

LEARNING MADE EASY

CyberArk Special Edition

Privileged Access Security

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



Aaron Pritz

About CyberArk

CyberArk is the #1 leader in privileged access security, 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 the industry's most complete solution to reduce risk created by privileged credentials and secrets. The company is trusted by the world's leading organizations, including more than 50 percent of the Fortune 100, to protect against external attackers and malicious insiders.

To learn more about CyberArk, visit www.cyberark.com.



Privileged Access Security

CyberArk Special Edition

by Aaron Pritz

**for
dummies**[®]
A Wiley Brand

Privileged Access Security For Dummies®, CyberArk Special Edition

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

Copyright © 2018 by John Wiley & Sons, Inc.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

Trademarks: Wiley, For Dummies, the Dummies Man logo, The Dummies Way, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. CyberArk and the CyberArk logo are registered trademarks of CyberArk. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc., is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN: 978-1-119-51538-8 (pbk); ISBN: 978-1-119-51544-9 (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 A. Burchfield

Acquisitions Editor: Steve Hayes

Editorial Manager: Rev Mengle

Business Development

Representative: Sue Blessing

Production Editor:

Mohammed Zafar Ali

Table of Contents

INTRODUCTION	1
About This Book	1
Icons Used in This Book.....	2
Beyond the Book.....	2
CHAPTER 1: Defining Privileged Access	3
Types of Privileged Access.....	4
Privileged access used by humans	5
Non-human privileged access	6
Is It a Privilege to Have Privileged Access?	7
Insider and External Risks Associated with Privileged Access	8
Why are the risks so high?	8
Where does privileged access exist?	9
Securing Privileged Access through High-Level Methods	10
People.....	11
Process.....	11
Technology.....	12
CHAPTER 2: Looking at the Risks of Unsecured Privileged Access	13
Defining Different Types of Data Loss	14
Personal information (PI).....	14
Intellectual property	15
Confidential information.....	16
Compliance Failures Related to Regulations, Laws, or Internal Standards.....	16
GDPR.....	16
HIPAA.....	16
HITECH	16
SOX	17
PCI.....	17
MAS TRM	17
SWIFT	17
Addressing Audit Findings.....	18
Third-Party Impacts and Risks	19

	Defining Attacker Compromise	19
	Data theft (confidentiality)	20
	Data corruption/manipulation (integrity)	20
	Ransomware (availability)	21
	Illicit crypto-currency mining	21
CHAPTER 3:	Securing Privileged Access for On-Premises Assets	23
	COTS Software, including IT and Security Applications	24
	Servers	25
	Databases	26
	Network Devices	26
	Endpoints	27
	IoT Devices	27
	Industrial Control Systems	28
CHAPTER 4:	Securing Dynamic Applications and Cloud-Based Infrastructure	29
	Understanding Cloud Options	30
	Securing the Management Console	32
	Securing API Access Keys	33
	Protecting Cloud Infrastructure	34
	Securing SaaS Applications	34
	Securing the DevOps Pipeline Tools and Processes	35
	Protecting Application Code Built with the DevOps Pipeline	36
CHAPTER 5:	Getting Started with a Privileged Access Security Project	39
	Understanding the Attack Life Cycle	40
	Taking Critical Steps to Action	41
	Assess your on-premises and cloud infrastructure and applications	41
	Classify types of privileged access by risk	42
	Evaluate existing process effectiveness	43
	Prioritize actions and where to start	43
	Find the right mix of controls	43
	Establish the right partnerships	44
	Select a privileged access security platform	45

CHAPTER 6: Ten Actions for Securing Privileged Access 47

- Eliminate Irreversible Network Takeover Attacks 48
- Control and Secure Infrastructure Accounts 49
- Limit Lateral Movement 49
- Protect Credentials for Third-Party Applications..... 50
- Manage *NIX SSH Keys..... 50
- Defend DevOps Secrets in the Cloud and On-Premises 51
- Secure SaaS Admins and Privileged Business Users 51
- Invest in Periodic Red Team Exercises to Test Defenses..... 52
- Invest in a Tool to Periodically Measure Reduction in Privileged Security Risk..... 52
- Utilize MFA..... 53

Introduction

Theft, disruption, and compromise throughout history has 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.

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.

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.



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.



TIP

Tips are the recommendations for how much you should PayPal the author and editor! 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.

Beyond the Book

It's my hope that this book gives you a better understanding of privileged access security, which helps you secure accounts, credentials, and secrets, 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 privileged security program.

IN THIS CHAPTER

- » Learning about the types of privileged access
- » Knowing if it's a privilege to have privileged access
- » Looking at internal and external risks
- » Securing privileged access through high-level methods

Chapter 1

Defining Privileged Access

My name is Billy. I have been a “freelance hacker” for 14 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’ computing mistakes.

These days, I don’t have to use most of my sophisticated hacking skills. Phishing people 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 computer access to a company ends up in one of my “nets.” My best days are when I get database admins, company network admins, infrastructure support personnel, or the accounts of company executives.

Well, it’s nice chatting with you, and I hope not too many people read this book because the less you know about privileged access, the more money that flows into my pockets. Keep doing everything just like you have been doing it. It. Is. Perfect.

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 to avoid folks like Billy.

Types of Privileged Access

Privileged accounts, credentials, and secrets are needed for an administrator, application, or device to access a system (such as applications, servers, switches, firewalls, routers) whether located in your on-premises data center or in the cloud. *Privilege* is a term used to designate special access or abilities, above and beyond that of a standard user.

If you aren't personally an "administrator" at work, think about how 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 have shared your password, which is another all-too-common story).

You will 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. Figure 1-1 shows you some examples of each. In this section, I also break down each category a bit further with examples.

Human Privileged Access	Non-Human Privileged Access
Domain Admin	Application Accounts
Local Admin	Service Accounts
Server Admin	API Keys/Access Tokens
SSH Keys	SSH Keys
Network Admin	Other Hard-Coded Application Secrets
Database Admin	Certificates
Application Admin	
Cloud Admin Console	
DevOps Admin Console	
SaaS Admin Console	
Emergency Account	
Privileged Business User	

FIGURE 1-1: Common types of privileged access.

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 include the following:

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

Example: Jim, the accounting application administrator, logs in with his super user account for a popular Customer Relationship Management (CRM) application to add and remove users who are starting in or exiting from the accounting department. He also makes system level configuration changes as requested by the head of accounting. Other examples of super user type accounts include the accounts used by server admins, network administrators, and database or application admins. Admin consoles for cloud-based infrastructure and applications and DevOps tools are highly privileged as well.

- » **Domain administrative account:** These accounts provide privileged administrative access across all workstations and servers within a network domain. 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 any organization.

Example: A common type of privileged administrative account that an attacker targets is a Windows domain controller account. If a hacker obtains this, he typically can access many servers and corresponding data on each server.

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

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) keys:** SSH keys are one of the heavily used access control protocols in the enterprise that provides direct root access to critical 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.

Example: An 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: An emergency account could be a specific application administrative account for a third-party software package that's installed on local servers 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 has access to sensitive systems. This could include someone who needs access to finance, human resources (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

The next type of privileged access is used by non-human automated processes. These automated processes are sometimes 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.

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 account:** This is a special account that an application or service uses to interact with the operating system. Services use these accounts to access and make changes to the operating system or the configuration.

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.

- » **SSH keys:** SSH keys are also used by automated processes.

Example: SSH keys are used in dynamic cloud environments that auto-scale infrastructure.

- » **Secrets:** The term *secrets* is most frequently used by 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 team may have secrets embedded in the software they're developing.

Is It a Privilege to Have Privileged Access?

Having privileged access may seem like an honor, but after hearing about the risks and threats, it may seem a little daunting. In this era of cybersecurity risk, the responsibility and exposure to compromise makes privileged access more of a liability if it's not managed safely.

Think about what attackers or malicious insiders may want to do with privileged access. They can

- » Change firewall rules so your network can be penetrated (or data can be extracted).
- » Access your infrastructure in the cloud to steal data or use your infrastructure without your permission.
- » Steal your customer list or very sensitive files/data or encrypt the data via ransomware.

The easiest way to attain all of this is for attackers or malicious insiders to get their hands on unprotected, unmonitored privileged credentials. If you want to attack or steal from a company, why would you want to use harder methods when it's this easy?

If a company wants to defend against these risks, why not start by better securing these super risky accounts, credentials, and secrets? The “privilege” isn't actually having the credentials; it's the duty of protecting them.

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. Damages often include

- » Theft (from people inside the company or external)
- » Disruption in business continuity
- » Data corruption or loss

Examples of the bad things that can happen with privileged access include

- » 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)
- » Capturing user activity (such as keystrokes: everything they communicate electronically)
- » 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. It is estimated that privileged accounts in a company typically are three to four times more than the number of employees. Examples of privileged access include the following:

- » Data centers, applications, servers, network devices, and other infrastructure
- » Cloud (more on that in Chapter 5)
- » Endpoints (iPhones, laptops, tablets, and so on)
- » Internet of Things (connected devices such as video cameras 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 people in their basements, but another big source of attacks come from within an organization.

External threat actors

External threat actors typically are referred to as *attackers*. However, “attackers” is a very broad term. There are adolescents hacking from their parents’ basement and well-funded cyber-criminals with full office building complexes. The latter is often funded by nation states (countries with a vested interest) or criminal organizations. Regardless of the scale of the external threat actor, the best day for these people is when they find uncontrolled/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:

» **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 workforce member can be an inadvertent risk. The easiest example is someone who clicks on a phishing email link or opens a malware infected file. In doing so, accounts (including any privileged accounts this person may have) become compromised.

» **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. The reasons themselves don’t really matter, but they can include being laid off, not getting a raise, being put on performance-related discipline, or being enticed by an outside party to sell company or personal information.



REMEMBER

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, not sharing passwords, following processes with guarding privileged accounts, and so on.
- » **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:

- » **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.
- » **Example:** Define the standard for changing admin passwords periodically or after use. Where do these passwords get stored? In an access controlled spreadsheet? In a secure password vault?

Technology

Technology in privileged access security has rapidly evolved in the last several years. Simple secure password vaults have evolved and can now provide a portal for system administrators to securely log into and be connected to a system they administer without ever knowing the privileged account password. These tools can also change the password to that privileged account automatically after every use. These tools take the protection of privileged access to the next level. However, without the right people engagement and process, such tools aren't fully effective.

Examples of privileged access security system capabilities include the following:

- » Storing privileged passwords, credentials, and secrets and rotating them based on policy (for example, rotate immediately after use or based on time parameters)
- » Granting privileges to privileged users only for systems on which they're authorized
- » Granting access only when it's needed and revoking access when the need ends
- » Avoiding the need for privileged users to have or need local/direct system passwords
- » Creating an unalterable audit trail for any privileged operation
- » Detecting and preventing attacks involving privileged access

IN THIS CHAPTER

- » Understanding the types of data loss that can occur
- » Looking at compliance failures 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 the Leak. 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 called “passwords.” It was the first thing I searched for.

I hope that my next company doesn't have this issue fixed. I could make a business out of just searching for passwords, gathering docs, and then taking this data to my next employer along with another big promotion! Enough sharing. I've got to get back to my document harvesting project. Liam — out.

Is it possible that someone like Liam exists within your company? If so, 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 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 in companies.

Personal information (PI)

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 (also commonly referred to as *personally identifiable information*, or PII) 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)
- » National Identification Numbers

- » Customer home addresses
- » Employee or contractor emergency contact info

In many countries, there is also 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:** These are a common target of identity thieves and fraudsters. Your credit card number has financial value because it's used by cybercriminals to make fraudulent purchases.
- » **Personal health information (PHI):** This type of info can be sold by the record on the black market within the dark/deep web (a layer of the Internet that's sometimes used for illegal actions). The dark web can be used for nefarious transactions to avoid broader detection. Additionally, health records are reported to yield a higher value for black market sales than credit card numbers.

Both types of data have a certain value to your company and must be protected. 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 privileged access to the information that's classified as most sensitive is a good place to start a privileged access security program.

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 product patent applications, product research, and innovative manufacturing methodology.

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.

Compliance Failures Related to Regulations, Laws, or Internal Standards

Protecting the data and information itself should be the primary driver for action. However, there are many current and emerging regulations, laws, industry frameworks, and internal company standards that require proper handling of privileged access. In this section, you discover some examples of regulations, laws, and internal standards that require securing privileged access.

GDPR

The Global Data Protection Regulation (GDPR) is a new 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 is focused on protecting the data and privacy of EU citizens and has been in the works for several years, and enforcement comes with significant fines: €20, which is approximately \$24.8 million at the current exchange rate, or 4 percent of the company's worldwide annual revenue of the prior financial year, whichever is higher.

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.

HITECH

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 is legislation that was created to stimulate the adoption of electronic health records (EHR) and the supporting technology in the United States. The HITECH Act

requires business associates to comply with the HIPAA Security Rule with regard to electronic protected health information (ePHI) and to report PHI breaches.

SOX

The Sarbanes-Oxley Act of 2002 (SOX) is a United States federal law that set new or expanded requirements for all U.S. 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.

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.

MAS TRM

The Monetary Authority of Singapore (MAS) Technology Risk Management (TRM) Guidelines provide banks and financial institutions (FIs) with a risk management framework for Internet banking. In the expanded guidelines (2013), there are several requirements related to privileged access security.

SWIFT

The Society of Worldwide Interbank Financial Telecommunication (SWIFT) network provides a global community of financial institutions (over 11,000 customers scattered across 200+ countries) the ability to exchange sensitive information relating to international financial transactions. SWIFT has specific requirements on privileged access control and monitoring.



WARNING

Each organization was required to self-attest to prove SWIFT compliance by January 1, 2018, and then annually thereafter. Failure to comply can result in being reported to the local supervisory authority as well as an organization's non-compliance status being viewable to all other users and counterparties within the SWIFT network.

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 actual terminations. 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 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 can be seen from a recent large U.S. 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 is good because it allows for a company to be more flexible as its business ebbs and flows.

However, managing third-party information security risk and specifically privileged access risks is not without challenges. There are several notable breaches that brought third-party risk front and center within corporations. One is an HVAC company that was a third-party supplier to a large U.S. retailer. It is believed that the attacker leveraged the privileged accounts of an HVAC supplier to pivot and ultimately steal data from the Point of Sale (POS) system. (The POS system included the actual cash registers and the supporting database that housed customer and credit card data.)

Third-party risk management is typically a difficult risk to manage because a company can audit or assess a third party and do some limited vulnerability scanning, but this only provides a snapshot in time of the third party's risk and its ability to sustainably manage controls to reduce risks.



TIP

A recommended best practice is to isolate third parties from direct access to corporate networks and systems to reduce risk. This can be done by using a jump server, which is a specialized server that a third party must connect to before accessing an organization's systems. This process prevents malware from a remote vendor's endpoint from infecting the network. Also, with this approach, credentials are never disclosed and third-party access can be monitored and recorded.

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. Some countries have been accused of sponsoring hacking groups for various political, social, economic, or financial motivations.

Attackers often find ways to use one form of access to lead to another more elevated form of access. This practice is called *pivoting*. 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.



REMEMBER

Regardless of how the attacker gains privileged access, the need, method, and impact of protecting are all the same.

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.

Typically, when privileged access is used to obtain these types of information, the data is encrypted (to avoid detection) and sent outside of the company to an untraceable server and location.

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.



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.

Illicit crypto-currency mining

Crypto-currency mining is a legitimate activity. However, a growing community of individuals and organizations try to mine for crypto-currency using illicit (or illegal) methods. These individuals and groups use malware/viruses to break in and harness the power of other people's/organizations' computers and servers. This is all done without the user or organization even being aware. Given that compromised privileged accounts, credentials, and secrets play a role in gaining maximum access to a computer or network, it typically is a key component in conducting illicit crypto-currency mining.

- » Looking at Commercial Off-The-Shelf (COTS) applications
- » Managing databases, servers, 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 at this for about ten years, but my job has become a lot easier in recent years. I used to spend a lot of time hacking into company's networks to steal and sell data like credit cards. However, these days I'm making more money by crafting my killer logic into an actual hacking platform with features that I sell to other less talented people. I can make more money and have less personal risk because I'm not the one taking actions against companies. Now, I get to sit back and watch my work spread through the world. I'm a CEO . . . or maybe CHO (Chief Hacking Officer).

I've spent a lot of time building a high-quality product and actually 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 new business don’t scare you out of your pants, you may just be in a coma. Privileged accounts and credentials are often referred to as “the keys to the kingdom.” They can be infrastructure and applications that run on-premises or in the cloud and can be managed by the IT team, business users outside of IT, or DevOps teams. They’re required to unlock access to systems with sensitive data, and they’re sought out by external attackers and malicious insiders as a way to gain direct access to an enterprise’s most valuable information. 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 commercially available 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. In Chapter 1, I cover the various types of privileged accounts and credentials, and many of these exist in COTS packages.



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). The attacker essentially attempts to log in with this default password found in product install manuals available on the Internet. Bad actors can typically be successful if that initial password hasn’t been changed or secured. This sounds so simple, but sometimes easy tasks such as this are overlooked. It’s an embarrassing

situations if such a breach turns into a public story because it tends to show carelessness of your IT operations.

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. Protecting these credentials is as important as human managed accounts.
- » Credentials are stored in COTS applications' configuration files or databases. This represents a significant security vulnerability because attackers or malicious insiders can easily gain access to these application credentials.
- » Credentials often remain unchanged because of the administrative burden required to rotate them periodically or because it requires application downtime. Additionally, if privileged passwords and SSH keys are added manually into applications but not changed frequently, they may be known to a broad set of people, and records of those unchanged credentials could be found in unsecure spots.

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 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.

Today's servers are often 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.



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 is often 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 system, 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, mobile devices (such as smartphones, tablets, smart watches), or other Internet connected devices. Many common business tasks, such as installing software, require privileged access. Some companies, by default, give employees admin 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 that aims to obtain admin access, and run a program called MimiKatz (which is a Windows script that can be run remotely) that essentially exports all the passwords that are stored in memory on that laptop. This can enable the attacker to then pivot to other exposed systems quite easily.

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.

Think about this: Literally during the authoring of this chapter, another hacker got into a major casino by logging into a connected casino fish tank water temperature thermometer and then pivoting into the casino network. What are the chances? Well, quite good, I guess, because everything is becoming connected. If you can connect it, someone can hack it.

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 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 safety, product quality, 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 cloud options
- » Securing the management console
- » Securing API access keys
- » Protecting cloud infrastructure
- » Securing SaaS applications
- » Securing the DevOps pipeline tools and processes
- » Protecting application code built with the DevOps pipeline

Chapter 4

Securing Dynamic Applications and Cloud-Based Infrastructure

Fernando Cirrus here. I recently left one of the major main-stream 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 and applications are making some simple mistakes that make my new start-up successful.

My company is focused on providing data exfiltration (extracting data for theft) for the highest bidders. I have a network of cloud knowledgeable operators that are able to prey on the mistakes of others to locate and exfiltrate the data we are requested to target, 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 managing cloud vendors, DevOps, and their security operations that they aren't all adopting these processes and tools like they should. This is fine with me though! Nothing to see here. Keep doing what you're doing, and my job will continue to be incredibly easy.

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 and DevOps assets, read this chapter to discover more about the specific areas of risk to focus on.

Understanding Cloud Options

Increasingly, companies are aggressively taking advantage of the benefits of running their applications in the cloud by transitioning from their traditional on-premises infrastructure and data centers to cloud-based infrastructure. The key difference is moving from running their applications on their own servers and equipment to running their applications on a dynamically available shared infrastructure. Some newer organizations are cloud native and only run cloud-based 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. However, each public cloud vendor's offering is different, and sometimes it can be difficult for organizations to switch between vendors or adopt multi-cloud approaches.
- » **Private cloud:** The computing infrastructure is dedicated to a particular organization and isn't shared with others but has some of the same self-service and dynamic capabilities of the public cloud.
- » **Community cloud:** This involves sharing computing infrastructure between organizations of the same community and may be offered as a public cloud by a third party

(for example, a cloud environment specifically set up to offer cloud computing resources across a nation's government agencies).

- » **Multi-cloud:** The organization uses several different clouds, including multiple public cloud vendors. This approach is becoming increasingly popular with organizations as they seek to manage costs and avoid getting locked into a specific public cloud vendor.
- » **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. Hybrid clouds may take advantage of *cloud bursting*, which is when an organization primarily uses its own infrastructure but accesses cloud services for high/peak load requirements.



Hybrid environments, which are the norm, are often quite challenging because organizations need to secure both the on-premises and cloud environments. Also, as organizations are increasingly looking to gain operational flexibility by using multiple public cloud providers, any approaches for securing privileged access to cloud workloads should address multi-cloud environments.

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.
- » **Software as a Service (SaaS):** Companies are also increasingly purchasing applications, such as accounting, Human Resources, and sales management as a service. These

applications are purchased by the user, seat, or other usage metric. 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.

The business benefits of moving to the cloud are real, but as more business-critical applications and services migrate to the cloud, ensuring the security of these cloud workloads, processes, and services becomes essential. In addition, as enterprise computing environments become more disparate, there's a strong need to maintain and enforce enterprise-wide privileged access security policies in a consistent and sustainable way.



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 applications, data, and access to external resources and other assets. Similarly, organizations leveraging SaaS need to secure and monitor access to these applications as well.



WARNING

For example, the public cloud provider can ensure that private data can only be accessed with specific keys, but it's the organization's responsibility to ensure the data is configured as private (not public), and the keys are only shared with authorized users. This unfortunately is a lot more difficult in practice than it may sound, and has led to many instances where private data has been inadvertently exposed.

Securing the Management Console

The management console 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 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 monitor any and all potential access paths to the management console.

A root account is created when an organization initially sets up the cloud environment or account with the cloud provider (similar to the main installation account for systems deployed on-premises). Root accounts enable the *most* powerful access to the management console and are used, for example, to grant privileged access to the individual administrators. While the root account should be used infrequently, it still needs to be protected because essentially whoever controls the root account controls the organization's cloud environment.

Securing API Access Keys

Application Program Interface (API) access keys are widely used to allow applications to “talk” (send and receive) requests to other applications and functions in the cloud environment. 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. Having the right process and technology to protect these keys is critical. After an attacker has the API access keys, the attacker could gain unrestricted access to the entire cloud environment.

Protecting Cloud Infrastructure

Cloud-based infrastructure enables new virtual servers, containers, storage, and other resources to be provisioned dynamically as needed. In simple terms, if a restaurant chain's pizza ordering application that uses cloud-based infrastructure needs X number of virtual servers to run on a regular weeknight, and then with the "big game" on TV, orders spike dramatically, new virtual servers can be provisioned and automatically released as needed.

When each virtual server is initiated and launched, it will be assigned privileged credentials that must be secured. In the pizza example, it would include credentials to process credit card payments and to access the customer database and other resources. In more static environments, administrators may use the management console to spin up and assign a new server — whereas in dynamic environments, automation, scripts, and provisioning tools would be used to automatically establish new virtual machines, containers, and infrastructure.

Consequently, credentials can be created at a rapid rate as organizations spin up infrastructure to be used for just a few minutes or hours to complete a specific task. This can happen multiple times a day, which is why it's critical to leverage automation to secure these privileged credentials.

Securing 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 the corporate 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. SaaS applications are routinely used by people who aren't IT professionals and don't necessarily follow typical security protocols, which creates the following vulnerabilities:

- » Passwords that are simple and guessable
- » Passwords that are left unchanged for long periods of time
- » Credentials that are shared by multiple users, making it difficult to determine who did what
- » No audit trail of users with privileged access — consequently, you can't look back and determine what was done, when it was done, or who made the change
- » Access that isn't systematically removed from individuals — giving individuals privileged access that's no longer required or authorized

Securing the DevOps Pipeline Tools and Processes

The DevOps or Continuous Integration and Delivery (CI/CD) pipeline helps organizations increase business agility by reducing time to deployment and bringing new applications and services into production faster. The CI/CD pipeline uses powerful automated tools to enable services to be automatically built and deployed.



WARNING

Ensuring the security and integrity of the tools and the interactions between the tools is a big concern because the DevOps pipeline enables applications to be updated and deployed at an incredibly rapid pace — potentially dozens or more times per day.

Just like with any admin console, the admin consoles for the tools are protected with credentials and passwords. But, additionally, because these tools are designed to automate the CI/CD pipeline, they run code to have other tools build, test, and configure

infrastructure and applications before going into production. Each of the interactions between the tools requires credentials that also need to be protected.



WARNING

A key challenge is that the workflow for controlling access to the secrets and privileged user accounts linked to these tools can also vary greatly. Unfortunately, this often leads to inconsistent, and even manual, strategies for controlling access to critical DevOps tools — which opens organizations up to vulnerabilities.

Frequently, it's automated processes, rather than human users, accessing tools. Regardless, organizations must secure all DevOps tools and it is critical to remove hardcoded credentials from code. It's also important to know what tools are used — by whom and where the automation is employed and to change credentials as needed. Companies must have a consistent and comprehensive approach to securing secrets used by DevOps tools.

Protecting Application Code Built with the DevOps Pipeline

Securing DevOps tools alone isn't enough to protect the full scope of the pipeline. The other critical area that must be secured is the application code that “flows” through the pipeline and is ultimately deployed by business operations. Applications built using DevOps methodologies typically rely on a large numbers of app credentials and access keys to enable applications to run and access databases and other resources.

Applications are based on code, and the consequences can be serious when code inadvertently includes hardcoded passwords, access keys, and other credentials. For example, it's particularly dangerous when access keys for an application are hardcoded in source code and then inadvertently placed into a public code repository.



WARNING

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

- » They're nearly impossible to rotate, making credentials an easy static target for attackers.

- »» They're usage is difficult to track because many scripts, automation tools, applications, and humans have access to them.
- »» They're 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.

- » Understanding the attack life cycle
- » Following the steps to project action

Chapter 5

Getting Started with a Privileged Access Security Project

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 myself 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 is automation to monitor for anomalous privileged activity and admin passwords can be changed automatically once they log out of a system. Automated monitoring is a nightmare for people like me. 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. 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 become on how to defend against attacks and get your company to action reducing privileged access security risks.

Understanding the Attack Life Cycle

A recently published Ponemon study revealed that 63 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. Industry reports from a recent CyberArk blog note that on average it takes 146 to 170 days to detect an attack, 39 days to contain it (keep it from spreading further), and 43 days to remediate (fully resolve the issue). Time seems to be on the side of the attackers.

Motivated attackers will find a way into your company (often by leveraging phishing attacks), 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.

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.

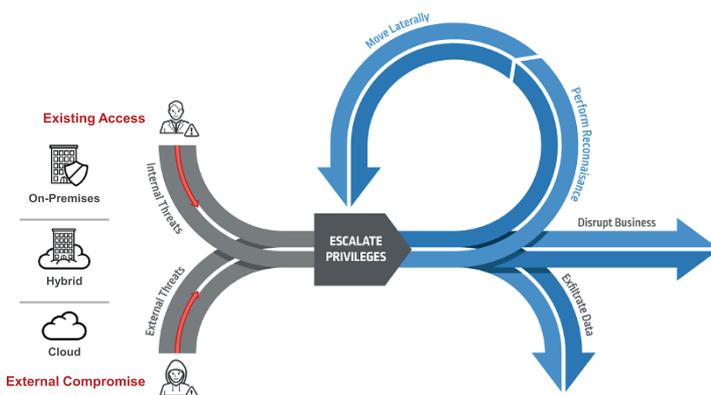


FIGURE 5-1: The attack life cycle.

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 to the most interesting things they want to take or exploit. This continues until they exfiltrate data of interest or they find a way to disrupt a system or service, or embarrass the company. In some cases, the attacker might be looking to operate in stealth mode and use the company's infrastructure illicitly for crypto-mining.

Taking Critical Steps to Action

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

- » **What should we do and when?** (You can't do it all!)
- » **What's the best mix of controls?** (Prevent and detect.)
- » **How much is enough?** (Find the balance between "sufficiently secure" and "overly restrictive.")

The seven sections here provide more detail to address these three key strategic questions.

Assess your on-premises and cloud infrastructure and applications

Knowing your scope of exposure through usage of privileged accounts, credentials, and secrets may seem like a daunting initial task. Depending on how many IT assets (systems, databases, applications, SaaS, cloud providers, DevOps tools, and so on) you have, there could be tens, hundreds, thousands, or hundreds of thousands of privileged credentials alone.

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 approach. This may entail identifying a small set of privileged accounts to secure first before expanding their ambitions toward more comprehensive coverage.



REMEMBER

Regardless of approach, it will still be important to continuously determine progress, priorities, and opportunities to secure privileged access. 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 systems (if you have a system classification process or a list of critical systems)
- » 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 will be important as you develop the go-forward process to secure privileged credentials.

Prioritize actions and where to start

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

- » Launch a process improvement initiative.
- » Time your project as part of, or immediately following, a major project, system launch, or infrastructure refresh (such as implementing as part of a cloud migration project, which many companies are going through now).
- » Secure privileged access as new applications are introduced or when existing applications are updated to newer versions.
- » 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.
- » 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.

Find the right mix of controls

Like many IT security risk reduction efforts, a number of different types of controls can be put in place to reduce risk. Intuitively, preventing something altogether sounds like the best control. However, that's not 100 percent possible, but detective and monitoring controls can at least allow you to catch and stop the bad things from happening.



TIP

Detective controls can often help in getting the balance right between enabling and restricting access. Rather than putting a preventative control in that could be overly restrictive, in some cases, a better approach would be less restrictive access that's carefully monitored. Detective controls can alert staff if something

is happening out of the ordinary. For example, someone logging in at a strange time is a potential but not definitive signal of a malicious action occurring.

Establish the right partnerships

You must establish the right partnerships among IT Operations, DevOps, developers, and business leaders to reduce privileged access security risk. This may feel like a lot of work, but trust me, it will pay off when you're in execution mode. Security and usability don't always have to be in conflict. Controlling privileged access can improve productivity and employee satisfaction. You should find a way to "sell" your privileged access security 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. Finding ways to not slow the IT Operations and DevOps teams is key. Examples of win-win benefits for IT Operations are shown in Table 5-1.

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.
Increased uptime	System availability can improve as a result of preventing user error. The mean time to recover from an outage can decrease through better forensic capability. If privileged sessions are recorded, it is faster to review recent changes in recordings than server logs.
Easier troubleshooting	IT issues can be easier to diagnose if detailed privileged user access logs are available to show, for example, that repeatedly, a particular set of user actions was made before a particular type of problem occurred.

Select a privileged access security platform



TIP

To help you pick the right privileged access security platform, consider these three essential activities:

» **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. Large organizations will find it nearly impossible to manually audit the thousands of privileged accounts, credits, and secrets used on-premises and in the cloud on an ongoing basis. 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 may drive efficiency day to day in addition to adding security controls.

» **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.

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?

» **Evaluate 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

- **Passwords:** Flexible and configurable password rotation for users, applications, and DevOps tools
- **Security and recoverability:** Isolated digital vault, hardened and secured to store credentials and privileged session recordings securely; multiple options for high availability and disaster recovery
- **Audit and monitoring:** Strong support for audit and monitoring and anomaly detection of suspicious privileged access activities



REMEMBER

- **Tool integration:** Integration with a broad range of IT and security operations tools
- **Privileged account discovery:** Capabilities to systematically locate privileged accounts and credentials
- **Privileged task automation:** The ability to automate routine privileged access tasks
- **Cloud:** Ability to secure, monitor, and control access to the “as a Service” offerings that your company uses or plans to use going forward
- **DevOps management:** Comprehensive management of all sensitive elements in the DevOps process
- **Flexible and scalable architecture:** Component-based architecture for flexible architecture and deployment options as your deployment scales

Ultimately, you should develop a simple privileged access solution scoring matrix that allows you to assess your current and future use cases and requirements against available features and providers. Select the provider that best meets your needs, best integrates with your broader security tool portfolio, and has the best long-term company health and support so you know it will be there when you need it.

IN THIS CHAPTER

- » Eliminating irreversible network takeover attacks
- » Securing infrastructure accounts and limiting lateral movement
- » Protecting credentials for third-party applications and *NIX SSH keys
- » Securing DevOps secrets, SaaS admins, and privileged business users
- » Investing in periodic red team exercises
- » Measuring privileged access security risk
- » Utilizing multi-factor authentication

Chapter 6

Ten Actions for Securing Privileged Access

To protect the enterprise and its customers, information security teams and their leadership must heavily focus on protecting the “keys to the kingdom” that are privileged accounts, credentials, and secrets. Doing this should be part of daily hygiene, like brushing your teeth. To be effective, it must become a routine that’s part of expected activities (not seen as extra efforts or special projects). This is often referred to as *cyber hygiene*.

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



REMEMBER

Your efforts should be iterative and use quick sprints to logically take on the highest scope 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 on your company and culture. The most important thing is prioritization of each sprint to ensure the most value and minimize scope creep.

Eliminate Irreversible Network Takeover Attacks

Don't let the attackers ruin your network and create long-term damage by gaining access to your domain controllers (flip back to Chapter 3 for a quick refresher if you need one). Attackers with domain controller access will establish “persistence” in an organization by running an attack that's hard to identify and detect so they can stay there a long time. So, what can you do about it?

- » Leverage your privileged access solution to enable/require Multi-Factor Authentication (MFA). MFA requires two or more forms of authentication — such as a password (something you know) and a one-time password sent to your mobile phone (something you have) — to access critical systems.

Ensure that all privileged access to tier 0 and tier 1 network assets is isolated and requires MFA. Tier 0 assets are the most sensitive and include administrative accounts, groups, domain controllers, and domains. Tier 1 assets are domain member servers and applications that can typically access sensitive business data.

- » Ensure that there are no hash residuals by design. A hash residual is like a fingerprint of a password that can be used by attackers to gain access to critical systems, including domain controllers.
- » Confirm that your privileged access solution can enable domain controller protection options, such as monitoring of suspicious access and blocking unknown applications.
- » Enable a method to detect attacks on domain controllers by identifying and blocking them.
- » Block the ability to create infrastructure accounts on tier 0 assets.

Control and Secure Infrastructure Accounts

You must control and secure access to your on-premises and cloud infrastructure accounts because these are some of the riskiest keys to your kingdom. Infrastructure accounts can be anything from server admin accounts to database instance accounts to cloud infrastructure accounts. At minimum, you must protect these from attackers who will leverage powerful default infrastructure accounts that are seldom used in day-to-day operations. Also, don't forget the infrastructure accounts used by your DevOps teams. If infrastructure accounts aren't properly secured, attackers can take ownership of the entire technology stack by compromising a single infrastructure account with a default and unchanged password. The same credentials can be used to access similar assets.

To protect your assets, make sure to

- » Have 100 percent managed accounts across your on-premises and cloud infrastructure (using secure processes and a privileged access security solution that consistently and securely manages these accounts).
- » Secure and rotate credentials for all well-known infrastructure accounts leveraging a digital vault that securely stores account passwords, credentials, and secrets.
- » Ensure infrastructure admin "sessions" are isolated and recorded.

A session is when infrastructure admins log into a system and perform tasks. This way, you can go back and evaluate what they (or their account) did to the system or network. This is helpful for forensics, and also modern behavior analytics tools can alert if things happen that may seem out of the ordinary.



TECHNICAL
STUFF

Limit Lateral Movement

Attackers love to steal credentials by moving laterally across the infrastructure, for example, by using pass-the-hash techniques in order to steal elevated permissions. If you aren't familiar,

pass-the-hash essentially utilizes a “hashed” or encoded password to directly log in to the application versus using the full password. You can keep attackers at bay by completely removing all end-point users from the local admins group on IT Windows workstations and preventing credential theft from endpoints.

Protect Credentials for Third-Party Applications

You are only as good as your weakest link, and your third-party applications could be one of them. Examples of common third-party applications include application servers, IT Operations tools, security software, and Robotic Process Automation. Compromised third-party applications are used to perform operations such as deep scans in order to steal your embedded privileged credentials. From here, cybercriminals execute their attack goals while completely circumventing the targeted company’s defenses.



TIP

What can you do? Make sure you vault all privileged credentials used by third-party applications and that they’re rotated frequently. This should be one of your first actions when you obtain or leverage a privileged access management solution.

Manage *NIX SSH Keys

SSH keys are gold to a hacker or malicious insider. Attackers can leverage unmanaged SSH keys in order to log in with root access and take over the *NIX (Linux and Unix systems) technology stack. Unix and Linux systems house some of an enterprise’s most sensitive assets, and Linux is a commonly deployed operating system in cloud environments. Individual accounts and credentials — including SSH keys — used to gain root privileges are often overlooked by security teams.



TIP

Get these keys in a vault ASAP. After you vault these, make sure to routinely rotate them based on policy. Your privileged access solution will work perfectly for this and enable significant event notifications and automation to take some human error out of the equation.

Defend DevOps Secrets in the Cloud and On-Premises



REMEMBER

Don't forget about DevOps. DevOps teams have the “need for speed,” and ensuring their tools and coding methods handle privilege access security is very important. Fixing these processes and tools as soon as possible will help avoid rework or time loss and prevent bigger problems down the road that become even harder to manage. Follow these security measures:

- » Secure the credentials and secrets used by DevOps tools, such as Ansible, Jenkins, and Docker, and Platform as a Service (PaaS) solutions such as OpenShift and Pivotal Cloud Foundry.
- » Make sure these credentials and secrets are retrieved on the fly and are automatically rotated and managed. This essentially means your code should be capable of retrieving the necessary privileged credentials from a privileged access solution versus hardcoding them. Policies for rotating secrets also greatly reduce the risk of secrets becoming compromised.

Secure SaaS Admins and Privileged Business Users

Software as a Service (SaaS) and privileged business users can be forgotten in prioritization efforts. Cybercriminals steal credentials used by SaaS administrators and privileged business users in order to get high-level and stealthy access to sensitive systems. Examples of SaaS applications could be anything from Customer Relationship Management software to applications used by the Finance, HR, and Marketing teams. Privileged business users with access to these types of applications can perform very sensitive actions such as downloading and deleting sensitive data.

To prevent this kind of attack, isolate all access to shared IDs and require Multi-Factor Authentication (MFA). Also monitor and record sessions of SaaS admins and privileged business users.

Invest in Periodic Red Team Exercises to Test Defenses

A *red team* is a team of individuals who focus on trying to break or compromise company assets much like attackers do. The difference is that they're doing it ethically and with approval, so the issues can be found and fixed before the attackers can exploit them.



TIP

When you hire and operate your own red team or hire an outside firm, the drills will be as real as possible. Follow these tips:

- » **Start small and grow.** You can have initial success with one red team member or one red team project with an outside firm. You can invest more as you prove the value.
- » **Hire or train experts with a passion for ethical hacking.** If you move forward with an in-house red team, make sure to give the team plenty of training about compromising privileged accounts and credentials so the team can help you get visibility to your weaknesses fast. Red teams can be an excellent way to drive interest for your security program because it can be fun for the right individuals.

Invest in a Tool to Periodically Measure Reduction in Privileged Security Risk

Measurement of risk and maturity is a critical capability. If you aren't gauging and adjusting for risk and change, you can't focus and know if you've done enough. To adequately measure reduction in privileged security risks, use a tool.



TIP

Measurement tools may be available from your privileged access management solution. There are also solutions in the market available to measure your entire security program against an established framework (such as NIST CSF). Ideally, your measurement of progress and risk around privileged access should roll into your broader measurement system and dashboards to tell a comprehensive risk reduction story. Whether you build it, buy it, or manually track it, measurement is critical to progress, success, and knowing your current level of risk.

Utilize MFA

Passwords are crackable, findable, and sharable. Good MFA that requires something you have and something you know exponentially decreases compromise. Attackers will do all sorts of things to get account passwords, credentials, and access keys. To thwart MFA, they oftentimes need to physically have the owner's phone or a security token. This is hard.



TIP

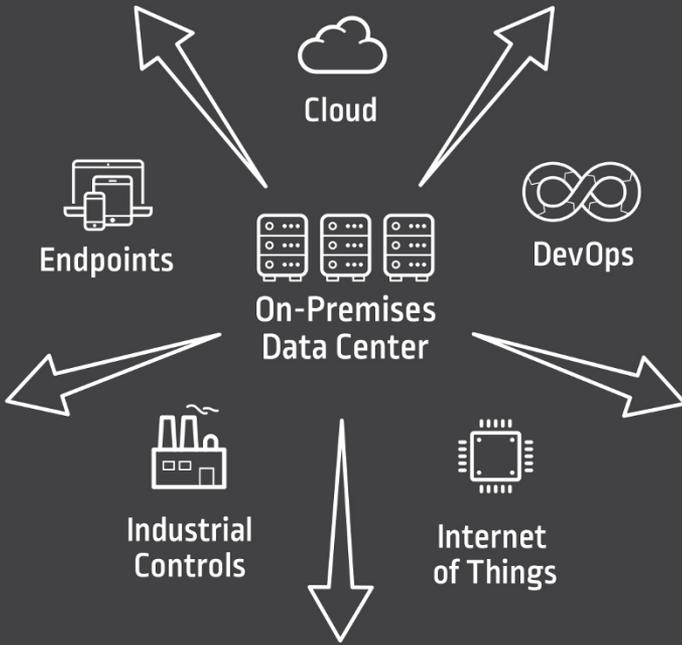
Ensure that your solution heavily leverages MFA to exponentially enhance the protection that you're investing in. The world is getting more used to this being required, so the requirement of using a second factor (like a pin texted to your smartphone) in addition to your password is a critical step to reducing your privileged security risk.

Notes

Notes

Notes

Notes



SECURE PRIVILEGE. STOP ATTACKS.

Interested in learning how the #1 leader in privileged access security can help reduce your risk?

- Schedule an assessment to understand your Privileged Access Security Score
- Scan your network with CyberArk DNA to locate unsecured credentials
- Take the free "Intro to Privileged Access Security" course

www.cyberark.com

Deploy a privileged access security program

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, on endpoints, and across DevOps environments. 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 tighten your privileged access security 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 healthcare. He's a creative strategist that brings strategy to life through successful execution. He runs a consulting company in successfully applying industry experience within security, privacy, IT, and risk management.

Go to **Dummies.com**[®]
for videos, step-by-step photos,
how-to articles, or to shop!

for
dummies[®]
A Wiley Brand

 Also available
as an e-book

ISBN: 978-1-119-51538-8
Not for resale

WILEY END USER LICENSE AGREEMENT

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