

the  
**GORILLA  
GUIDE**<sup>®</sup> to...



# Endpoint Privilege Management

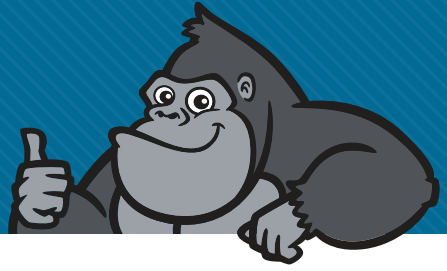
Stop Cyber Risks Before They  
Start with Smarter Privilege  
Control

**ED TITTEL**



POWERED BY  **ActualTech**  
MEDIA

the  
**GORILLA**  
**GUIDE**<sup>®</sup> to...



# Endpoint Privilege Management

Stop Cyber Risks Before They Start  
with Smarter Privilege Control

By Ed Tittel

POWERED BY  **ActualTech**  
MEDIA

Copyright © 2025 by Future US LLC  
Full 7th Floor  
130 West 42nd Street  
New York, NY 10036

All rights reserved. This book or any portion thereof may not be reproduced or used in any manner whatsoever without the express written permission of the publisher except for the use of brief quotations in a book review. Printed in the United States of America.

[www.actualtechmedia.com](http://www.actualtechmedia.com)

---

## PUBLISHER'S ACKNOWLEDGEMENTS

### DIRECTOR OF CONTENT DELIVERY

Wendy Hernandez

### GRAPHIC DESIGNER

Olivia Thomson

### WITH SPECIAL CONTRIBUTIONS FROM PALO ALTO NETWORKS

Andrey Pozhogin

DIRECTOR PRODUCT MARKETING

## ABOUT THE AUTHOR

Ed Tittel is a 30-plus year veteran of the IT industry who writes regularly about cloud computing, networking, security, and Windows topics. Perhaps best known as the creator of the *Exam Cram* series of certification prep books in the late 1990s, Ed writes and blogs regularly for GoCertify.com, ComputerWorld, and other sites. For more information, including a resume and list of publications, please visit [EdTittel.com](http://EdTittel.com).

# ENTERING THE JUNGLE

<b>Introduction</b>	<b>6</b>
<b>Chapter 1: Endpoint Privilege Management: A Primer</b>	<b>7</b>
Endpoint Privilege Management—Critical to Identity Security	8
Why Endpoint Privilege Management Matters: Cases in Point	9
<b>Chapter 2: Access and Privilege Security</b>	<b>12</b>
Verdict-Based vs. Access and Privilege-based Security	12
Access and Privilege Security Implementation Examples	16
Protection from Cyberattacks	19
<b>Chapter 3: Practical Endpoint Privilege Management</b>	<b>22</b>
Remove Local Administrator Access	22
Enforce the Principle of Least Privilege	23
Define Restrictions for Unknown Applications	24
Best Practices for Endpoints	24
Making Endpoint Privilege Management Work for Your Organization	25
<b>Chapter 4: How Endpoint Privilege Management Drives Overall Security</b>	<b>26</b>
Identity Is the Cornerstone for Security	27
Key Components of Endpoint Privilege Management	28
Understanding Adaptive Risk Reduction	29
<b>Chapter 5: Getting Started with Idira Endpoint Privilege Manager</b>	<b>31</b>
Rapid Risk Reduction	31
Compliance and Auditability	32
Stay Cyber Secure	33

# CALLOUTS USED IN THIS BOOK



## SCHOOL HOUSE

In this callout, you'll gain insight into topics that may be outside the main subject but are still important.



## FOOD FOR THOUGHT

This is a special place where you can learn a bit more about ancillary topics presented in the book.



## BRIGHT IDEA

When we have a great thought, we express them through a series of grunts in the Bright Idea section.



## DEEP DIVE

Takes you into the deep, dark depths of a particular topic.



## EXECUTIVE CORNER

Discusses items of strategic interest to business leaders.



### DEFINITION

Defines a word, phrase, or concept.



### GPS

We'll help you navigate your knowledge to the right place.



### KNOWLEDGE CHECK

Tests your knowledge of what you've read.



### WATCH OUT!

Make sure you read this so you don't make a critical error!



### PAY ATTENTION

We want to make sure you see this!



### TIP

A helpful piece of advice based on what you've read.

# INTRODUCTION

**Welcome to The Gorilla Guide® To... Endpoint Privilege Management.** In the upcoming chapters, this book will explain the fundamentals of endpoint privilege management and the cornerstones of identity and privilege, providing real-time privilege usage tracking, application information, audit trails with forensic depth, and shadow IT detection. It also speaks to the difference between verdict-based access controls and the systematic, best-practices-driven management of privileges and access found in endpoint privilege management. Through examples based on real-world security incidents, best implementation practices, and principles, this Guide explains how to put endpoint privilege management to work to boost your security posture, lower cyber risk, and achieve improved compliance and auditability. It all starts with Chapter 1, which explains and explores endpoint privilege management in greater detail. Buckle up: we're on our way!

## CHAPTER 1

# Endpoint Privilege Management: A Primer

**Endpoints are where identities, privileges, and data come together.** Without proper and proactive protection, especially privilege- and identity-based controls, attackers can compromise endpoints and use them to move laterally. With a foothold in your environment, attackers can then expand their access, collect and exfiltrate sensitive data, attack mission-critical assets and deliver damage to an enterprise or organization. These potential exposures explain why protecting identities and managing privileges are vital. And because endpoints are where users interact with internal servers and external networks, they are a primary focus for attack from the outside, and protection and security from the inside.

Here's how best to understand identity and privilege. Identity is who you are, as demonstrated by things you know and things you have. Permissions encompass the things an identity can do or touch. In this context, it's vital to understand that many identities belong to applications or infrastructure components—a good example is middleware or databases—as well as to people and job roles they occupy.

EPM represents a specialized collection of tools and technologies designed to discover privileged accounts, remove local admin rights and replace them with policy-based elevations, implement

application control and ringfencing, endpoint sign-in and AD bridging. When it comes to a specific aspect in endpoint privilege management—namely privilege elevation and delegation management (sometimes abbreviated PEDM), this is vital because of its focus is on controlling and monitoring elevated access to sensitive systems and data by privileged users. We'll go into much greater detail in the sections that follow to help you better understand endpoint privilege management solutions and PEDM, and why they're so important.

## Endpoint Privilege Management—Critical to Identity Security

A good “mission statement” for endpoint privilege management reads like this: “Secure every identity—both human and non-human—on endpoints with the right level of privilege controls and security-first access management from the moment they log in to that endpoint. Use strong, phishing-resistant and passwordless multi-factor identification when launching and elevating native applications, or working with SaaS applications as a regular or privileged user.” The overarching strategy is to manage and secure privileges and end user identity at the endpoint. Using the right level of privilege controls and security-first access management, endpoint privilege management solutions proactively prevent breaches, compliance failures, and operational disruptions.

Elements of endpoint privilege management solutions include:

- **Privilege Elevation and Delegation Management:** Elevated privileges only get granted when they're needed, and only to authorized identities. When elevated privileges are delegated to authorized staff (e.g., IT workers or help desk personnel), they receive only the barest minimally workable set of such privileges only for as long as they need them. There is no extra grant involved, such as system level or policy control.

- **Comprehensive Application Control:** Only authorized, white-listed applications may access the organization's networks and resources. Unrecognized applications may be denied access or sandboxed. Blacklisted applications will be completely blocked.
- **Continuous End-User Identity Assurance:** Obtaining access is not "one and done." Each time an identity uses elevated privileges, it must authenticate. Zero trust also dictates that for ongoing sessions, recurring, periodic authentication must occur.
- **Identity (AD) Bridging:** Integrate non-Windows machines with centralized accounts in active directory and modern cloud-based directories to unify identity and access management across the entire infrastructure.
- **Identity- and Privilege-Based Incident Response:** When investigating an alert, in addition to traditional network isolation PEDM tools can provide granular privilege reduction and additional end-user identity verification.

## Why Endpoint Privilege Management Matters: Cases in Point

Exploring risks, vulnerabilities, and losses may be best understood through a handful of brief, but pointed examples based on recent incidents. These help to show why and how proper endpoint privilege management fends off or avoids risks and exposures. Each of the following cases could have been stopped before they ever got going with a proper endpoint privilege management solution in place.

## HEALTHCARE SERVICES COMPANY BREACH

A data breach exposed sensitive data from over 165 organizations through a prominent healthcare services company. Its patient records and operational details were compromised and exposed. Attackers exploited stolen credentials and leveraged privilege escalation within the healthcare services IT environment, bypassing insufficient access controls to extract huge data volumes. The breach highlighted how unmanaged or excessive privileges created a dangerous and critical weakness. Had a proper endpoint privilege management solution been deployed, it could have enforced least privilege policies and credential protection at the endpoint level, preventing unauthorized access and escalation before the breach occurred.

## HEALTHCARE PRESCRIPTION AND BILLING SERVICES PROVIDER

A major healthcare services company suffered a devastating ransomware attack that exposed up to 6TB of sensitive patient data. It also disrupted billing operations nationwide. The breach was enabled by stolen credentials and the absence of multi-factor authentication (MFA) on remote access servers, allowing attackers to escalate privileges and move laterally across the network. This failure to enforce basic access controls made it possible for a notorious eastern European ransomware group to exfiltrate data and cripple services for weeks. Modern endpoint privilege management solutions could have prevented this incident by enforcing least privilege policies, credential protection, and MFA enforcement at the endpoint level, blocking unauthorized access and privilege misuse before it began.

## CREDENTIAL MANAGEMENT APPLICATION VENDOR

A company that provides a program designed to manage and protect user and system credentials was breached. In its ongoing and protracted aftermath, attackers used stolen vault data—including API tokens, MFA seeds, and encryption keys—to siphon over \$16

million in cryptocurrency from users, many of whom were part of a healthcare services ecosystem who relied on the app for credential management. By exploiting stored seed phrases and private keys, cybercriminals escalated privileges and bypassed protections, draining crypto wallets across multiple incidents. This exploit shows the dangers of storing sensitive credentials in cloud-based password managers without endpoint-level safeguards. An endpoint privilege management solution could have mitigated this risk by enforcing credential protection policies, blocking browser memory and password dumping, and preventing privilege misuse at the endpoint level.

## **SUPPLY CHAIN SERVICES FILE TRANSFER TOOL EXPLOIT**

Attackers exploited a zero-day vulnerability in a supply chain service provider's file-sharing tool. Because that tool is used widely by healthcare services companies and government agencies, it hit hard and big. Attackers gained access to and exfiltrated sensitive data from 1,000-plus organizations and impacted over 60 million individuals. Another eastern European ransomware group leveraged this flaw to escalate privileges within the company's servers, bypass authentication, and deploy custom web shells for persistent access. Victims included healthcare and financial institutions whose data was exposed due to insufficient privilege boundaries and lack of endpoint-level controls. An endpoint privilege management solution could have mitigated this breach by enforcing least privilege policies, blocking unauthorized command execution, and detecting anomalous behavior before escalation occurred.

Please notice the common threads across all these various incidents: elevated access to protected, internal resources, especially administrator-level functions and/or privileged data repositories. Blocking such access; maintaining privilege boundaries; and detecting, then blocking unauthorized commands serves well to stop such attacks before they can do harm.

## CHAPTER 2

# Access and Privilege Security

**The principle of least privilege seeks to match current access needs and scope with privileges granted to identities, or to role groups to which such identities may be assigned.** Why is this a vital security principle? Over time (or by mistake) privileges may exceed what the user's role actually requires. Alternatively, groups and identities involved in starting up efforts may get blanket access and permissions, which never gets reduced or revoked later on. Indeed, given a huge number of identities for various endpoints, it can be challenging for organizations to determine which and how many such users are “over-privileged.”

## Verdict-Based vs. Access and Privilege-based Security



Verdict-based security focuses on threat detection and analysis, often driven through machine learning. Typical examples include anti-virus programs, firewalls, and intrusion detection systems (IDSes). These items are important, and not to be overlooked, but they only provide part of a complete endpoint security strategy.

Why is privilege-based security a key complement to verdict-based security? Because verdict-based security is reactive, and comes into play only after something has happened. If implemented correctly, on the other hand, access and privilege security is proactive and significantly reduces the endpoint attack surface. As explained in the preceding cases, a proper endpoint privilege management solution could have stopped all those expensive attacks dead in their tracks had it been in place.

Intelligent privilege controls zero-in on the end-user identity and its access and privilege to resources. This provides a useful way to prevent developing attacks, and to contain attacks in progress. All in all, access and privilege-based security answers these questions:

- How can an organization stop attackers from obtaining the keys to the kingdom once they get past perimeter defenses?
- How can a company prevent attackers from accessing sensitive data, changing configurations, or tampering with verdict-based security?
- How can a business create maximum friction for threat actors at every step if infrastructure is targeted?

Limiting or completely preventing misuse of compromised, cracked, or stolen credentials is possible using tight privilege controls. Attackers can only do limited damage if their access to resources is also limited. Simply by rigorously limiting access for any identity to only what's explicitly allowed through assigned permissions is an incredibly powerful deterrent. Consider ransomware: these attacks can be quickly—and automatically—contained if compromised software has only limited access and privileges to an organization's data. Ransomware can't encrypt what it can't access. Without holding data hostage and inaccessible, the attack itself fails.

Verdict-based solutions focus on specific file attributes, content patterns, or behavior patterns, such as signatures or heuristics.

Extensive event recording abilities also give security teams the ability to perform retro-analysis or forensics, as well as do proactive hypothesis testing and threat hunting. Essentially, verdict-based security gets invoked upon analysis of data or behavior pattern, where something in the input triggers a decision that something malicious or suspicious is at work.

Typical forms of verdict-based approaches include:

- Endpoint detection and response (EDR) is a classic example of verdict-based security. Such systems analyze files and behaviors and look for signatures or use heuristics to block, quarantine and alert when detection occurs. EDR's decisions are typically based on known threats or suspicious patterns. Its verdicts are also tried to process execution not to user intent or (mis)use of privileges. EDR is thus subject to privilege misuse, including installing hacking tools, disabling agents, or making lateral pivot. Endpoint privilege management solutions focus primarily on use of privileges within the context of related access controls, and block all such activities.
- Security information and event management (SIEM) tools typically ingest logs from endpoints, servers, apps and security tool. They apply rules and make correlations to detect anomalies and flag known threat patterns. Their verdicts are based on event patterns, but do not attend to matters of identity or use of privileges. SIEM tools are passive, and do not intervene. Thus, SIEM might log use of a command shell, but cannot block or elevate it safely. Indeed, SIEM is unaware of use of privileges, and cannot tell if privileges are elevated, access is allowed or disallowed, or policy-compliant. Endpoint privilege management is acutely aware of identity and use of privileges, and can actively block out-of-bounds, unsafe, or non-compliant actions before they can complete.

- Indeed, behavior analytics monitor user actions over time. And while they can report on login patterns, apps usage, access times and locations, they are purely reactive and pattern-based. Endpoint privilege management, on the other hand, is acutely privilege aware, and able to enforce blocks and restrictions in real-time, as they occur. As with previous examples, behavior analytics may flag risky and even malicious behaviors, but cannot stop them from occurring. Such analytics are also typically tied to user IDs not to their privilege context, where endpoint privilege management operates directly from an understanding of this context, and how behaviors match up against access controls, policies, governance and compliance.

Such traditional, verdict-based approaches have not yielded satisfactory cybersecurity outcomes nor reduced cyber risk. The primary cause is disregard for identity security on the endpoint, which serves attackers far too well. Lack of strong, preventative, and continuous identity assurance makes it easier for attackers to pose as legitimate users. Overprivileged users and applications facilitate malware deployment, initial access, and lateral movement. Unmanaged endpoint attack surfaces present entry points for attackers and create data exfiltration paths. Consequently, a full spectrum of identity-based attacks, including web session hijacking, malware and ransomware attacks, insider threats, and data leakage, are routinely carried out by threat actors. Endpoint privilege management solutions can stop all these things before they cause harm or data loss.

In fact, endpoint privilege management is a game changer because it introduces dynamic, policy-based elevation based on app reputation and user content. Better yet, an endpoint privilege management solution can provide offline enforcement for roaming endpoints. It can even use AI-powered verdicts and community-sourced decisions to drive control and access. Thus, endpoint privilege management solutions integrate well with broader PEDM strategies for hybrid and cloud-native environments.

This is not to denigrate verdict-based security, nor to suggest it has no place in a security scheme. That said, it's best not to solely rely on verdict-based security, and to make sure that adequate access and privilege security exists to complement its capabilities. Verdict-based security is key to detecting and prompting attack response. Access and privilege security reduce the attack surface, disrupt attack techniques and limit the attack blast radius. Each by itself is only a half-measure, but together they are complementary, where each handles possible gaps in the other's coverage.



## **WATCH OUT FOR COMPLIANCE AND REGULATION**

**A majority of compliance frameworks such as HIPAA, PCI-CSS, Sarbanes-Oxley (aka SOX), GDPR, NIST, and the Gramm Leach Bliley Act (GLBA) require organizations to enforce endpoint protection controls such as least privilege, application control, and detection and response controls, as well as maintain certain reporting and auditing standards.** Proper endpoint privilege management systems will be able to help implement policies, controls, and reporting capabilities to meet these compliance framework standards.

## **Access and Privilege Security Implementation Examples**

All modern operating systems include access and privilege controls. The following examples highlight Windows-specific capabilities for brevity and relevance to most endpoints. User accounts provide the

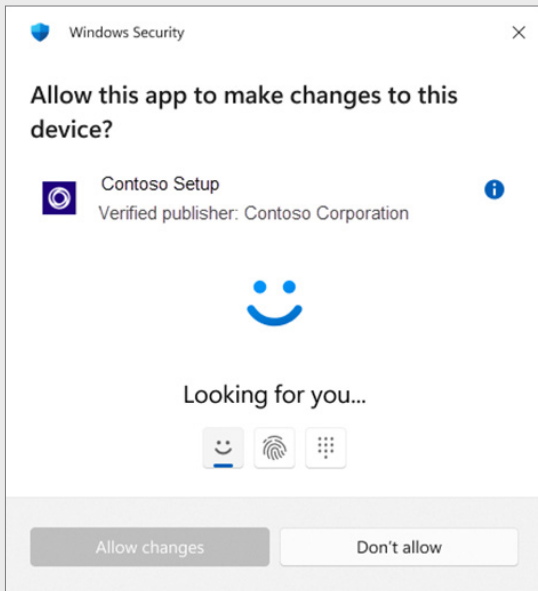
basic focus for access control, though it's important to remember two things:

- A “user” may be a person (e.g., “john@doe.com”) or a service (e.g., “Trusted Installer”).
- User accounts may be subject to controls based on the account name or through membership in one or more groups (e.g., users, administrators, or domain admins, and so forth).

User roles are essential for establishing and using identity, especially when privileges come with such roles. Administrators are a classic example, because they have elevated privileges they need to handle certain tasks (e.g., set up accounts or applications, manage configurations, provision users for specific job roles or tasks, and so forth). In the Windows Active Directory (AD) environment, users or groups may be assigned to specific roles. Each such role defines the resources a member can access, and restrictions that limit such access. In other words, roles determine the privileges granted to a user so they can perform related tasks and functions.

Privileges may be defined in terms of an AD domain (a group of resources and devices under common control) or locally (on a specific named endpoint). This can lead to role confusion. A common issue in AD environments occurs because domain users may get added to the local administrator's group on their endpoint, so they have the privileges necessary to execute daily processes and tasks. This creates a potential gap in security that endpoint privilege management solutions can address, as described in a later chapter.

The key to establishing access is to first establish identity. By then associating an identity with one or more user roles, access may be determined once that identity is authenticated and proven. That process is well-understood, and increasingly, involves modern multi-factor authentication with passwordless options. As an example, in some Windows Insider releases for Windows 11, the OS may be



**FIGURE 1:** In some newer releases, Windows itself will enforce identity checks whenever administrator privileges are exercised

configured for Administrator Protection within the built-in Windows Security facility (see **FIGURE 1**). This requires users to provide proof of identity for any activity that requires elevated privileges.

Modern identity security involves the use of multi-factor authentication, passwordless authentication, and continuous authentication when elevated privileges are used. This prevents hijacking of endpoint sessions from which a legitimate administrator has stepped away. Otherwise, someone else at the helm could obtain unauthorized or unwanted access. Presumably, such third parties will be unable to provide the necessary proofs of identity (time-based one-time passwords, aka TOTP; push notifications, hardware tokens or ID tokens) to successfully undertake such actions should they make that attempt.

Indeed, modern endpoint privilege management needs to be tightly integrated with modern identity providers for continuous user identity assurance. Each time access to risky applications or sensitive resources are requested, or elevated privileges get invoked, the user must provide current proof of identity before the request is granted, or the privilege may be used.

The key here is to seek solutions that rely on open industry standard for the interlocks with identity providers to ensure progress driving strategic IAM initiatives through support for modern cloud-based directories and modern authentication workflows with password-less options.

## Protection from Cyberattacks

---

In addition, access- and privilege-based security can prevent certain cyberattacks that verdict-based methods are not designed to detect or handle. Privilege escalation attacks are a good example. Such attacks seek to obtain access to restricted resources outside the scope of typical user roles. Escalation may occur either horizontally or vertically. Horizontal privilege escalation starts when an attacker takes over some end user account (usually a lower-level, standard account). Such an account serves as a foothold to take over other accounts with the same or similar privileges. Vertical privilege escalation attacks, seek to use a compromised account to take over another account with higher privileges and thereby gain elevated privileges.

When access and privilege security is properly implemented, it enforces the principle of least privilege through intelligent privilege controls—privilege management, application control, and so on. This means that any user account is granted only the privileges necessary for users to do their jobs (to fulfill some specific role). The principle of least privilege can stop escalation attacks before they can snowball. If endpoint privileges are strictly limited, then monitored

for all user accounts, an attacker who takes over any account will be limited in reach and scope. Application control and ringfencing can also prevent exploitation attempts, limit threat actors' ability to gain persistence, and more. Damage will be contained and circumscribed as the attacker keeps running into roadblocks and denials. Likewise, attempts to pivot more laterally can be easily detected.

Intelligent privilege controls can also hinder ransomware attacks. Such attacks often begin with tricks (such as phishing or scareware) to install penetration and attack tools. If an attack somehow evades detection, limiting the scope and reach of the compromised user's privileges insulates underlying system security and configuration data. Endpoint privilege management solutions that include application controls, such as ringfencing, usually also suffice to prevent such software from interacting with command and control servers, limit access to sensitive data, and stop it from spreading to critical resources (e.g., backup servers, a favorite target for ransomware encryption attempts).

Given that Palo Alto Networks' Identity Security Landscape report shows that 96% of human identities have access beyond what is required for their role (excessive or unnecessary permissions) while Unit 42's 2026 Global Incident Response Report shows that endpoints were involved in 61% of all intrusions, such protection is vital. Indeed, 9 out of 10 organizations reported that they've fallen victim to a successful identity-centric breach of some kind. With AI agent identity being the fastest growing segment projected to grow 85%, the attack surface continues to expand rapidly.<sup>1</sup>

This is all while the threat from ransomware remains active and dangerous, with the costs and consequences of successful attacks mushrooming (the median initial ransomware demand surged to \$1.5 million in 2025, and median payments after negotiation came in at \$500,000, illustrating the severe financial risks). No wonder that

<sup>1</sup> Identity Security Landscape 2026, Palo Alto Networks; Global Incident Response Report 2026, Unit 42.

89% of respondents note that cyber insurers are requiring stricter adherence to the principle of least privilege. Endpoint privilege management and access-based security can fill those gaps, as you'll see in the next chapter.

## CHAPTER 3

# Practical Endpoint Privilege Management

**Organizations can start with endpoint privilege management safely and effectively.** They should be sure to apply access and privilege-based security to their endpoints immediately, and adhere to a daily regimen of practical endpoint privilege management principles and practices. Various key activities, configuration changes, and best practices are explained in the sections that follow next.

## Remove Local Administrator Access

A good first step is to remove local administrator access on all endpoints. On Windows PCs, for example, that means moving users and groups from the local administrators group, except for built-in accounts. Exceptions may be allowed, but must be explicitly handled case by case.

The basic idea is that nobody is allowed local administrator privileges, so nobody can abuse them because they can't actually use them. Then, careful use of the right tools allows organizations to define policies (GPOs in Windows-speak) to give users the access they

need. That means the right access to the right resources at the right time, and then only for so long as they need them. This approach helps to simplify and enhance the user experience.

## Enforce the Principle of Least Privilege

---

Remember the principle of least privilege means granting only the privileges needed to perform a specific task or role, and nothing more. This plays directly into Zero Trust model, which never assumes anything about identities that request resources or access: Identity is always solicited, authenticated, and privileges are constantly checked to make sure they still apply.

The principle of least privilege gets its real value from making sure there's nothing in the user's permissions that could allow them to access data or resources that they don't need. Thus, users typically won't be able to perform actions on resources except through authorized actions within applications whose security is known and acceptable. This limits the scope of data and resources available to users and helps contain damage when an attack occurs.

Remember that the principle of least privilege is an ongoing process that comes into play every time a request for access occurs. Continuous diligence follows from tracking and monitoring activity and role changes over time. It also ties directly into auditing and logging whenever users interact with sensitive, private or regulated data such as health records, PII, or protected intellectual property. The primary goal for rigorous application of the principle of least privilege is to avoid what's called "privilege creep"—that is, a growing and expanding collection of privileges that adheres to a user identity as they move around the organization. Proper application of the principle of least privilege means that when a user's role changes, they not only gain new privileges, they also lose their previous ones.

That's how privilege creep gets stopped. Managing privileges to rigorously enforce the principle of least privilege remains an essential feature in endpoint privilege management solutions, if not the most essential one.

## Define Restrictions for Unknown Applications

---

On endpoints, users may attempt to install or run applications or services previously unknown to the organization. The organization must decide in advance whether such unknown applications are blocked by default. They may also decide on mechanisms whereby users may run such applications normally or request their elevation. Endpoint privilege management solutions can help to put a fence around such things, so that they can be blocked from accessing the Internet for example (prevents exfiltration), from accessing credential stores (prevents pre-attack reconnaissance), or from accessing sensitive data (meets compliance and regulatory requirements). In addition, the organization should define workflows wherein they regularly review and categorize attempts to run unknown applications. These might uncover legitimate user needs, or they may reveal possible attack vectors. A good review can help improve user capabilities while stopping potential attacks. A proper endpoint privilege management solution will provide such insights to its management staff.

## Best Practices for Endpoints

---

When working with endpoints, using a secure browser can be critical in protecting them from unauthorized access attempts, privilege escalation attacks, and the rest of the usual destructive privilege-based behaviors. Because so much software can run inside a web browser, a secure browser is an essential tool for maintaining

endpoint security. It can prevent unknown software from running inside the browsers, just as app and application restrictions do likewise on the desktop. It can also block session hijacking attacks, prevent attempts at credential theft, and requests to access data and resources outside the user's scope of permission. To provide defense-in-depth for your endpoints, identity and privilege controls should extend into the browser.

## **Making Endpoint Privilege Management Work for Your Organization**



By putting the principles and practices outlined in the preceding sections to work, you can bring all the useful protection and added security that endpoint privilege management delivers in your organization. In the chapters that follow next, you'll learn more about how endpoint privilege management helps improve your organization's security posture, and strengthens its resilience against breach and attack.

## CHAPTER 4

# How Endpoint Privilege Management Drives Overall Security

**Because endpoint privilege management take an identity first approach to access of all kinds—including on-premises, but also in hybrid and multi-cloud scenarios—it offers organizations improved peace of mind in working with and securing today’s typically multi-faceted and widely distributed digital estates.** Starting with sound and secure human and machine identities, and a strong set of associated permissions available to such parties, this toolset provides a powerful way to prevent attack. Endpoint privilege management goes further, helping to limit the scope and reach of any attack that should actually occur. Given that a fundamental truth of Zero Trust is “Assume you’ve been compromised, and proceed from there,” this is an essential value that endpoint privilege management bring to its users. In the same vein, an endpoint privilege management solution’s ability to monitor and log use of elevated permissions also helps to bridge the gap needed to support identity governance, comply with laws and regulations, and keep endpoints protected. In the sections that follow, you’ll explore how endpoint privilege management solutions boost an organization’s security posture, resilience, and capabilities.

# Identity Is the Cornerstone for Security

---

Identity comes from data that defines a user and associates specific values and special data with providing proper proof that the actor claiming an identity is in fact that very actor. When it comes to identity from a security standpoint, two key questions are

- Who are you? (This is where various proofs of identity come into play, ideally well beyond account name and password.)
- What can you do? (This is where permissions come into play, via access control lists or other similar data structures, that define in granular detail what operations an identity is allowed to perform on the governed object at hand).

Managing application access is becoming an increasingly important activity on endpoints because applications are the gateways into data and resources that users employ to do their jobs. This gets into software guardian technology, which not only manages whitelisted applications it knows about for which it has explicit access controls and permissions. It also applies to unknown applications (which may run in the OS, or inside a Web browser) that might be benign, might be overtly malicious and extremely dangerous. Proper endpoint privilege management includes such technologies, because they are essential to avoiding attempts at lateral moves, privilege escalation, and unauthorized access to resources outside the endpoint user's scope and remit.

Indeed, endpoint privilege management is essential for modern security because so many identities are present but ever-changing. Likewise, the inherent complexity of cloud computing, especially

for cloud native applications, makes the endpoint the key focus for managing access, application, and watching for activities outside the bounds of what's allowed—and safe.

## Key Components of Endpoint Privilege Management

Several aspects are necessary to qualify a solution that purports to deliver endpoint privilege management. In fact, it's arguable that omission of one or more of these must-haves should disqualify a platform from further consideration. Those components are as follows:

- **Managing endpoint privileges:** Remove local admin rights, elevate applications on demand, enforce the principle of least privilege, and report on out-of-bounds or out-of-scope attempts.
- **Credential theft protection:** Secure privileged credentials, prevent harvesting tools (e.g., Mimikatz) from scraping and exfiltrating the credentials.
- **Application control:** Whitelist trusted apps, block unknown executables, isolate risky behaviors with ringfencing, provide mechanisms to run unknown apps in restricted form (or in a sandbox) if users can make the case it's necessary.
- **Just-in-time elevation:** Provide elevated privileges for approved tasks while active. Again, such elevation must not confer across-the-board admin access or status. No privilege creep should be allowed, under any circumstances.
- **Audit & Forensics:** Capture detailed logs of privilege activity for compliance, investigations, and audits.

- **Compliance:** Many regulations and compliance frameworks include requirements for identity and application controls built into endpoint privilege management. They also require audit trails that endpoint privilege management solutions are built to provide on demand.

When it comes to business value, Idira Endpoint Privilege Manager (EPM) provides every one of the preceding key components. Its primary goal is to protect critical resources, including identity, data, applications, networks and resources. To that end, Idira implements a Zero Trust approach that requires verification of identity, validation of permission for each access request, and contextual checks to make sure such requests are normal and allowed within the usual user context, as each request occurs. This helps to security of all identities, while meeting compliance and audit needs and requirements.

## Understanding Adaptive Risk Reduction

Adaptive risk reduction dynamically applies evolving security policies to handle an organization's exposure to risk. Arguably, this is an approach that requires lots of data and subsequent analysis, if not outright AI, to incorporate observed behavior, risk signals, and organizational context to work. Idira EPM uses a layered approach—including its QuickStart policies (see **CHAPTER 5**)—to address known risks, block suspicious activity, and uncover new threats.

Idira EPM's layers include predefined risk reduction policies, role-based access controls (RBAC), and behavioral discovery mechanisms. All these things help administrators fine-tune privilege elevation and application controls. Because it adapts to real-time endpoint activity and user behaviors, Idira EPM decreases the attack surface while also maintaining operational flexibility. This makes Idira EPM the linchpin for modern, identity-aware endpoint security.

Ultimately adaptive risk reduction helps organizations overcome what some security experts call the “binary hurdle”—that is “do something drastic” versus “do nothing.” Its adaptive, context-sensitive capabilities help Security Operations Centers (SOCs) organize timely threat responses, perform recovery and remediation, and implement future blocks or avoidance techniques.

## **WHAT IDIRA ENDPOINT PRIVILEGE MANAGER CAN DO FOR YOUR ORGANIZATION**

Identity has emerged as the final standing perimeter between “us” and “them”—or perhaps more appropriately, between “the good guys” and “the bad guys.” Securing identities properly must come from a defense-in-depth approach with multiple layers of protection for identities, software, resources, and devices. It all comes down to the endpoints, which are both the first mile for user access (outbound) and the last mile for information delivery (inbound).

Idira EPM takes an approach that protects your identities and their permissions. But it also protects other investments you can make in securing and enabling such identities—namely, Endpoint Detection and Response, Endpoint Data Loss Protection, and Unified Endpoint Management.

That’s it for Chapter 4, which explains what Idira EPM does to boost your organization’s security posture and resilience, while it provides a solid safeguard based on securely managing identity and permissions. In the last and final chapter that follows, you’ll learn how to give Idira EPM a try, and where to go to learn more.

## CHAPTER 5

# Getting Started with Idira Endpoint Privilege Manager

It's easy to get started with Idira EPM. You can activate the EPM Rapid Risk Reduction and Least Privilege Framework in QuickStart mode, for immediate out-of-the-box protection. This should instantly improve your organization's security and compliance postures.



### DO THIS!

**During your initial setup**, simply click the "Activate QuickStart" button for instant, immediate risk reduction.

## Rapid Risk Reduction

The QuickStart environment applies a set of predefined policies carefully crafted by Idira's EPM specialists. In a nutshell, those policies do the following:

- Remove local admin rights safely
- Block common attack vectors

- Discover application usage patterns
- Enable role-based access control (RBAC)
- Provide immediate protection without disrupting user workflows

At the same time QuickStart also supports key policy layers, evaluated in the order presented, to ensure granular control and visibility for your organization. Those layers are:

- Exceptions: allow trusted apps to run that otherwise would be blocked
- Risk reduction: block known threats and block elevation for risky apps
- Role-based access: approve necessary actions for specific user roles, including just-in-time elevation where needed
- Discovery: log unhandled events to help drive future policy definitions and changes

In general, QuickStart reduces your organization's attack surface, sets up discovery policies, activates role-based least privilege, and prepares the environment for removal of local administrative privileges.

## Compliance and Auditability

---

Certain regulations require organizations to remove all local administrator rights from every user account. At a bare minimum, you must clearly separate privileged and non-privileged actions between accounts.

Likewise, cyber insurance policies—which many organizations require to demonstrate compliance—impose similar restrictions and limitations. Such policies demand a minimum level of assurance for

cyber risk management. Here again, removing local admin accounts and enforcing the principle of least privilege across the organization is just the starting point.

The Idira EPM QuickStart feature helps achieve compliance by removing local admin privileges across all endpoints. The built-in Policy Audit feature will maintain an audit trail, as it tracks and analyzes all subsequent attempts to elevate any account's privileges. Such audits will reflect your organization's policy usage and highlight suspicious activity.

## Stay Cyber Secure



In this Gorilla Guide, you learned about endpoint privilege management: how it works, and its basic principles and practices. You saw how exactly it fills the gap that other traditional security models often miss. Indeed, Identity Security sees what every firewall, antivirus or intrusion detection will miss—namely, a user seeking to exploit local administrative privileges, or to escalate account privileges.

Finally, this guide made the case for why Idira Endpoint Privilege Manager is an ideal solution that provides comprehensive, in-depth endpoint privilege management by removing local admin rights, enforcing the principle of least privilege, defending against ransomware, boosting visibility with policy audits, and helping to stop credential theft.

To see the platform in action and learn more about how it works, take the [interactive product tour](#).

The threat landscape is ever evolving and increasingly dangerous, so ensure your cybersecurity strategy evolves as well, and closes all doors opened by each new attack vector.

Thank you for taking the time to read this guide and stay cyber secure!

# ABOUT PALO ALTO NETWORKS



Palo Alto Networks (NASDAQ: PANW), the global AI cybersecurity leader, protects our digital way of life with a comprehensive portfolio of cybersecurity solutions and platforms across Network, Cloud, Security Operations, AI, and Identity. Trusted by more than 70,000 customers and powered by Unit 42® threat intelligence, our AI-driven platforms eliminate complexity, empowering enterprises to modernize with confidence and securing the speed of innovation. Explore the future of security at [paloaltonetworks.com](https://paloaltonetworks.com).

# ABOUT ACTUALTECH MEDIA



ActualTech Media, a Future B2B company, is a B2B tech marketing company that connects enterprise IT vendors with IT buyers through innovative lead generation programs and compelling custom content services.

ActualTech Media's team speaks to the enterprise IT audience because we've been the enterprise IT audience.

Our leadership team is stacked with former CIOs, IT managers, architects, subject matter experts and marketing professionals that help our clients spend less time explaining what their technology does and more time creating strategies that drive results.

If you're an IT marketer and you'd like your own custom Gorilla Guide® title for your company, please visit [actualtechmedia.com](https://actualtechmedia.com).