Brought to you by:

thycotic

Least Privilege Cybersecurity

for dummies®
A Wiley Brand

Understand least privilege security basics

Plan your least privilege strategy

Apply least privilege with application control

Joseph Carson, CISSP

Thycotic Special Edition

About Thycotic

Thycotic powers easy-to-manage and ready-to-adopt privilege management solutions. Thycotic's security tools empower over 10,000 organizations, from small businesses to the Fortune 500, to limit privileged account risk, implement least privilege policies, control applications, and demonstrate compliance. Thycotic makes enterprise-level privilege management accessible for everyone by eliminating dependency on overly complex security tools and prioritizing productivity, flexibility, and control. Headquartered in Washington, D.C., Thycotic operates worldwide with offices in the UK and Australia. For more information please visit **www.thycotic.com**.

Least Privilege Cybersecurity

Thycotic Special Edition

by Joseph Carson, CISSP

for dummies®
A Wiley Brand

Least Privilege Cybersecurity For Dummies®, Thycotic Special Edition

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

ISBN: 978-1-119-56525-3 (pbk); ISBN: 978-1-119-56526-0 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

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

Project Editor: Carrie A. Burchfield
Editorial Manager: Rev Mengle
Production Editor: Mohammed Zafar Ali
Acquisitions Editor: Ashley Barth
Business Development Representative: Sue Blessing

Introduction

Companies are spending billions on cybersecurity, yet hackers, cybercriminals, and disgruntled employees continue breaching computer systems, stealing sensitive information, or disrupting services. With more than 80 percent of breaches involving the compromise of IT and business user credentials (IDs and passwords), organizations want to limit what's known as privileged access to services, applications, data, and systems — a concept called *least privilege cybersecurity.*

Privileged accounts exist everywhere in your IT environment. In many cases, users may not even realize the type of access they possess. They only know that when access is denied, they can't get their work done. Hackers and cybercriminals target these privileged accounts because once compromised, they give the ability to move across your systems and networks undetected.

Despite efforts to raise cyber awareness and train users on secure behavior, nearly one in four employees will open phishing emails, and more than one in ten will click on an attachment that contains malware. These types of successful social engineering attacks are one reason employee workstations and personal devices are the most vulnerable part of your IT systems. All it takes is one compromised user with local administrative privileges to gain full control or even take down your entire network.

About This Book

Organizations today typically face major challenges when seeking to implement least privilege because built-in limits on access can impact employee productivity. If users can't get access to an account, a service, or a device such as a printer, they have to spend time calling the IT helpdesk for a "fix." In many cases, busy IT helpdesk workers may give users more privileges than needed to expedite resolution of user problems. Least privilege is meant to prevent "overprivileged access" by users, applications, and services to help reduce the risk of exploitation without impacting productivity.

This book is a first step in understanding the mechanics and value of implementing a least privilege cybersecurity strategy. It gives you the basic principles behind least privilege as well as how to plan your own strategy with key actions to get started. ***Note:*** Throughout this book, the phrases "least privilege cybersecurity," "least privilege security," and "least privilege" are used interchangeably.

I wrote this book for IT managers, administrators, systems administrators, and security professionals who are responsible for protecting their organizations from hackers, cybercriminals, and malicious insider threats. I assume a basic level of IT expertise and experience, including familiarity with IT networks and the use of privileged accounts (human and non-human) across the organization. *Least Privilege Cybersecurity For Dummies,* Thycotic Special Edition, provides an easily digestible introduction to the concept of least privilege cybersecurity for business executives and users.

Icons Used in This Book

This book uses the following icons to indicate special content:

REMEMBER

You don't want to forget this information. It's essential to gain a basic understanding of least privilege cybersecurity.

TECHNICAL STUFF

This icon indicates more technical information that is of most interest to IT and system administrators.

TIP

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

Beyond the Book

Developing, implementing, and enforcing least privilege cybersecurity only *begins* with this book. To learn more, visit `www.thycotic.com`. You'll find resources, including free software tools, white papers, videos, and product information, that help explain and manage least privilege security.

IN THIS CHAPTER

- Getting started with zero trust
- Classifying users
- Enforcing least privilege
- Meeting compliance

Chapter 1
Defining Least Privilege Cybersecurity

Least privilege cybersecurity enables enforcement of a zero trust risk-based security model whereby once a user is verified, the user's access is limited to only what's necessary to accomplish the specific task or job. If any user action requires more access than granted via policy rules, permissions to elevate privileges are strictly controlled and monitored. While simple in concept, enforcing least privilege in IT environments can be highly complex and involve hundreds, if not thousands, of users, applications, and services that need access to privileged permissions.

Starting from Zero Trust

Zero trust assumes any user or system that accesses the network, services, applications, data, or systems starts with zero trust. To gain authorized access, trust must be earned by the prospective user through verification. For example, verification can require two-factor authentication. In this instance, a user provides a password but then must take an additional step by using an authentication application. When new devices are introduced on the network — and before they obtain access to any resources — they must first identify and verify themselves based on various

security controls. The more sensitive the resources to be accessed, the more security controls they must satisfy.

Cybersecurity should always begin with zero trust, ensuring that only authorized access is permitted. After verification of identity is established, users can be classified according to the access they need to perform their jobs.

Classifying Trust Dynamically

Cybersecurity classifications of trust and accepted risk should be dynamic. This means you need to create policies or rules across the enterprise for identities, services, applications, data, and systems. For example, you can have an "always verify" and "always monitor" policy for third-party vendors or contractor identities. Internal employee classifications would be adaptive based on the sensitivity of the data being accessed.


TECHNICAL STUFF

An always verify policy would require credentials and multifactor authentication, while an always monitor policy would audit and record all activity.

PREVENTING THE EXPLOITATION OF OVERPRIVILEGED USERS

Many times, companies inadvertently give their employees too much access to account information. This oversight results in overprivileged users and can lead to breaches within your company. Take Sarah, for example, who is an employee at a manufacturing company. As an easy way for her to perform her job, she's been given a laptop that has local administrator admin account rights. In effect, the local admin account gives her relatively unlimited access to run applications, even though she may not be aware of it. She has just become an overprivileged user.

One day, Sarah receives an email with an attached document that appears to be a legitimate request from the CEO of the company. She clicks on the attachment, and unbeknown to Sarah, she downloads malicious software that kicks off processes that capture her user ID and password.

Because Sarah's computer contains local admin rights, the malware has succeeded in editing the computer's registry, allowing the malware — and the cybercriminal — to persist on Sarah's computer. Without Sarah

realizing it, the malware has also captured the hashes of Sarah's credentials, allowing it to traverse other areas within her company's IT network. The malware covers its tracks by changing audit logs. No one knows that the cybercriminal is inside the network. And all of this occurs through what's known as a *local admin rights takeover* — a compromised privileged account resulting from an overprivileged user.

Other classifications are as follows:

- **Services and applications** can be classified by the sensitivity of the data that the service or application has access to. For example, does it contain sensitive information such as credit card details or health records?
- **Devices** can be classified as employee personal devices and contractor devices, versus corporate owned and managed issued devices. Personal or contractor devices should fall into the "never trusted" classification because you never know what applications or malicious software exists on these devices to exploit opportunities. Therefore, segment networks to distinguish untrusted networks such as personal or contractor devices, versus trusted networks that can connect only to known managed corporate systems.

Enforcing Least Privilege

Least privilege enforcement has two aspects:

- **Privacy:** When a user logs in, she can only see what she's permitted to access.
- **Security:** Based on specific privileged access, a user has limits on what applications/tasks she can run.

Least privilege enforcement typically starts by removing local administrative privileges on endpoints, such as user laptops or mobile devices, so you can reduce your attack vulnerabilities and prevent most attacks from occurring. Least privilege is effective at reducing major patch management headaches. Enforcing least privilege security can help eliminate more than 90 percent of Microsoft Windows patches because most vulnerabilities require admin privileges to exploit them.

A HOTEL ACCESS ANALOGY

Implementing zero trust with least privilege may be easier to understand when expressed through a hotel access analogy. Some cybersecurity systems look at verifying employee users at the entrance to the hotel lobby. After the identity of a person is verified, he basically gets a master key with access to all the areas and rooms in the hotel. He can roam freely throughout the hotel corridors and enter any room even if it's locked. No one will challenge his actions, and he doesn't need anyone to help him gain access. He's an overprivileged user.

However, when least privilege is applied, after the identity is verified, the user gets a key that allows him only into a specific room and/or onto a specific floor. And when least privilege is combined with application control, the individual can enter a room but is limited in his actions once he's in the room. He may, for example, be able to turn on a faucet in the bathroom but not open a window. If he tries to open a window, an alarm will go off, and a hotel security person will investigate the potential security risk.

Imagine managing thousands of people who enter the hotel to conduct business. Verifying identities at the lobby may seem to be logical, but once a user enters, giving him free access to every room and part of the hotel is extremely risky. At the same time, you don't want users to be so restricted in where they can go and what they can do that the restrictions keep them from completing their work.

Meeting Compliance Requirements

Many compliance and regulations require strict security controls in the use of privileged access. Organizations that provide end-users with too many privileges will always struggle to satisfy most compliance requirements. And when they do apply strict controls to meet regulations, they can negatively impact user productivity. Thus, it's critical to create a least privilege strategy that both restricts end-users' privileges without preventing employees from performing tasks needed to successfully do their jobs.

IN THIS CHAPTER

- Finding your most critical assets
- Matching privileged accounts to critical assets
- Establishing a PAM program
- Implementing a least privilege life cycle approach

Chapter 2
Getting Started with Least Privilege

This chapter highlights the key functions you must perform to set the proper course for your least privilege security journey. They provide the foundational elements that allow you to implement least privilege enforcement tailored to your specific organization's assets and business model.

Identifying Critical Assets

A risk-based approach to cybersecurity enables you to determine what assets to protect, what security controls you need, and what security challenges you must address to effectively reduce risks.


TIP

Start with a data impact assessment to determine what services, applications, data, and systems are most critical to your specific business, along with compliance and regulations you must meet. You must identify those critical data assets that, if compromised, could cause either major financial harm or disruption of business services.

Mapping Privileged Accounts to Critical Assets

After you've identified your most critical information assets, you can then define what kind of privileged accounts are associated with these assets:

- Human (interactive) services, applications, or systems
- Accessible via hardware, software, on-premises, or in the cloud
- Used in internal networks or by external services
- How often they're used
- Department or location specific
- Sensitivity of the service, application, or data the account is protecting
- Service or system owner for accountability

Incorporating the Privileged Access Management Life Cycle

Like any IT security measure designed to help protect critical information assets, managing and protecting privileged account access requires both a plan and an ongoing program. You must identify which privileged accounts should be a priority in your organization and ensure that those employees who are using these privileged accounts understand acceptable use and their responsibilities.

Figure 2-1 illustrates a privileged access management (PAM) life cycle approach that should be incorporated into your least privilege strategy to

- Define privileged access and accounts
- Discover privileged accounts continuously
- Manage, secure, protect, and control privileged accounts
- Audit and monitor usage

- Investigate unusual behavior
- Respond to incidents
- Review and evaluate privilege access controls

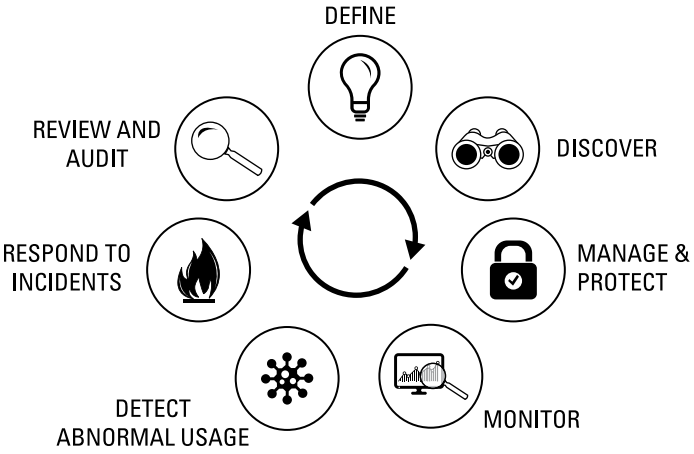

FIGURE 2-1: The PAM life cycle.

Your next step in implementing a least privilege strategy will be to determine privilege usage across your environment based on how you define privileged access:

- Who has privileged access
- When it is being used
- What actions require privileged access
- What security controls should be applied
- Compliance requirements associated with privileged access

Taking a Least Privilege Life Cycle Approach

After identifying your critical assets, mapping them to privileged accounts, incorporating PAM, and defining privilege usage, you're ready for least privilege implementation.

REMEMBER

A sustainable least privilege strategy isn't something that can be set up overnight. It takes planning, collaboration, and the right tools to meet the needs of security, IT, desktop support, and users.

TIP

In taking a least privilege life cycle approach, you increase your odds of implementation success. When trying to achieve least privilege cybersecurity in your organization, follow these key steps:

- Conduct discovery to find out which endpoints and local users have admin rights, what applications are in use, and if they require admin rights to run.
- Create a whitelist of acceptable trusted applications and processes.
- Block known bad files with a blacklist or incorporate a reputation service.
- Manage unknown areas with a greylist and an automated workflow to allow approved apps to run and to block malicious apps.
- Set contextual policies that align with the risk assessment.
- Plan for users to change roles or departments.
- Don't limit yourself to domain-controlled endpoints only.
- Don't forget child processes.
- Integrate workflow into existing tools.
- Measure success coverage and existing risks.
- Enable user interactive elevation requests/workflows.

REMEMBER

This book focuses on the topic of least privilege cybersecurity applied to an end-user due to many major cyber incidents resulting from overprivileged users. Overprivileged users are the best place to start applying least privilege security; however, it can readily be extended to any privileged account, even non-human system, application, service, or domain accounts.

IN THIS CHAPTER

- Creating a list of your devices and software
- Integrating compliance requirements
- Combining least privilege with PAM to control access
- Adding application control
- Managing users' privileges

Chapter 3
Five Actions to Least Privilege Success

In this chapter, I give you five action steps that set you on the right path to a successful least privilege implementation journey. These steps highlight the key stages of activity but are shortened and simplified for this book. They are meant to spur further research so you can be fully prepared with the tools you need to make least privilege cybersecurity a reality.

Inventory Devices and Software

TIP

Produce a comprehensive inventory of your corporate devices, installed software, and software licenses. You also need to determine where applications typically are being installed from, as well as the software vendors that are approved to be used within your organization.

During the inventory process, create a list of trusted vendors, including signed certificate and trusted software sources for approved applications. These could include a software delivery

solution, a software catalogue, a network location, or Microsoft SharePoint. You also need to list the places you don't want software being installed from that could include downloaded program files, email attachments, or any download locations on various devices.


REMEMBER

With a complete device inventory, you can develop policies that incorporate trusted and untrusted privilege elevation requests. This process ensures employees can use a least privileged account to perform privileged actions based on approved policies.

Integrate Compliance and Regulations

Almost every organization faces some kind of compliance mandate or regulatory requirement. There have, for example, been major recent updates to regulations such as the Payment Card Industry Data Security Standard, National Institute of Standards and Technology, Cyber Essentials, EU General Data Protection Regulation, and the California Consumer Privacy Act. They all include requirements for data privacy meant to rein in overprivileged access by users. Therefore, you must integrate compliance and regulations that apply to your organization into your data impact assessment, risk-based assessment, and privileged access management (PAM).

Combine PAM and Least Privilege to Control Access and Actions

A PAM solution helps with defining policies, discovering privileged accounts, applying security controls, auditing usage, and alerting abuse. Combining PAM with least privilege security allows an organization to elevate privilege OnDemand, offer one-time passwords, and increase and decrease privileges based on dynamic risk and threats. PAM helps control privileges, so they're available when needed, and end-users aren't overprivileged all the time.

ARE YOU AUDITING AND REMOVING UNNEEDED ADMINISTRATOR RIGHTS?

Continuous auditing of administrator and privilege usage allows an organization to determine if the access is still required. This should be done when privileges are set to expire or on a scheduled basis to determine if privileges need to be updated. This process could mean demoting a user's privileges to least privilege and applying a policy that enables privileges to be elevated on demand by using previous known behavior. Therefore, the user can still be productive and least privilege can be hidden in the background without any impact or knowledge to the end-user.

Incorporate Application Control

Application control is technology that enables an organization to elevate application privileges so trusted and approved applications can execute even if users don't inherently have access. On the flip side, application control prevents untrusted applications from executing even if the user has the privileges that permit them to install applications. If an application is unknown, it can be "quarantined" and prevented from executing until further analysis determines whether the application is malicious or authentic.

Manage/Protect Privileges Granted to Users

Separating least privileged users from privileged accounts allows an organization much more control and security over how privileges are granted to users and determines a risk-based approach to what's an accepted risk. This step allows the organization to adopt a zero trust security posture that's enforced by a least privilege strategy, reducing the risk from cyberattacks but maintaining empowered employees and productivity without the pain.

REMEMBER

Least privilege security with application control are both necessary. Least privilege with application control solutions helps organizations reduce security threats and maintain productive employees who can continue performing privileged tasks and actions under trusted predefined policies. With least privilege alone, you produce unhappy employees and increased helpdesk calls but increased security. But when you add application control, your employees are empowered and continue to be productive with increased security working in the background to prevent cyber threats. At the same time, this step helps reduce helpdesk calls.

TIP

The key benefits of implementing a least privilege strategy with application control include

- **Reduced costs:** Save time and money in managing users securely.
- **Empowered, happier employees:** They can perform their duties without encountering roadblocks.
- **Fast tracks compliance:** Automate reporting to satisfy auditors.
- **Improved security:** Block cybercriminals and malicious insiders from exploiting password compromise.

Applying the core principles of least privilege is a foundational element of your cybersecurity strategy. By removing local administrative privileges on endpoints, you reduce your attack surface and block the primary attack vector, preventing the vast majority of attacks from occurring.

REMEMBER

Before you start implementing next-generation Endpoint Protection Platforms (EPP) or complex Endpoint Discovery and Remediation solutions (EDRs), you should consider a least privilege strategy with application control solution. Proactive protection based on least privilege means less time and resources spent detecting an infection, chasing down hackers once they've already entered your network, and remediating the damage.

Let your least privilege cybersecurity journey begin!

FREE from Thycotic

LEAST PRIVILEGE CYBERSECURITY TOOLBOX

Download them all at: www.thycotic.com

FREE

Free White Papers & Reports

Top 10 Keys to Successful Least Privilege Adoption via Application Control
thycotic.com/keys-to-privilege-adoption

Boost Your Endpoint Security with a Least Privilege Strategy
thycotic.com/windows10-least-privilege

Top 5 Least Privilege Reports CISO's Live For
thycotic.com/top-ciso-reports

FREE

Free Cybersecurity Software Tools for IT Professionals

Free Least Privilege Discovery Tool
thycotic.com/least-privilege-tool

Free Windows Endpoint Application Discovery Tool
thycotic.com/free-endpoint-discovery

Free Privileged Account Discovery for Windows and UNIX Tools
thycotic.com/windows-discovery-tool
thycotic.com/free-unix-discovery

FREE

Free eLearning Tools for IT Professionals

Free Privileged Password Security Online Training Course
thycotic.com/password-security-certification

Free eLearning Tools for IT professionals
thycotic.com/e-learning-tools

FREE

Free Cybersecurity Benchmarking Tools for IT & Risk Professionals

Free Privileged Account Management (PAM) Risk Assessment
thycotic.com/pam-risk-tool

Your least privilege security strategy starts here

This book helps you develop a least privilege approach to secure your IT environment, especially endpoints like laptops and mobile devices. Applied to privileged accounts, least privilege with application control is becoming a requirement to protect IT systems from hackers, cybercriminals, and malicious insiders. With a clearer understanding of how least privilege fits into your cybersecurity strategy, you can plan how best to implement least privilege successfully in your own organization.

Inside...

- Why enforcing least privilege is essential
- Start from a "zero trust" perspective
- Map info assets to privileged accounts
- Incorporate privileged access management
- Ensure least privilege & application control
- Key steps to a successful implementation

thycotic

Joseph Carson has 25+ years of experience in enterprise security. He's the author of *PAM For Dummies* and *Cybersecurity For Dummies*. Joseph is an active member of the cyber community, speaking at global conferences and advising governments and critical infrastructure, financial, and maritime industries.

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

ISBN: 978-1-119-56525-3
Not For Resale

for dummies®
A Wiley Brand

Also available as an e-book

WILEY END USER LICENSE AGREEMENT

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