensitive resource, embedded in the software they're developing.

REMEMBER

Cloud shadow admins exist on the non-human side just like they do for human privileged users. If an attacker gets access to a cloud service account, they can elevate their permissions to gain additional access to sensitive resources.

Insider and External Risks Associated with Privileged Access

Many risks come as a result of privileged access. These risks can come from external attackers or malicious insiders within a company. Either way, the risks make it important to ensure the security of privileged access at all times. In this section, you explore why these risks are so high and where privileged access exists.

Why are the risks so high?

If an account, credential, or secret that provides elevated and privileged permissions to sensitive assets is compromised, it could result in significant damage to a company, such as

- Theft (from people inside the company or external) or accidental data loss/exposure
- Disruption in business continuity (knocking out a manufacturing facility or office)
- Data corruption or loss (changing data or information creating fraud or unusable data)

Negative outcomes that can occur if privileged access is used with malicious intent include the following:

- Leaking or stealing sensitive data leading to financial and reputational damage
- Connecting to a command and control server (this is typically a system that allows an attacker to stay hidden in your network and remotely operate systems or extract data)
- Installing bad software (malware)
- Locking true users out of their machines so only the attacker has access (ransomware)
- Conducting illegal or unauthorized crypto-currency mining

Where does privileged access exist?

Privileged access exists everywhere when you consider all the work that's now handled by automated processes instead of by people. Examples where privileged access can be found include the following:

- Cloud (cloud consoles, applications built using DevOps tools and methodologies)
- Data centers, applications, servers, network devices, and other infrastructure
- Endpoints (iPhones, laptops, tablets, and so on)
- Internet of Things (connected devices such as video cameras, wearables, augmented reality, and other smart devices)
- Industrial Control Systems that allow operators to monitor and control industrial processes in a variety of industries in oil and gas, utilities, manufacturing, chemical, and so on

REMEMBER

Privileged access can be compromised or abused by malicious people external to or within a company. Most people think of attackers as being external "hackers," but another big source of attacks comes from within an organization.

External threat actors

External threat actors typically are referred to as *attackers.* However, "attackers" is a broad term — they're everything from hobbyist hackers with a range of motivations to well-funded cybercriminals with full office building complexes and particualr targeted intentions. The latter is often funded by nation states (countries with a vested interest) or criminal organizations. Some criminal organizations sell their tools like a legitimate software provider, with customer support and toll-free helpdesks. Regardless of the scale of the external threat actor, the best day for these people is when they find uncontrolled and unmonitored privileged access.

Internal threat actors

Internal threat actors can be people within the workforce whether they're employees, contractors, consultants, or collaborators. They can range from inadvertent to malicious workforce members, such as

REMEMBER

- **Inadvertent workforce members:** These folks are team members who inadvertently compromise themselves or their companies by disclosing or losing control of a privileged account.

  Any onsite or remote workforce member (for example, employees, contractors, consultants) can be an inadvertent risk. The easiest example is someone (who can be any "insider" even if that person does not have privileged access) who clicks on a phishing email link or opens a malware infected file.

- **Malicious workforce members:** These people can be team members who aim to harm or steal from a company. An example is a system administrator within the IT group supporting all the financial and accounting systems for the company who becomes disgruntled or financially motivated to steal.

Securing Privileged Access through High-Level Methods

In other chapters in this book, I help you take a deeper dive into various methods, tips, and tricks to secure privileged access. So you may want to peruse the other chapters for more information. However, here, I give you the three fundamental categories of actions that can be taken.

People

The best processes, technology, and tools are useless if the people who interact with them aren't doing what they need to do. Fundamentally, people are the most important part of security defensive and offensive controls. However, people alone won't solve the numerous privileged access management challenges that exist. There are just too many things that can go wrong. Leveraging people to reduce risk can include

- **Workforce awareness training:** Emphasize the importance of strong passwords, following processes to guard privileged accounts, not coding applications with hard-coded credentials, and so on. Multiple stakeholders need to be involved

including IT, cloud operations, DevOps teams, and business admins because all of these stakeholders have privileged access.

- **Ethical phishing exercises:** Many companies use ethical phishing to simulate attackers trying to compromise employees through realistic and alarming looking emails that try to convince users to click links and attachments. However, more mature companies focus targeted ethical spear phishing simulations on their privileged account holders to give them additional training. These are the people who definitely must not fall for the phish.

Process

Process controls can include policies and procedures to establish a common and secure way of doing certain tasks around privileged access. Examples are as follows:

- **Just-in-time (JIT) privileged access:** Privileged access is often granted "always on", when in reality, it is only required for brief periods of time. It's important to implement the principle of least privilege to reduce standing access via JIT access. This ensures that the right access is provided to the right users for the right users at and for the right amount of time. This is consistent with the adoption of "Zero Trust" security models.
- **System administration policies and procedures:** Define how system administrators should do their job, access the systems by using their privileged accounts, and care for the credentials themselves. These policies and procedures can either dictate manual methods of controlling the accounts or require use of security tools.
- **Privileged account/credential inventory:** You can't protect what you don't know about. You need to understand where your accounts and credentials are across the organization and prioritize them to be securely managed within your PAM processes.
- **Secure coding standards:** In DevOps and other development teams, it's critical to remove hard-coded credentials from applications, robotic process automation platforms, and other non-human entities.

Technology

Technology in PAM has rapidly evolved in the last several years, with PAM as a Service increasingly becoming the preferred deployment model. PAM as a Service allows organizations to off-load the majority of the work of managing PAM infrastructure, handling upgrades and freeing IT security staff up to concentrate on risk and compliance. PAM is no different than other SaaS or security solutions being deployed as a service.

Examples of PAM as a Service system capabilities to secure cloud and on-premises workloads include the following:

- Store passwords, credentials, and secrets used by privileged human users and applications and rotate them based on policy to prevent credential theft
- Isolate access to critical assets with transparent connections to target systems to prevent credential exposure, including securing remote user access
- Implement JIT policies to minimize standing access and unnecessary permissions
- Remove local admin rights on endpoints and elevate privileges as needed to stop lateral movement
- Detect and prevent attacks involving privileged access
- Create an unalterable audit trail for any privileged operation

IN THIS CHAPTER

- Understanding the types of data loss that can occur
- Looking at privileged access requirements related to regulations, laws, and internal standards
- Recognizing the importance of audits
- Minimizing third-party impacts and risks
- Defining attacker compromise

Chapter 2
Looking at the Risks of Unsecured Privileged Access

"My name is Liam. I've been passed up for promotion for the last two years, and my boss has the world's biggest ego. I've already decided that I'm leaving the company and have luckily found my next opportunity at a competitor. I'm in the progress of 'packing my bags,' but no one at the company knows this yet. I've been on our critical engineering project that will likely result in a billion-dollar product. Most of the ideas are mine, and I've not been well compensated for bringing these ideas to the table. My plan is to spend about two months collecting all key documents about this product design (because I wrote most of them), and I plan to take them to my new job. I also realize I should bring a related, unlaunched product with me. I am utilizing a combination of documents I have access to (including those that are inadvertently exposed within the corporate network), and I've been able to obtain some admin credentials for critical

storage locations. These credentials are a jackpot for me. I can't believe they were stored in a spreadsheet in an open access network folder called 'network and cloud admin passwords.' It was the first thing I searched for. I was also able to use the cloud access keys to set up a script that runs monthly and copies newly created project files to a shadow cloud environment that I've set up. Clever, huh?!"

Is it possible that someone like Liam exists within your company? Most organizations have an insider threat risk whether they want to acknowledge it. Pay attention to the analysis of risks and impacts in this chapter that can result from Liam and his friends. If you can understand the real risks and threats, you'll be more motivated and knowledgeable in implementing measures to protect or detect them.

Defining Different Types of Data Loss

Theft of information (especially personal information) is usually the most media covered breach. Personal information (PI) breaches almost universally are required by state, federal, or country law to be reported and disclosed to the public. However, intellectual property theft currently has less mandated obligations to be reported externally. This creates an imbalance of information about threat actor motivations and what is really happening to companies.

Personal information

Protecting PI is critical and becoming more prevalent in discussions, regulations, and new laws. Complying with laws is important, but ensuring you protect the PI of your customers and other stakeholders is critical to your brand and company trust. PI, which can also sometimes be referred to as personally identifiable information (PII), is a lucrative target for the bad guys because it can be sold for sizable amounts per record to entities looking to profit through identity theft or other types of fraudulent activity. Social Security Numbers (SSN), credit cards, driver's licenses, and medical records can all be sold on the dark web (a portion of the Internet often utilized for illegal activity).

PI is any information that is identifiable for an individual (workforce member, supplier, customer, shareholder, and so on). Some examples of PI include

- Social Security numbers (SSNs) or National Identification Numbers (outside the United States)
- Customer home addresses
- Employee or contractor emergency contact info

In many countries, there is also a category of sensitive personal information (SPI), which is a subset of PI that's considered more damaging if lost, stolen, or disclosed. Examples of these are as follows:

- Credit card numbers
- Personal Health Information (PHI)

Many companies have implemented information classification frameworks that rank information by sensitivity. By using this classification, there are various information handling methods based on the sensitivity of the data. Using the maximum effort to protect every type of information a company has wouldn't be feasible or sustainable. Therefore, effort is applied more strongly where it matters most.

TIP

Securing access to the highest sensitivity assets is a good place to start a privileged access management (PAM) program. You can't do everything at once, so start with what's most critical.

Intellectual property

Intellectual property (IP) is any work or invention, such as a manuscript or a design, that's the result of creativity to which one has rights and for which one may apply for a patent, copyright, trademark, and so on. Examples of IP are source code, product patent applications, product research, and innovative manufacturing methodologies.

Confidential information

Confidential information (CI) is any information that isn't public or intended for public or broad consumption. Some types of CI include customer lists, organizational charts, and business plans.

Looking at Privileged Access Requirements

Protecting the data and information itself should be the primary driver for action. Beyond that, regulations, laws, industry frameworks, and internal company standards require proper handling of and/or enforcing privileged access. In this section, you discover some examples of regulations, laws (legal requirements), and frameworks/standards (best practices or internal requirements) that require securing privileged access.

Regulations and laws

Regulations and laws span from those that focus on data privacy protection to those that aim to prevent financial fraud. In this section, I explain some of the more prominent ones and how they tie into requirements around managing privilege access.

Regional/country/state privacy laws

Privacy laws have been strengthened or have been newly published in many countries around the world, including the European Union and United States:

- **European Union:** The Global Data Protection Regulation (GDPR) is a unified regulation for the European Union (EU) that began enforcement on May 25, 2018, for any organization that does business in the EU. This regulation protects the data and privacy of the EU citizens and has been in the works for several years, and enforcement comes with significant fines. Per the regulations, a company can be fined up to $20 million Euros (or 4 percent of revenue; whichever is higher.)
- **United States state laws:** The California Consumer Privacy Act (CCPA) is a state statute from California intended to enhance privacy rights and consumer protection for residents of California. It became effective on January 1, 2020.

  At the time of publication of this book, other states with enhanced regulations include New York, Massachusetts, New Jersey, Maryland, Oregon, Texas, and Washington. It is expected that additional states will adopt similar legislation with the potential at some point for the establishment of United States privacy regulations at the national level.

HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is United States legislation that provides data privacy and security provisions for safeguarding medical information. Strong PAM (or the lack thereof) can make or break a healthcare organization's ability to demonstrate compliance and avoid financial penalties.

A Florida-based healthcare system recently failed to review access controls and examine audit logs, giving unauthorized employees access to electronic personal health information (ePHI) through shared login credentials. The infraction resulted in a fine of $5.5 million from the United States Department of Health and Human Services (HHS) to settle violations of HIPAA HITECH rules.

SOX

The Sarbanes-Oxley Act of 2002 (SOX) is a United States federal law that set new or expanded requirements for all United States public company boards, management, and public accounting firms to disclose accurate accounting information. These laws were set after major corporate and accounting scandals, including Enron and WorldCom.

Many of the SOX controls are rooted in access management and knowing who did what to prevent or detect corporate fraud. For example, a person who configures the accounting "general ledger" is a "privileged user" and could make critical fraudulent changes if that account is compromised or not monitored.

PCI

Payment Card Industry Data (PCI) is a set of security standards designed to ensure that *all* companies that accept, process, store, or transmit credit card information maintain a secure environment. PCI requirements include elements such as appropriately managing admin passwords, access rights as "need to know," and tracking and monitoring all access to cardholder data.

Frameworks and standards

Frameworks and standards are intended to unify security related controls into commonly adopted frameworks that can help companies improve their security posture.

NIST 800-53 R4

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 provides guidance for the selection of security and privacy controls for United States federal information systems and organizations. Beyond federal systems, NIST is a widely adopted control framework across private sector companies.

Given the escalating threat landscape, a major focus area for many organizations aligning to NIST is improving the implementation of controls regarding privileged access. The most recent release at the publication of this book, Revision 4, includes an extensive array of controls that relate to protecting privileged accounts and strictly controlling and monitoring their use.

ISO 27002

The International Organization for Standardization (ISO) 27002 standard is an internationally acclaimed standard of best practice for information security. ISO 27002 is often used to help organizations meet contractual obligations with customers and business partners. Auditors worldwide also rely on ISO security 27002 as a basis for evaluating controls and/or verifying compliance to various regulations and standards.

ISO provides control guidance around protecting privileged accounts and warns that inappropriate use of system administrator privileges contributes to failures or breaches of systems. Required controls related to privileged accounts include segregation of duties, privileged password management, and the logging/monitoring of privileged access.

Addressing Audit Findings

Internal audits are typically corporate mechanisms for ensuring compliance to internal policies and procedures that often map back to regulations and laws. They also are leveraged to independently assess corporate risk.

As audits occur within an organization, it's typically not acceptable to have repeat findings. Repeat audit findings signal that the executive leadership team and its organization aren't taking audit findings and company policy or procedures seriously. The repercussions of a repeat audit finding typically result in additional forms of action ranging from disciplinary action from Human Resources, team reorganizations, or even terminations of employment. In many organizations, these findings are reviewed periodically by the board of directors and/or the audit/risk committee.

WARNING

Not fixing issues signaled in audits are obviously bad for leaders and the morale of the department (because audit issues are often very visible and point out failed processes and controls), and this poor practice puts the company at risk. With the stakes rising higher and higher in cybersecurity, there is more scrutiny on audit findings as company boards, audit committees, and risk committees don't want their company to have the next breach heavily covered in the media.

TIP

Internal and external audit groups like to see problems solved holistically versus in a "one-off" or "whack-a-mole" fashion. Developing solid processes and tools for managing privileged access risk is a good opportunity to avoid repeat audit findings or scrutiny. See Chapter 5 for more information on implementing processes and tools.

A RETAIL EXAMPLE

An example of what can happen in a breach can be seen from a recent large United States retailer breach. As a repercussion of this highly publicized breach, a class action lawsuit was filed against the company. A "derivative suit" was also filed by shareholders against the board of directors for allegedly breaching its fiduciary duties and then later dismissed. Other high-profile breaches have led to dismissal of several C-level leaders, including CEOs. These actions send a new message that accountability extends beyond the IT and security leadership.

Third-Party Impacts and Risks

Many companies use third-party vendors and suppliers to drive key business processes or support functions. From a business standpoint, this allows a company to be more flexible as its business ebbs and flows.

However, managing third-party information security risk and specifically privileged access risks isn't without challenges. There are several notable breaches that brought third-party risk front and center within corporations. One retail home improvement store had a compromise stemming from stolen third-party vendor credentials and malware. If the attackers didn't possess third-party vendor credentials and if the payment network was segregated from the rest of the network, the results may have been different.

Another risk related to third parties that organizations should consider is related to hiring remote vendors to manage all or part of an organization's IT infrastructure. This creates significant risk if there aren't clean processes in place to provision and deprovision third-party access and if proper controls aren't in place to monitor the privileged access of these third parties.


TIP

A recommended best practice is to isolate third parties who manage sensitive IT systems from direct access to corporate networks and systems to reduce risk. This process prevents malware from a remote vendor's endpoint from infecting the network.

Defining Attacker Compromise

Hacker compromise is largely the most sensationalized form of compromise covered by the media. Allegations of nation state funding and coordinated cybercrime and hacking groups drive a scary but intriguing story line. Some countries have been accused of sponsoring hacking groups for various political, social, economic, or financial motivations.

Attackers often find ways to find human and non-human privileged access for applications, scripts, cloud environments, and other machine identities to lead to another elevated form of access. This practice is called *pivoting* or *vertical and lateral movement.* The

first point of access is known as a foothold to be able to move from place to place laterally inside a company's network. As the attacker moves laterally, his or her ultimate goal is to gain access to privileged accounts, credentials, and secrets to steal data, encrypt data with ransomware, or engage in illegal crypto-mining operations. The impact of these illicit activities can affect confidentiality, integrity, and availability.

Data theft (confidentiality)

Data theft, often referred to as *data exfiltration,* is typically the motivation of identity thieves in taking confidential personal information or payment info to sell or utilize fraudulently. Additionally, theft of intellectual property and company secrets is often a target for unethical companies or nation states to improve competitive and economic advantage.

Malicious insiders (employees or contractors) could also be the source of data exfiltration for a variety of reasons and motivations. Enhancing controls on protecting privileged access can reduce risks from both internal and external threat actors.

Data corruption/manipulation (integrity)

Data corruption or manipulation that affects the integrity of data is often associated with financial fraud but can be driven from other motivations as well, such as embarrassment and stock price manipulation.

The cult classic movie *Office Space* depicted several disgruntled IT employees utilizing their privileged access to shave off pennies on all the dollars in the financial system to then be deposited into their accounts. The collusion of several IT employees was necessary to get enough access to make the change.

Despite this being a fictional comedy, this topic depicted both insider threat (the employees) and data manipulation (shaving the cents off the dollar). It also shows how privileged access can be abused (by the internal workforce) to fraudulently compromise a company.

Ransomware (availability)

Ransomware is a technique of using a computer virus or malware to hold data hostage and make it unavailable. While this technique has been around for decades, it has grown in volume over the last couple of years. The technique is similar to kidnapping in that you take something of value to someone and threaten to not give it back until a ransom (money, often crypto-currency) is exchanged. Recent ransomware tactics didn't have the capability or intention to recover the files that were held hostage because the files were *permanently* wiped.

The more access a user has to his computer (for example, local domain rights) the more susceptible it is to ransomware.

WARNING

Please be aware that even if you pay the ransom, you may never see your files again. This is similar to a kidnapper who has no intention of returning the victim after the ransom is paid. Some organizations may not be allowed to pay ransom and then have to hope they can recover their data from a backup or another type of forensic recovery method.

IN THIS CHAPTER

- Looking at Commercial Off-The-Shelf (COTS) applications
- Managing servers, databases, and network devices
- Locking down endpoints and IoT devices
- Exposing industrial control systems

Chapter 3
Securing Privileged Access for On-Premises Assets

"My name is Michela. I'm the self-proclaimed queen of malware. I've been doing this for a while, but my job has become a lot easier in recent years. These days I'm making money by crafting my killer logic into an actual hacking platform with features that I sell to other less brilliant people on the dark web. I can make more money and have less personal risk because I'm not the one taking actions against companies. I've spent a lot of time building a high-quality product and have a 24/7 call center to help my users with any problems they may have, which there aren't many because my software is so awesome. My biggest claim to fame is the method I use to obtain privileged credentials. After I have these, my software can perform actions on a significant scale to obtain access to the applications with the most sensitive information. I call this module 'Lateral Collateral,' and it's a bestseller. I'm confident that if companies don't shore up their defenses to solve the 'privileged access' problem, they aren't going to be able to stop me and all my customers from doing what we do."

If Michela and her thriving Cybercrime as a Service business doesn't scare you out of your pants, you may just be in a coma . . . (or a long time cybersecurity professional who has seen it all). Privileged accounts and credentials are often referred to as "the keys to the kingdom." If you want to prevent Michela and her fellow attackers from compromising your sensitive assets, pay attention to the types of environments and systems that you may have at your company and how to better protect them.

COTS Software, including IT and Security Applications

Commercial Off-The-Shelf (COTS) packages are enterprise-ready software products that are made by a company other than your own. As a result, your organization's critical systems and sensitive data are only as secure as the privileged accounts and credentials required to access these applications as well as the applications themselves being properly vetted, QA'd and secure.

COTS package use has significantly declined with the rise of Software as a Service (SaaS). That said, many companies are still dealing with legacy software and systems for the foreseeable future. Managing privileged access for COTS software also remains important. This shift to SaaS can also lessen your organization's institutional knowledge of these applications and how to protect them. Even if you have a smaller footprint of this type of software remaining, don't forget about it and the risks that come with not managing privileged accounts.

WARNING

When COTS application privileged credentials aren't handled securely, accounts and credentials can be comprised by attackers and then used to pivot to other more desirable systems and data. A common way to get into an administrator account of a COTS package is to find a system that used an *installation account* (a username and password used to initially install the system and usually having full administrator capabilities). The attacker essentially attempts to log in with this default password found in product install manuals available on the Internet.

Other examples of COTS privileged access security issues include the following:

- Many organizations overlook that COTS software itself is often granted administrative privileges to access other sensitive assets in the network. This is especially the case for COTS software that performs security scans. Software often uses automated processes that require privileged credentials.
- Credentials are often stored in COTS applications' configuration files or databases.
- Credentials often remain unchanged because of the administrative burden required to rotate them periodically or because it requires application downtime.

Servers

Servers are systems that do a lot of the heavy lifting in a typical data center, from serving web applications to acting as a file server. If an attacker can get directly into the server by using an administrator password, it's likely she can find data to steal or havoc to wreak without having to even directly log into the application. It's like going in an unlocked back door of a house after finding the front door locked.

Most servers are now virtualized, which means that a single physical server can be logically divided into multiple "virtual" servers. Access to the virtualization layer and each of the virtual machines needs to be secured.


TECHNICAL STUFF

Containers offer another type of virtualization but at the operating system level instead of at the server level. They're favored by developers and DevOps teams because of the flexibility they provide. The main thing you need to know is that you need to secure the privileged access to physical servers, virtual servers, and containers.

A domain controller is a specialized type of server that responds to security authentication requests (logging in, checking permissions, and so on) within a Windows domain. This allows an administrator to grant access to a number of computer resources for a single user, account, or credential. Securing access to domain

controllers is critical because if an attacker gains access to these systems, she can pivot to a large number of other computer assets and servers.

Databases

Databases connect to a server (see the preceding section) and represent a consolidated source where sensitive data often resides. Gaining access to the credentials of a database administrator allows an attacker to steal sensitive data or encrypt it in the case of a ransomware attack.

Beyond the database administrator passwords, application credentials often allow an application itself to "talk" to the database to add, edit, or remove information from it. It's risky to have unchanged passwords that are hard-coded (physically written into the application's code itself) because these can be a major vulnerability.

Network Devices

Network devices include routers, switches, firewalls, and so on. They make the computer network run. However, when they're left unprotected, they can leave your company's computer network exposed to both attackers and malicious insiders. Like other IT systems, assets, and tools, these devices also have privileged accounts and credentials that allow an administrator to log in and perform any necessary changes or configurations.

Endpoints

Endpoints can include computers and mobile devices such as smartphones and tablets. Many common business tasks, such as installing software, require privileged access. Some companies, by default, give employees admin level access to their own laptops for this reason. Unfortunately, this practice can leave these employees, their laptops, and the entire network open to significant risk. A common technique to exploit these risks is a phishing

campaign whose sole aim is to obtain the local administrator accounts on the computer. This can enable the attacker to then pivot to other exposed systems quite easily.

It's important these days to explore endpoints that are accessing your internal network from outside of your company's four walls and how this exposes your company to risk. Examples are external workforce (contractors and consultants) as well as individuals using personal devices (whether part of a bring-your-own-device — BYOD — program or not). This is even more critical if any of your remote workforce has access to sensitive on-premises systems.

IoT Devices

The Internet of Things (IoT) is a system of interrelated computing devices that are provided with unique identifiers and the ability to transfer data over the Internet without requiring human-to-human or human-to-computer interaction. Examples of IoT devices include a heart monitor implant, a farm animal with a biochip transponder, or an automobile that has built-in sensors to alert the driver when the tire pressure is low.

A good example of IoT security compromise is a security researcher who tested his hacking skills by hacking into his smart coffee machine and sending it commands without any authentication. If you can take control of a coffee maker, what's next? This becomes even scarier when you think about connected vehicles, planes, or medical devices.

Industrial Control Systems

For decades Industrial Control Systems (ICS), which are critical production systems in industrial enterprises and manufacturing facilities, were completely isolated from IT systems and the Internet. An example of an ICS device could be something like the software to control a liquid pump, machinery, or even robots.

The network for ICS systems is often referred to as Operational Technology (OT). But as IT and OT networks converge to enable more direct control and more complete monitoring, ICS systems are now exposed to IT systems and the Internet, significantly increasing the chances that these devices become compromised or hacked. When you think about the implications of these devices getting compromised, the fears of facility availability, safety, product quality (by way of integrity of the data and the product the machinery touches), and theft of manufacturing secrets may all come to mind.

WARNING

An ICS compromise can occur if you engage in any of the following risky practices:

- A high number of administrative or privileged accounts that enable user and application access to ICS systems
- The use of shared accounts that enable access to automated critical systems without human interaction
- The use of industrial applications with embedded hard-coded credentials
- The use of workstations on the OT network with full administrator rights
- Insertion of a USB (infected with malware) into ICS equipment, which launches a "worm" (malicious software designed to disrupt and then expand or "worm" its way through the network)

IN THIS CHAPTER

- Understanding the types of cloud
- Securing the cloud management console
- Sending and receiving requests with secure API access keys
- Protecting cloud infrastructure
- Securing SaaS applications
- Deploying custom-built apps securely
- Managing cloud permissions

Chapter 4
Securing Privileged Access for Cloud and Dynamic Applications

"Fernando Cirrus here. I recently left one of the major cloud service providers to pursue my own 'start-up.' After helping architect significant cloud solutions, I've personally realized that most services themselves are pretty secure (the cloud provider's data centers, platforms, and so on). However, companies that are leveraging cloud-based infrastructure, using code repositories, and creating containerized applications are making some simple mistakes that make my new start-up successful. My company is focused on obtaining (through any means necessary) and selling sensitive data to the highest bidders. I feel like a prospector exploring for the next mother lode of gold. I have a network of cloud-knowledgeable operators that are able to prey on the mistakes of others to find and retrieve the golden data, and of course opportunistically leverage other cloud data and

resources. The funny thing is some simple processes and helpful tools could minimize these companies' risks, but they're so busy rolling out new applications that they aren't all adopting these processes and tools like they should. This is fine with me though!"

Do you want to steer clear of the Fernandos in the world? If your answer is yes and your privileged access program hasn't yet considered all the potential sources of compromise in your cloud infrastructure, DevOps tools, and cloud native applications, read this chapter to discover more about the specific areas of cloud risk to focus on.

Understanding the Types of Cloud

In today's age of digital transformation, many organizations are aggressively taking advantage of the benefits of Software as a Service (SaaS) by transitioning from traditional on-premises to cloud-based deployments. In fact, some newer organizations are cloud native (only run cloud-based applications and infrastructure.)

There are multiple types of cloud-based infrastructure:

- **Public cloud:** The computing infrastructure is hosted by the cloud vendor at its facilities and shared between many organizations. Today, this is the most widely used form of cloud computing and is becoming increasingly widespread and feature rich.
- **Private cloud:** The computing infrastructure is dedicated to a particular organization and isn't shared with others. It's server-based computing residing on customer data centers and managed by the owning company. Many companies are deploying technologies such as OpenStack to enable private clouds that offer some of the same self-service and dynamic capabilities as the public cloud.
- **Hybrid cloud:** The organization hosts some applications or services on-premises, and other applications are hosted in the public cloud. This approach is common because many

organizations have a mix of on-premises and cloud infrastructure.

- **Multi-cloud:** The organization uses several different clouds, including multiple public cloud vendors or a combination of cloud providers and their own private cloud.

  The 2019 State of the Cloud Survey found that 84 percent of enterprises have a multi-cloud strategy, with hybrid cloud being the most common model.

TECHNICAL STUFF

REMEMBER

Hybrid environments, which are the norm for many companies, are often quite challenging because organizations need to secure both the on-premises and cloud environments. Also, as organizations are increasingly using multiple public cloud providers, the connection to consistently and effectively managing privileged access across all cloud providers and environments has never been more important. Companies don't have the time to have separate tools and processes across every provider.

Some other cloud-related terms fall into the "as a Service" category:

- **Infrastructure as a Service (IaaS)** provides basic cloud computing capabilities, focused around compute, storage, and other resources. IaaS capabilities are offered by all the major public cloud vendors.
- **Platform as a Service (PaaS)** provides organizations with a platform for application development and deployment. Some PaaS platforms include compute and are really extensions of IaaS, while other PaaS platforms don't include compute but instead enable enterprises to more easily run their applications in the compute environment of their choice.
- **Function as a Service (FaaS)** is a serverless way to execute modular pieces of code. FaaS lets developers write and update a piece of code on the fly, in real time, which can then be executed in response to an event, such as a user clicking on an element in a web application. This makes it easy to scale code and is a cost-efficient way to implement microservices (which are basically pieces of code that perform functions that can be built together like Lego blocks).

- **Software as a Service (SaaS)** is a popular option that allows software to access online and purchases via a subscription versus buying a version and deploying it independently. Companies are also increasingly purchasing applications, such as accounting, Human Resources, and sales management as a service. With SaaS, the application user gets web-based access, and the organization doesn't have to invest in computing infrastructure to host the application or worry about keeping the application up to date because this process is handled by the SaaS provider.

REMEMBER

As cloud vendors make clear, security in the cloud is a *shared* responsibility. Though the public cloud vendors take great efforts to secure the cloud infrastructure (such as basic compute, storage, networking), their customers are fully responsible for protecting basically everything above the computing infrastructure provided by the cloud provider, including the operating system, network and firewall configuration, applications, identity and access management, and data. Similarly, organizations leveraging SaaS need to secure and monitor access to these applications as well.

Cloud Management Console

The management console to public clouds is an incredibly powerful portal that enables complete management and control of an organization's cloud resources. This truly holds the keys to the cloud kingdom similar to the way certain privileged assets like domain controllers or root accounts hold the "keys to the kingdom" for on-premises infrastructure and applications. This console is typically accessed by both humans and automated scripts (for example, coded instructions that use secure keys and other credentials to access the required resources). Consequently, cloud management consoles are attractive targets for attackers.

If an attacker reaches the management console, the impact can be significant. This can lead to data extraction, a shutdown, or a takeover of the entire cloud environment. *All* use of the management console should be considered privileged access, and organizations should secure and actively monitor any and all potential access paths to the management console.

CLOUD-FOCUSED ATTACKS

The cloud-focused attack called "Cloud Hopper" breached several major enterprises, including five top technology companies, and lasted several years. According to the FBI, the malicious actors, from a nation state, sent spoofed emails to individuals that had privileged credentials. The attackers used a "spear phish" approach (using customized info to trick the specific recipient) to install malware that enabled them to obtain privileged credentials. According to press reports, the attackers were successfully able to gain enough privilege to move (hop) across the jump servers which separated the compute provider from their clients, extracting vast amounts of data and IP. Tightening controls around how these credentials are managed can lessen the risk of this sort of compromise.

API Access Keys

Application Program Interface (API) access keys are widely used to allow cloud and on-prem applications to "talk" (send and receive requests) to other applications and functions in cloud and on-premises environments. This could include requests like stopping or launching (starting) a virtual server or container, copying, or erasing a database.

Automation enables organizations to leverage the dynamic capabilities of the cloud to the fullest by executing code and scripts and invoking orchestration software that coordinates activity between cloud components and other automation tools. Each case uses API keys to provide secure access.

WARNING

The bottom line is that if not properly secured and rotated, these API keys can increase cloud vulnerabilities and potentially enable unrestricted access to the cloud environment. Because API access keys are powerful credentials and used widely, securing them and applying the principle of least privilege (meaning limiting the access or privilege of the user, whether human or machine, to the minimum needed for a specific job or role) is imperative. After an attacker has API access keys, the attacker could escalate privileges and potentially gain unrestricted access to sensitive data stored in the cloud.

Cloud Infrastructure

Cloud-based infrastructure enables compute, storage, and other resources to be provisioned dynamically as needed, typically to support some form of containerized application. In simple terms, if a food delivery business's mobile ordering application uses cloud-based infrastructure and needs certain cloud-based compute resources to run on a regular weeknight, and then with the national final broadcast live at 8 p.m., orders spike dramatically, new cloud compute resources are automatically made available on-demand and released as needed. It's like having just the right amount of food to meet every hungry guest's needs (literally, in this example).

Assume the food delivery ordering app comprises of multiple container-based microservices (for example, restaurant selection, menu presentation, ordering, kitchen scheduling, driver scheduling, customer payment processing, driver tracking, survey, and so on). When each container or serverless function is initiated and launched, it will be assigned privileged credentials that must be secured.

SaaS Applications

While many enterprises use SaaS business applications such as Salesforce, Microsoft Office 365, or SaaS-based social media tools such as Twitter and Facebook, the critical need to secure the administrative consoles for these cloud-based applications isn't always fully recognized until there's a problem — such as publicly posted corporate data stolen from a SaaS-based application or a hacker's Tweet on a corporate social media account.

SaaS admin consoles are often used by enterprise administrators to grant access to individual users, such as by a sales administrative leader for Salesforce or by a marketing leader to establish a common shared account for social media or another shared business application.


TIP

Using Multi-Factor Authentication (MFA) is a best practice to secure access to SaaS applications along with privileged access management (PAM) controls for SaaS admins and others who have highly privileged access to these applications.

Custom-Built Apps with DevOps

The DevOps or Continuous Integration and Continuous Delivery (CI/CD) pipeline helps organizations increase business agility by reducing time to deployment and bringing new applications and services into production faster. This approach typically leverages containerized application platforms, such as Kubernetes, and powerful automated tools to enable services to be automatically built and deployed. Privileged access to these containerized environments and powerful tools is obviously important.

In addition to the DevOps tools themselves, credentials in the application code that "flow" through the pipeline must also be secured. Cloud native applications, such as containerized apps running in a Kubernetes environment, typically rely on a large number of embedded application credentials and access keys. In this case, the application is comprised of multiple containers, with each container providing a specific microservice (such as order verification, inventory check, and so on). Containers can be automatically created and terminated to meet changes in demand, enabling high levels of stability and availability. However, to secure the application, all these dynamically created containers need credentials to interact with the other containerized microservices as well as to securely access databases and other sensitive resources.

TECHNICAL STUFF

Applications are based on code, and the consequences are serious when hard-coded credentials, such as secrets, passwords, and cloud access keys, are deliberately or inadvertently included in the application code.

WARNING

While easily done, hardcoding and embedding credentials in code or scripts creates significant risk:

- They're nearly impossible to rotate, because you don't know what else is using the credential, making credentials an easy static target for attackers.
- Their usage is difficult to track because many scripts, automation tools, applications, and humans have access to them.
- It's difficult to monitor or assign accountability to the applications that may be using the credentials without a centralized credential management function.

- They're risky because application credentials can be used to gain access to important and sensitive systems, and they're frequently targeted by attackers.
- If the organization suffers a breach, you need to manually rotate the credentials, first finding where they're used, changing them, and once changed, dealing with the consequences of the credential(s) that weren't updated blocking apps from running.

Cloud Permissions Management

As companies speed to migrate to the cloud, and often are managing a multi-cloud environment (not just one cloud provider), the challenge of managing permissions across the different cloud platforms can be great, especially as these permissions are increasingly used by automated processes. Many of the stories about breaches involving cloud platforms involve misconfigured and exposed storage areas without sufficient controls on who has access, with the "who" often being a machine identity vs. human admin. This is kind of like having a security system in your house, double locks on all doors, a really big dog, but then leaving the doors unlocked and the windows open. Security is only good if it is turned on and managed appropriately.

Evolving modern solutions allow cloud stakeholders (security, operations, admins, and developers) to get visibility and control of their cloud environments while keeping "least privilege" (only giving access when it is needed).

Think about it. If your company has systems and projects running in Amazon, Azure, and the Google Cloud Platform, and permissions need to change dynamically often and rapidly, you can't successfully do this with three different teams each trying to run its own manual processes. Companies using modern multi-cloud must think about how to streamline this experience to meet their internal customers' demands and "need for speed" without sacrificing security.


TIP

Look for solutions that can integrate, automate, and simplify your ability to manage permissions across numerous (and growing) cloud environments.

IN THIS CHAPTER

- Understanding the attack life cycle
- Following guiding principles to manage risk with privileged access
- Taking critical steps to action

Chapter 5
Getting Started with PAM as a Service

"My name is Tai-Shu. If you've read this book up to this point, you've already met some of my dear partners in crime. You can consider yourself lucky because most cyber magicians never reveal their tricks. The things I'm about to tell you will make life much harder on me and my friends. The fact is that I'm constantly evolving my techniques. You and your company need to maintain a committed focus on your processes and technology to keep up with me. However, the defensive technology is getting much better than I've ever seen in previous years. Five years ago, company defenses consisted of telling admins not to write down or share passwords. Now there are robust privileged access management (PAM) programs and automation tooling to monitor for anomalous privileged activity. The smarter these systems get, the sneakier I have to be . . . and I'm running out of sneakiness. I've already said too much; it's time to step up my game. Tai-Shu signing off."

This chapter contains many secrets, tips, and tricks to keep folks like Tai-Shu out of your company and, most importantly, *not* stealing credentials and escalating privileges to gain access to

your most sensitive applications, infrastructure, and data. You need to understand his attack life cycle because it's also similar for his friends. The more that you can understand the attack path, the smarter you'll be on defending against attacks. From there, I help you plot out a path for a top-notch PAM as a Service program.

Understanding the Attack Life Cycle

Motivated attackers will find a way into your company, but how are they able to prolong their undetected presence once inside? Privileged access is often used to get in and stay in the network and on systems, whether located on-premises or in the cloud. It's often hard to detect this because it looks like a normal privileged user or service is logging on.


TECHNICAL STUFF

Time seems to be on the side of the attackers as they have months and months to lurk in the shadows, undetected. A recently published Ponemon study revealed that 68 percent of organizations have experienced an advanced attack within the last 12 months. An advanced attack is designed to evade an organization's security defenses. IBM also surveyed 507 previously breached organizations and found that the average time to identify a breach in 2019 was 206 days and to contain a breach was 73 days, for a total of 279 days.

In Figure 5-1, you see a visual representation of the attack life cycle. This image outlines how "escalating privilege" or obtaining and using higher and higher levels of privileged access are a fundamental mechanism to a successful attack.

Essentially, the external attackers obtain an initial foothold to a company through finding a gap in security. Then, they find a privileged account, compromised user credentials, or secret to leverage. On the flip side, internal attackers may already have this access or be able to find the credentials (often exposed somewhere on-premises or in the cloud).

In the next few steps, the attackers figure out how to get their access elevated to see as much as they can, scan for goodies (reconnaissance), and move laterally and vertically to the most interesting things they want to take or exploit.

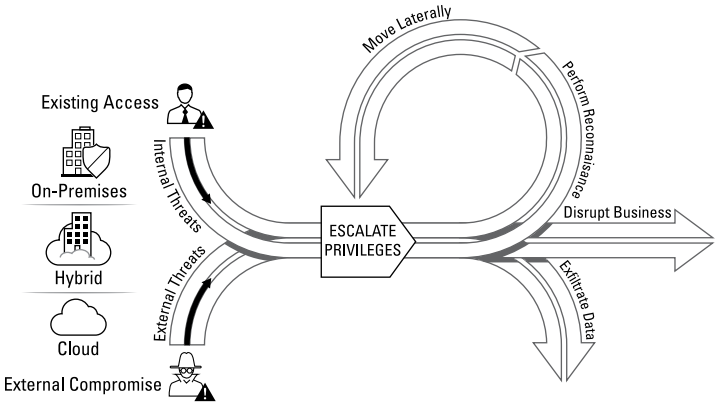

FIGURE 5-1: The attack life cycle.

Using Three Guiding Principles to Manage Risk with Privileged Access

You can use three simple high-level guiding principles to guide every program across every environment type. Think of these as the goals or risk reduction outcomes for any PAM program. Every action you take for your company should enable one or more of the principles in this section.

Preventing credential theft

Preventing credential theft starts with keeping the bad guys from getting the keys to the kingdom. The vast majority of cyberattacks today rely on getting privileged accounts, domain admins, IaaS admin, API keys, and beyond. So, locking these down through activities to prevent theft is step one. Three recommended actions for preventing credential theft include the following:

- **Use session isolation to prevent credential residue from hitting machines.** This means finding ways to allow privileged users to connect to systems without exposing the password to end-users or their machines.

- **Remove hard-coded credentials from apps, scripts, and code repositories.** This involves finding anywhere that your credentials and passwords are embedded in clear text and replacing them with a secure API call.
- **Detect and block threats that are trying to access credential stores on endpoints.** This involves using monitoring capabilities to determine suspicious credential activity and blocking their ability to proceed wherever possible.

Stopping lateral and vertical movement

Stopping lateral and vertical movement focuses on enforcing credential boundaries, just-in-time access, and credential randomization to block the attacker from moving up and on to bigger or broader parts of your kingdom. Three recommended actions for stopping lateral and vertical movement include the following:

- **Use credential boundaries with session isolation to limit an attacker's range of motion.** These methods limit the range of motion for any given account. This ensures that an attacker can't simply steal one credential and then have access to your whole environment.
- **Randomize credentials to eliminate account reuse and reduce the overall time to live.** This is enabled by tools that can automatically reset passwords after every session or enable access without the human knowing the password.
- **Enforce just-in-time (JIT) access by providing privilege only when needed.** With this approach, you elevate access to higher levels only for as long as needed and then promptly remove the access.

Limiting privileged escalation and abuse

Limiting privileged escalation and abuse focuses on stopping adversaries from attaining elevated access to resources that should normally be unavailable given the level of privileged access they have. Three recommended actions for limiting privileged escalation and abuse include the following:

- **Enforce least privilege to reduce the attack surface and control elevation.** Privileged access and permissions should be limited to drive down risk.
- **Analyze session activities to look for signs of anomalous or malicious activity.** In other words, sort the good from the bad, so you can stop the bad.
- **Implement continuous session monitoring to stop threats early.** Monitor privileged user activities and automatically respond by cutting off malicious access.

Taking Critical Steps to Action

When it comes to privileged access security, ultimately, information security leaders and their companies need to determine the answers to the following strategic questions and decisions:

- **What should we do and when?** You can't do it all at once.
- **What's the best mix of controls?** Balancing effort across preventative, detective, and responsive controls that you could spend time and money on is important to make progress.
- **How much is enough?** Find the balance between "sufficiently secure" and "overly restrictive."

This section provides more detail to address these three key strategic questions.

Assess your environment

Knowing your scope of exposure through the use of privileged accounts, credentials, and secrets may seem like a daunting initial task. Depending on how many IT assets (systems, databases, applications, and so on) you have, there could be tens, hundreds, thousands, or hundreds of thousands of privileged credentials to secure. As more workloads move to the cloud, understanding whether human and machine identities have excessive permissions is another area that must be investigated and continuously monitored.

Depending on the culture and style of the teams and leadership, some Chief Information Security Officers (CISOs) set a goal to deploy a comprehensive program and others begin with a more exploratory "top risks" approach. This may entail identifying a small set of privileged accounts to secure first before expanding their ambitions toward more comprehensive coverage.

The bottom line is, you can't protect what you don't know about, so it's crucial to start somewhere and take an inventory, so you can prioritize your actions. Regardless of whether you can develop a process in house or bring in consultants to guide you through it with expertise, I can't emphasize how important it is to get this done right up front.

REMEMBER

Regardless of approach, it will still be important to continuously determine progress, priorities, and opportunities to secure privileged access and reduce unnecessary permissions. Flip to Chapter 1 to assess the types and categories of privileged accounts, credentials, and secrets that you have in your organization. Then, choose whether to launch a full discovery and inventory of all privileged access and establish ownership for each, or start smaller if you need quick wins to prove out a process or technology.

Classify types of privileged access by risk

After or during your inventory process, you need to determine a method to evaluate risk. You can't fix everything at once, and most organizations determine where to start by using a risk-based approach. Some examples of risk-based prioritization may include identifying the following:

- The organization's most critical users and systems (if you have a system classification process or a list of critical systems ranked by confidentiality, integrity, and availability concerns)
- Systems that contain data that needs to be secured due to regulatory requirements
- Systems with intellectual property or customer data
- Known vulnerable systems (if issues have already been identified from audits, pen tests, and so on)

TIP

In many companies, previous work has already been done to identify the organization's "crown jewels," so definitely use that if it exists. It also may be helpful to do a pilot by starting with a small set of accounts that aren't critical to test your process, so you aren't experimenting on a critical system.

Evaluate existing process effectiveness

During your discovery process and inventory assessment, gather any details around existing processes to protect privileged access. This step is important as you develop the go-forward process to secure privileged credentials.

Timing is another critical decision. How are you going to mandate that action takes place? Some ideas include the following:

- Launch an iterative process improvement initiative. Build on good existing processes. Build in fixes to gaps that you observe.
- Time your project as part of, or immediately following, a major project, system launch, or infrastructure refresh (such as removing local admin rights on endpoints as part of a workstation refresh initiative).
- Secure privileged access as new applications are introduced or as existing on-premises applications are "lifted and shifted" to the cloud.
- Drive a strategic sourcing initiative to make it a requirement that there be robust privileged access controls to manage third-party access when any new outsourced provider is selected.
- Work with cloud security architects to evaluate the risks associated with over-permissioned access for human and machine identities for cloud workloads.
- Have the security team reach out proactively to its DevOps counterparts to secure privileged credentials and secrets as an integral part of the build, deploy, and operate DevOps cycle.

Establish a PAM program with KPIs

When creating a PAM as a Service program, set up key performance indicators (KPIs) to help your company know how well it's doing in the cyber risk management game. Example KPIs may include

- Time to onboard credentials when new servers and virtual machines are rolled out
- Percent of Tier 1 infrastructure such as database servers, Continuous Integration servers, and domain controllers secured with session isolation and monitoring
- Percent of Tier 1 applications that are vaulting and rotating application credentials versus using hard-coded secrets
- Percent of critical workstations that have local admin rights removed
- Percent of users accessing sensitive systems via the PAM as a Service solution leveraging multi-factor authentication

Enable organizational change management

The biggest mistake you can make in cybersecurity is to assume buying a cyber tool or technology alone reduces risk. Some of the hardest and most important work is getting that tool to an appropriate scale of use so it mitigates risks to an appropriate level and making sure that the people using the tools are enabled to utilize them correctly. There is no easy button for this, despite what you may hear from sales reps.

In order to get any PAM as a Service capability to scale, you need organizational change management (OCM). OCM should be a foundational effort within every cybersecurity project, especially if you're implementing PAM as a Service. OCM has five themes for PAM. Each has several tactics:

- **Top-down consistent messaging:** Active and visible leadership fosters partnership among senior leaders and drives user buy-in. People support what they see their leaders support. Maintain ongoing communication vehicles such as a Slack channel or monthly newsletter.

- **User enablement:** User enablement is critical to the success of your PAM program and shouldn't be neglected. Invest in end-user training and admin guides to help drive usage.
- **People's pulse:** Show Me Sessions, Lunch and Learns, and Open Microphone type sessions provide opportunities for two-way communication. These examples are various ways of having live or virtual sessions to get people engaged and talking.
- **Gamification:** Contests promote adoption and engagement. A little healthy competition never hurt anyone.
- **Empowering operations:** Look at ways to empower your operations teams. Some ideas to consider include implementing a single request system for all privileged access requests and automating the onboarding of new privileged accounts.

Invest in PAM team training and skills

Training and building the right skillsets across your organization is a critical action. Investing in this up front saves you time over the life of your program. When going about training, you have three audiences to consider.

PAM as a Service team

The PAM as a Service team includes roles such as the PAM architect and PAM engineers. The investment your organization makes in training these team members pays off in terms of your ability to derive the maximum value from your PAM as a Service investment. Ideally, this team should have scripting skills or know how to use APIs; if not, it can hopefully work with others in the organization with these skills to automate as many privileged access tasks as possible.

Internal customers

Your internal customers are those that utilize PAM services for their systems and applications. They include privilege users, operations teams, application developers, and application owners. This population makes or breaks adoption. You want to make training and the services they consume as intuitive as possible so they will see the benefit and advocate PAM to their peers.

External teams

Your external teams are those that support or interact with PAM indirectly such as the Security and Operations Center (SOC) and Compliance and Audit teams. Although not direct users, they need to understand the value that an effective PAM program can deliver to them. For the SOC team, sharing information bi-directionally between PAM and Security Information and Event Management (SIEM) solutions can eliminate information silos and unify threat intelligence across the enterprise. A well-run PAM program can reduce the time needed to complete an audit and reduce audit findings.

Establish the right partnerships

You must establish the right partnerships among security architects, IT operations, DevOps, developers, and business leaders to reduce privileged access management risk. This may feel like a lot of work, but trust me, it will pay off when you're in execution mode. You should find a way to "sell" your privileged access management initiative by focusing on the productivity benefits *in addition to* security. Finding these opportunities for the win-win among security, IT Operations, and DevOps teams could result in a significant timesaver for doing routine or mundane activities. Examples of win-win benefits for IT Operations are shown in Table 5-1.

Select a PAM as a Service platform

TIP

To help you pick the right PAM platform, consider the essential activities in this section.

Use automation

Determine where automated tools and services can *help* you (versus doing something manually). While ultimately it's better than doing nothing, manually protecting, managing, and monitoring privileged access can be a tedious, time-consuming, and resource-draining process.

WARNING

In addition, manual analysis and alerting can be prone to human error, and the consequences of failure can result in millions of dollars spent in incident response, recovery, and lost productivity. Implementing privileged access tools that automate these manual tasks drives efficiency day to day in addition to adding security controls.

TABLE 5-1 Win-Win Benefits for IT Operations

Benefit	Description
Increased efficiency	Administrators save time through single sign-on, automated password resets, and production of audit reports.
Streamlined workflow	Approving or reviewing privileged actions can become more reliable and predictable if automated security controls are well-integrated into IT Operations processes.
Fewer user errors	Every IT department has incidents of a user or administrator accidentally mistyping something wrong that creates an undesirable outcome or brings down a system. Controls can be configured to force review and confirmation when certain commands are used to prevent damaging accidents.
Reduced calls to the help desk	Removing local admin rights on workstations and only allowing approved applications to be installed reduces calls to the help desk due to end-user error.
Greater velocity for DevOps teams	Providing developers and DevOps teams with a self-service approach to secure secrets makes these teams more productive

Understand use case

Understand what your current and future use cases for a platform would be. Based on your inventory and assessment of privileged accounts, credentials, and secrets, determine what features and use cases are desired or required.

REMEMBER

Keep in mind future requirements, taking into account how your company's technology strategy is evolving. Are more workloads moving the cloud? Is there an initiative underway to adopt DevOps practices?

Assess platform feature capabilities

Evaluate capabilities of available platform options and providers. As part of the selection process, identify a set of capabilities that are desired or required to be mapped to your use cases. Some examples of these include

- **Credential management:** Flexible and configurable credential vaulting and rotation for passwords, credentials, and secrets used by human users and applications for on-premises and cloud workloads

- **Session isolation:** Isolated access to critical assets with transparent connections to target systems to prevent credential exposure, including securing remote user access
- **Audit and monitoring:** Strong support for audit and monitoring and anomaly detection of suspicious privileged access activities to prevent and detect attacks
- **Tool integration:** Out-of-the-box integrations available for a broad range of IT and security operations tools
- **Privileged task automation:** The ability to automate routine privileged access tasks, including the discovery and onboarding of privileged accounts and credentials
- **Least privilege management:** Support for JIT capabilities to minimize standing access and unnecessary permissions
- **DevOps management:** Comprehensive credential management of all sensitive elements in the DevOps process

  Research whether your short list of providers meets your security and availability requirements. Looking at these requirements is just as important as the feature capabilities of your PAM provider.

Assess platform security and availability

Along with platform features, you should also look at the security and availability capabilities of your PAM as a Service provider:

- **Security:** Storing the accounts, credentials, and secrets to your highest risk assets requires a service that was built with security in mind. This includes
  - Hosting in premier Tier IV data center facilities that are highly secure, fully redundant, and certified for SOC-2 and ISO 27001 compliance

    
    TIP

    Validate that your PAM as a Service provider has achieved SO2-2 certification and isn't relying only on the certifications provided by their cloud provider.
  - Hierarchical encryption of data at rest to protect privileged account credentials, policies, and audit information

    
    TIP

    Look for solutions that are FIPS 140-2-compliant to protect your data.
  - Session encryption for data in transit

- Hardening of all on-premises solution components to reduce attack surfaces
- Support for multi-factor authentication and policy-based access controls to protect against unauthorized access

» **Availability:** Your PAM as a Service solution is mission critical for your organization, so uptime is extremely important. Investigate these areas:

- **SLA guarantees:** Here, it's important to understand the SLA provided by your PAM as a Service vendor and not just the SLA from the cloud provider it's using. Make sure to find out what remediation is in place if the SLA isn't met.
- **Redundancy:** The solution should be deployed in multiple availability zones for maximum redundancy.

IN THIS CHAPTER

- Securing privileged human credentials
- Securing non-human privileged access
- Implementing least privilege
- Detecting and preventing anomalous privileged behavior
- Securing your PAM as a Service solution
- Investing in periodic red team exercises

Chapter 6
Six Actions for Success in PAM as a Service

You won't be hearing any voices from attackers in this chapter. This chapter is all about *you* and getting to action in reducing critical risks for your company by building your Privileged Access Management (PAM) as a Service program.

This chapter gives you critical actions for reducing privileged access risk. Together, these six actions help you establish essential privileged access management controls to strengthen your security posture. Implementing a program that leverages these actions can help your organization achieve greater risk reduction in less time and help satisfy security and regulatory objectives with fewer internal resources.


TIP

Your efforts should be iterative and use quick sprints to logically take on the highest priority items quickly and effectively. Some companies use a 30-day sprint methodology to accelerate the pace to implement critical controls in a short period of time. The best sprint time for you may vary depending on your company and culture. The most important thing is prioritization of each sprint to ensure the most value and minimize scope creep.

Secure Privileged Human Credentials

Privileged access can be just as powerful whether it's a human or a machine using an admin account. I personally like to start with human credentials because they instill immediate value and education for developers, admins, and power users that hold these important accounts; plus, it's easier for humans to envision human use. It is easy to "find" human credentials, because they all tie to a person.


TIP

Think through how you can inventory or discover privileged credentials used by human users. If your company has an IT system inventory and critical system list, I like to start there to determine priorities. From there, you have to determine how best to work across system owners to help them inventory the privileged accounts and work them into your team's PAM as a Service onboarding processes.

Secure Non-Human Privileged Access by Applications and Other Entities

Non-human privileged access can be a bit more opaque to discovering and identifying than human accounts. They can live in code, objects, APIs, and more, so finding them can be a bit more challenging. Luckily, scanning tools exist to help surface these types of credentials. That said, I recommend a two-pronged approach:

- Rely on the expertise of individuals that know the systems and assets best.
- Leverage automated scans and continuous discovery tools.

These approaches maximize your success for reining in non-human privileged access, identifying which ones are under current eyes of human users, and reducing risk.


REMEMBER

Whether human or non-human, a magical "easy button" doesn't exist that you can push to automatically find, control, and manage privileged access. Use all the tools, people, and processes that you can to your advantage. You can't protect what you don't know about.

Implement Least Privilege

Least privilege is an important concept to consider (or even reconsider) when implementing a PAM as a Service program. Least privilege really pertains to the philosophy and actions to prevent human and machine identities from having more access to systems and resources than they should.

In your PAM as a Service program, you're changing the way that privileged access is managed. Why would this not be the perfect time to reduce unnecessary privileges?

TIP

To achieve least privilege through your program, consider the following three tactics:

- **Educate and influence** stakeholders and customers to adopt the least privilege concept and understand the importance of taking action to achieve it. This includes looking at approaches that implement just-in-time access and reduce standing privileged access.
- **Define least privilege assessment/change process** so changes can be considered during the move to your new tools and processes. Consider gamifying the process to give points for finding opportunities to improve.
- **Set up a review cadence** to make sure the philosophy and action aren't only a one-time exercise but also continue to live over time. Reviewing for least privilege can also be integrated into privileged account access reviews. For example, on endpoints, this process could translate into periodic inspection of how many workstations have local admin rights removed. For cloud workloads, this review entails ongoing review of permissions granted to human and machine identities to enforce least privilege concepts.

Detect and Prevent Anomalous Privileged Behavior

If you've read this far in the book, you likely know and are on board with protecting privileged access. Beyond "locking down" the access and the way that employees utilize their privileged

access, monitoring and detecting anomalies can greatly reduce risk and take action when need be. You may not be able to stop every bad thing from happening, but if you can detect and respond to an incident, you may be able to limit and contain the impact and damage caused.

TIP

Some things to think about from a detection standpoint are

- Establishing a baseline for what "normal" user behavior looks like and monitoring for abnormal privileged user behaviors in comparison
- Monitoring credential theft from known credential repositories (dark web)
- Sending your analytics data from your PAM as a Service solution to your security operation center (SOC) team and integrating with your User and Entity Behavior Analytics (UEBA) solution — which is a type of tool specifically designed to determine anomalous behaviors

Secure Your PAM as a Service Solution

The security of your PAM as a Service solution is critical due to the various important accounts, credentials, and keys that it protects. You want to avoid your PAM security tools either being misconfigured, partially deployed, or using manual processes that could expose sensitive passwords and credentials. This is what you are trying to *avoid* with your program to begin with.

TIP

The controls you put around your PAM as a Service solution should be holistic and cover people, processes, and technology:

- **People**
  - **Awareness:** People can't use or secure what they don't know about. Getting the PAM as a Service mission, goals, and processes communicated to the workforce is a critical first step to making sure the security enhancements of your PAM processes are maximized.
  - **Training:** Make sure people — users, stakeholders, support staff, architects — know their roles, responsibilities, and how to properly use the solution and protect the actions that they're responsible for; don't overwhelm them.

- **Processes**
  - **Customer interactions:** The "customers" of your PAM service are important, and how they interact with the service team is critical from a security standpoint. Ensuring that these interaction processes are defined and built from a security-minded standpoint is important to make sure a human misstep in attempting to do the right thing doesn't void all the hard work of the PAM service team.
  - **Monitoring:** Some of the PAM solutions provide monitoring and detection tools that look for suspicious behaviors or actions. Build processes around these features so they're leveraged and acted on in a timely manner.
- **Technology**
  - **Secure configurations and implementations:** Many tools, whether they're deployed in the cloud or within your company premises, are securely built. However, depending on the way they're configured, they may leave "holes" open that could be abused. Partnering with your PAM as a Service vendor and tech staff to securely configure and maintain the configurations and settings over time shouldn't be an afterthought.
  - **Multi-factor authentication (MFA):** MFA is a key control for protecting your PAM as a Service environment. This includes MFA when you access your PAM as a Service solution via the console.

Invest in Periodic Red Team Exercises to Test Defenses

Red teaming is the practice of rigorously challenging plans, policies, systems, and assumptions by adopting an adversarial approach in testing your network. Essentially, the red team gets to play the bad guy and use many of the same tactics.

Red teams can be incredibly helpful to ensure your privileged access is as controlled as you hope it is. Similar to the bad actors, a red team member's top goal is to obtain privileged access and then move laterally into other systems. This process is a *great* way to find gaps, and you may also find some privileged accounts and/or credentials that haven't been onboarded into your PAM service.

Deploy PAM as a Service

In today's digital world, the key to most companies' crown jewels is through privileged access. Privileged accounts, credentials, and secrets are everywhere — on-premises, in the cloud, and in DevOps environments, as well as on endpoints. Most security breaches of sensitive data from customer records to intellectual property involve the use of stolen privileged credentials. This book educates you on how to leverage Privilege Access Management (PAM) as a Service to reduce risk from attackers and malicious insiders.

Inside...

- Types of privileged access
- The risks of unsecured privileged access
- How to secure privileged access: on-premises, cloud, and DevOps
- The privileged attack life cycle
- Reducing privileged access security risk

Aaron Pritz is an IT and security leader with 20+ years of experience in life sciences. He's a creative strategist that brings strategy to life through successful execution in security and privacy. He's the CEO and cofounder of Reveal Risk and enjoys speaking and writing on cyber industry topics.

ISBN: 978-1-119-72157-4
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.