# Definitive Guide™

to

# *Endpoint Privilege Management*

Secure Your Most Vulnerable Endpoints by Putting Least Privilege into Practice


**Allen Bernard**

**FOREWORD BY:**
**Joseph Carson**

*Compliments of:*

thycotic

**About Thycotic**

Thycotic is the leading provider of cloud-ready privilege management solutions. Thycotic's security tools empower over 10,000 organizations, from small businesses to the Fortune 100, 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, DC, Thycotic operates worldwide with offices in the UK and Australia. For more information, please visit www.thycotic.com.

# Definitive Guide™
## to
# *Endpoint Privilege Management*

Secure Your Most Vulnerable Endpoints by Putting Least Privilege into Practice

**Allen Bernard**
Foreword by Joseph Carson

CYBEREDGE
PRESS

**Definitive Guide™ to Endpoint Privilege Management**

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



ISBN: 978-1-948939-17-1 (eBook)

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

## Publisher's Acknowledgements

CyberEdge Group thanks the following individuals for their respective contributions:

**Editor:** Susan Shuttleworth
**Graphic Design:** Debbi Stocco
**Special Help from Thycotic:** Mina Bellamy, Joseph Carson, Erin Duncan, Barbara Hoffman, John Ortbal, Nate Otiker, Chris Smith, and Jordan True

# Table of Contents

**Foreword** ..... **v**

**Introduction** ..... **vii**

Chapters at a Glance ..... vii

Helpful Icons ..... viii

**Chapter 1: Understanding Endpoint Privilege Management** ..... **1**

What is EPM? ..... 1

Components of an EPM Solution ..... 2

The Defining Elements of PAM ..... 4

**Chapter 2: Exploring Privileged Access Management** ..... **7**

The Beating Heart of PAM: Least Privilege Security ..... 7

How PAM Differs from Other Tech ..... 11

**Chapter 3: Exploring Endpoint Application Control** ..... **13**

What is Endpoint Application Control? ..... 13

The Components of Application Control ..... 14

How Application Control Stacks Up ..... 17

**Chapter 4: Integrating EPM into Your Existing IT Security Ecosystem** ..... **19**

How EPM Works with Existing Endpoint Security Tools ..... 19

Exploring What EPM Can and Can't Do ..... 23

**Chapter 5: Common EPM Pitfalls and How to Avoid Them** ..... **25**

The Keys to EPM Success ..... 25

**Chapter 6: Getting Started** ..... **29**

The Lay of the Land ..... 29

**Chapter 7: Selecting the Right EPM Solution** ..... **33**

What to Look for in an EPM Solution ..... 33

What to Avoid ..... 37

So, that's it... ..... 38

**Glossary** ..... **39**

# Foreword

All signs point to 2020 as a year when our view of cyber security underwent a rapid, fundamental shift. One of those shifts has been a growing recognition of the importance of *endpoint privilege management*, now that endpoints have left the office.

In an environment where our workforces are increasingly remote and more reliant than ever on cloud services, endpoints – including laptops, tablets, and phones – have replaced physical office workspaces. As a result, user identity has become the new "perimeter" of cyber security. In that sense, all users (not just IT staff) must be considered privileged users, as privilege is no longer just about authorization but also about access.

The good news is that we can protect our endpoints using a zero-trust, risk-based security model and the principles of *least privilege*.

*Zero trust* assumes that any user or system accessing the corporate network, services, applications, data, or systems must start from a position that assumes nothing and no one is trusted. To gain authorized access, the prospective user must earn trust through verification. For example, a logon can require multi-factor authentication, whereby a user provides an identifier such as a biometric or verifier such as a password, but then the organization must take additional security control steps such as using privileged access security.

Whenever new devices or users are introduced to the network — and before obtaining access to any resources – they must identify and verify themselves based on various security controls. The more sensitive the resources to be accessed, the more security controls they must satisfy.

Cyber security should always begin with zero trust to ensure that only authorized access is permitted. After their identity is verified, users can be classified according to the level of access they need to perform their jobs. That's where the principle of least privilege is applied.

Least privilege enables enforcement of the zero-trust risk-based security model: once a user's identity is verified, access is limited to only what is necessary to accomplish a specific task or job. If any user action requires more access than is granted via policy rules, permissions to elevate privileges must also be strictly controlled and monitored.

My own experience over 25 years in the cyber security industry has convinced me that endpoint security must be executed as seamlessly and simply as possible so users can smoothly access the resources they need. It is crucial to minimize any learning curve for users, make implementation rapid and relatively easy from an IT perspective, and ensure monitoring, management, and maintenance of security solutions are efficient and cost-effective. To be successful, security must be usable.

The endpoint privilege management solution you choose should balance comprehensiveness with usability. As you implement your endpoint security strategy, focus first on the most important and highest-value endpoint security tools that also have the least impact on your users. You can then implement and continually enforce least privilege access gradually across your environment. Once you have your least privilege policies and enforcement in place, you will be able to integrate antivirus, endpoint detection and response (EDR), or endpoint protection platform (EPP) solutions to ultimately develop a comprehensive defense-in-depth posture.

The principles of endpoint privilege management are straightforward, but their implementation and execution represent a significant challenge. This guide provides a strong starting point, with the goal of making your journey more informed and productive.

**Joseph Carson**
**Chief Security Scientist**
**Thycotic**

# Introduction

When it comes to cyber security, one thing is clear: the most potent threat vectors into any organization are its endpoints. And not just any endpoints, but those running Windows, Linux, macOS, or Unix operating systems. These endpoints represent fertile ground for attacks because, more often than not, their users, applications, and services have elevated privileges that give cyber criminals an easy on-ramp to the inner workings within your organization.

But you can fight back. Endpoint privilege management (EPM) is a set of technologies IT security teams can use to automatically contain threats long before they become exploits. It all comes down to applying the cyber security strategy of least privilege. By limiting access to just the functionality each user, application, and service needs to do its job, EPM and least privilege ensure that if malware or a cyber criminal gain a foothold, the threat is eviscerated and the damage contained.

In this guide we explain what EPM and least privilege are, how they work, how they connect to a larger privileged access management (PAM) strategy, and, most importantly, how you can deploy these powerful tools to keep your most vulnerable assets secure.

In a world where cyber crime is an industry, it is critical to use every tool at your disposal to keep your endpoints, data, and networks secure. When combined with a defense-in-depth endpoint security strategy, EPM will keep you one step ahead of the bad guys for years to come.

## Chapters at a Glance

**Chapter 1, Understanding Endpoint Privilege Management,** lays out the three foundational technologies and six defining elements of EPM and least privilege.

**Chapter 2, Exploring Privileged Access Management,** explains how least privilege sits at the core of every EPM strat-

egy and how PAM solutions are used to implement it across your organization.

**Chapter 3, Exploring Endpoint Application Control,** outlines how least privilege is applied to applications and services.

**Chapter 4, Integrating EPM into Your Existing IT Security Ecosystem,** describes where EPM fits in your overall endpoint cyber security strategy and technology landscape.

**Chapter 5, Common EPM Pitfalls and How to Avoid Them,** lays out different strategies you can use for a successful EPM roll-out.

**Chapter 6, Getting Started,** outlines the technologies and processes you will need to begin your EPM journey.

**Chapter 7, Selecting the Right EPM Solution,** lists the features and functions you should look for before signing on the dotted line.

## Helpful Icons


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


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


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


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


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

Chapter 1

# Understanding Endpoint Privilege Management

## In this chapter

- Learn what EPM is
- Understand the EPM lifecycle
- Explore the functional components of EPM

## What is EPM?

When a cyber criminal wants to break into your network, the number one way they succeed is by attacking Windows, macOS, and Linux endpoints. The goal is to steal privileged account credentials that open the door to the device's operating system (OS) and, all too often, the organization's network.


This type of attack is primarily driven by poor password hygiene and users, applications, and services that have unneeded permission (i.e., privileges) to access endpoint and network resources. Even in the most sophisticated IT environments, these privileged accounts reuse the same passwords across multiple systems. People share these passwords, write them down on the proverbial (and often literal) sticky notes, and forget to change default passwords.

Endpoint privilege management (EPM) stops this from happening by enforcing a *least privilege* security posture on all users, applications, and services. Least privilege ensures each of these entities can access only the data, applications, and services they need to function. That's it. It's not fancy, but it is highly effective at keeping exploits contained and your data safe.

# Components of an EPM Solution

As described below, an EPM solution is made up of three essential components that work together to offer CISOs and their security teams comprehensive control over all human and *non-human accounts* that have access to or run on the endpoint.

## *Privileged access management (PAM)*

The idea behind PAM is straightforward. Privileged accounts, e.g., administrator accounts on a Windows laptop, need to be managed so that only those that absolutely require elevated permissions – the ability to perform tasks such as installing new software, accessing an application's full functionality, or running updates – are allowed to do so.


Privileged accounts are everywhere in your organization. They are granted to humans, applications, and services to facilitate the smooth functioning of the organization. But they are often unneeded and, left unchecked, increase the attack surface exponentially, as shown in Figure 1-1.

These excess privileges often lead to *privilege escalation attacks*. Cyber criminals break into one endpoint and then use the passwords found there, and the privileges they provide, to move laterally from the endpoint onto your network. Such attacks are common and highly successful. The goal of PAM is to monitor and control, through policies and direct action, the privileges of each user, application, and service in real time.

A PAM solution utilizes policies, discovers privileged accounts, applies security controls, alerts security teams of suspicious behavior, audits usage, and reduces abuse. By removing or reducing local administrative privileges on endpoints with PAM, you can prevent the majority of attacks from escalating into a major security incident.

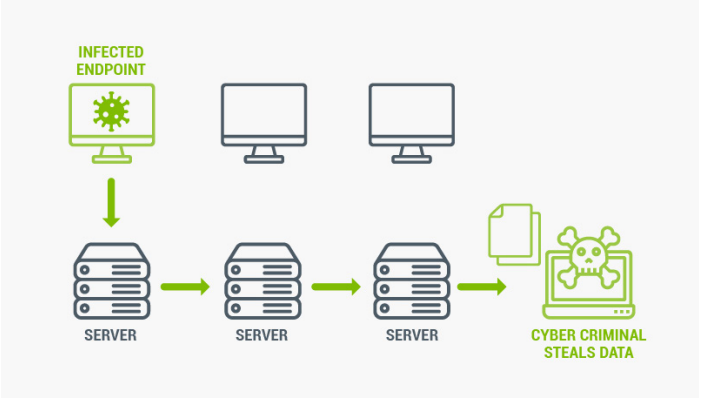


**Figure 1-1:** Cyber criminals move easily from one computer to another.

## *Endpoint application control*

Endpoint application control (EAC), or just application control, applies least privilege restrictions to applications and services by permitting specific processes and applications to run only under predetermined conditions. Application control also allows humans to use the applications they need to do their jobs, even if they do not have local admin privileges on the endpoint.

Applications can run with reduced privileges, meaning even if you have admin privileges, certain applications will run as if you are a standard user. This restriction is used for tools like cmd (aka, command *shell*) and PowerShell to limit abuse of these powerful executables. Application control also allows you to define the services that can start or stop without having to change access control lists (ACLs) or user accounts.


Many common processes, such as installing printers, updating software, and changing system preferences, require administrative rights to operate. If users are required to request exceptions from IT every time an application needs to run a required process, script, or ActiveX control, productivity grinds to a halt.

When desktop support staff are flooded with requests, IT expenses increase and implementation of a robust least privilege endpoint security program across your organization

becomes unattainable. In contrast, because users can continue using the applications they need with no downtime or loss of productivity, application control enables successful, wide-scale least privilege programs.

### *Local account management*

A local account, such as an administrator account on a Windows PC, controls access to a single endpoint. Credentials are stored locally and verified by the host machine when you log in. This is different from a network *domain* account, which grants access to applications, services (like help desk or HR self-service), and data only available via the organization's network that require separate login credentials from the endpoint. Because a single endpoint can have many local accounts, implementing least privilege means controlling the privileges of all of these accounts just as you would the privileges of the primary user, in this case the endpoint's administrator.

This is done by removing accounts from privileged groups such as administrators, Microsoft remote desktop protocol (RDP) users, and management applications, and setting up rules that dictate what accounts can or cannot be added to privileged groups on the endpoint. This prevents group membership changes from being made on the endpoint directly, which would escalate privileges of a new or guest account, for example. It also allows for account password rotation, ensuring that password best practices are automated.

## The Defining Elements of PAM

PAM is composed of the seven essential elements outlined in Figure 1-2. These elements combine to keep users from intentionally or, more likely, inadvertently exposing sensitive data and applications. While each element, such as discovery, can stand alone, when working in concert they form a lifecycle approach to EPM.


When backed up by automation, machine learning, and ongoing cyber security awareness training, the PAM lifecycle creates a self-reinforcing privileged account and endpoint cyber security protection program that is much greater than the sum of its parts.


**Figure 1-2:** The defining elements of EPM and PAM.

## Define

You can't get where you're going if you don't know where you are. That's why every PAM journey starts by defining what least privilege account access means in *your* organization. This includes human and non-human accounts. Defining PAM may be the most time-consuming part of the entire process, as it involves the most stakeholders, and it sets the stage for all that follows. Because you'll be unable to protect every data asset, you must prioritize where the most critical keys to your kingdom reside, who uses them, when, and for what purpose.

## Discover

The discovery portion of PAM is all about uncovering who (and what) has privileges, what those privileges are, why they have been granted, and if they should be. Answering these questions gives you the risk-defined foundation upon which to build the PAM policies that will govern access to resources and functions based on roles, function (in the case of software), responsibilities, and authorization. It also provides a definitive map of how your organization actually works vs. how you think it does. It's like an org chart that also includes applications, services, and systems.

## Manage & protect

Manage and protect is what PAM is all about. Every other element supports this function. PAM automation helps enforce least privilege through proactive management of privileged accounts, password rotation policies, and remote sessions using credentials stored in a *password vault*. For *superusers* like IT admins and privileged account users, PAM can prevent malware from running remote access tools and commands. It provides monitoring as part of the session launchers that admins use to open remote connections. It prevents service account sprawl by implementing proactive service account governance while enabling the automatic elevation of allow-listed application privileges. PAM also provides a way to secure access to on-prem and cloud systems, including IaaS, PaaS, and SaaS.

## Monitor & detect

Monitoring (and recording) privileged account activity enforces policies and uncovers major issues like third-party users with high privilege levels. It also aids in after-incident forensics to help identify root causes and suggest security policy improvements. Incident detection based on AI-driven behavioral analytics and live session monitoring gives security operations center (SOC) teams deep visibility into and control over account activity.

## Respond

Sophisticated PAM solutions give you the ability to trigger alerts and automatic responses to suspicious activity, such as locking down accounts, rotating or elevating credentials, or terminating a suspicious session in real time.

## Review & audit

By utilizing audit trails, out-of-the-box reports, and password vaults to store and encrypt passwords, PAM gives you the tools and reporting capability you need to ace any audit. With more privacy regulations around personal data likely in the coming years, and with cyber security standards imposed by *HIPAA*, *SOX*, and PCI-DSS the norm, organizations will need all the help they can get to stay compliant.

Chapter 2

# Exploring Privileged Access Management

## In this chapter

- Understand common use cases
- See least privilege in action
- Learn about the PAM maturity curve

## The Beating Heart of PAM: Least Privilege Security

As we laid out in the previous chapter, PAM relies on a number of components that work together to form an overlapping system of endpoint protection. This system is based on automated policy enforcement and real-time actionable intelligence about users, applications, and services on systems running Windows, macOS, or Linux operating systems.

What lies at the heart of PAM is the philosophy of least privilege – that users, applications, or services should only have permission to access the accounts, applications, and services that are absolutely necessary to the performance of their jobs or the execution of a function.

Why is least privilege so important? Good question! As Figure 2-1 shows, privileged local admin accounts, or root accounts as they are sometimes called, give unlimited access to the entire endpoint and, by default, any network resources the endpoint has access to.

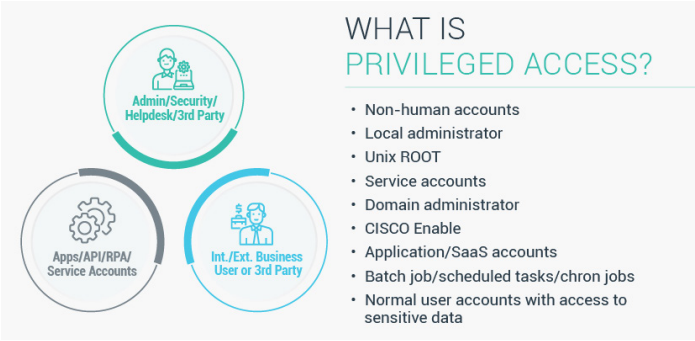


**Figure 2-1:** Privileged accounts take many forms.

If a cyber criminal compromises just one endpoint with local admin rights, they can (and do) use it to access other computers, data stores, domain resources, and critical servers across your network. The networks connected to your network (think third parties such as cloud – particularly IaaS and PaaS – contractors, partners, and suppliers) are also put at risk. This is one of the main reasons why most of all network attacks begin with a compromised endpoint (plus an unsuspecting human victim in many cases). This is why it is critical for any sound defense-in-depth security policy to begin with endpoints and user access.

While everyone in the cyber security world knows that relying solely on perimeter defenses for security is a lost cause, implementing least privilege is a crucial first line of defense. The more rings you have around your corporate castle, the better. If the first wall (i.e., least privilege) keeps the barbarians on the other side of the gates, then the good guys may win the battle before it begins.


Most CISOs have no idea how many privileged accounts are running on endpoints with access to their networks.

## How least privilege reduces threats before they become exploits

Although it's becoming a bit dated, the 2013 breach of retail giant Target is a textbook example of how a compromised endpoint on a third-party network can lead to the pilfering of millions of credit card numbers.

Cyber criminals didn't breach Target's network directly. They didn't have to. Instead, they went after the unprotected endpoints of an HVAC contractor that had unrestricted access rights to Target's network. It was only a matter of time before a keylogger Trojan captured an employee's login credentials. From there, Target's point of sale (POS) system in over 1,700 stores nationwide was compromised, stealing data on an estimated 110 million credit cards as it was being entered.

A more recent – and equally devastating – example is the NotPetya wiperware attack of 2017, which caused billions of dollars in damage to organizations around the globe. In that instance, NotPetya was uploaded via phishing emails and a compromised software update to the popular Ukrainian accounting software, MeDoc.


Once installed, the virus used a modified version of the open-source Mimikatz toolkit to scan the endpoint's RAM for credentials. After acquiring the local admin's cached credentials, it was off to the races. In a matter of hours, NotPetya brought major corporations to their knees. It has been reported that the shipping giant Maersk resorted to paper and pencil to keep its fleet of vessels and ports operational.

In both of these instances, properly implemented least privilege policies and rules would have reduced the risks before they began by denying Target's cyber criminal and the NotPetya virus access to the credentials they needed to escalate the attacks. In the case of NotPetya, the virus simply would have become dormant on the endpoint if it couldn't access any admin privileges stored in the endpoint's RAM.

## *PAM is more than just least privilege*

By now, you've undoubtedly become pretty familiar with least privilege and how it reduces the chance that threats will become exploits. But least privilege is just one aspect of PAM. You need to wrap the philosophy of least privilege with the tools, rules, and policies required to make least privilege effective over the long run and scalable for your entire organization.

There are four phases of PAM maturity: analog, basic, advanced, and adaptive intelligence.

1. Analog phase organizations face a high degree of risk because they apply PAM manually using, dare I say it, spreadsheets. This method is not scalable, nor particularly effective or secure.
2. Basic phase organizations have begun automating these processes but are mostly reactive. They're using password vaults to store privileges but are still relying on password management software more appropriate for consumers than businesses.
3. Advanced phase organizations have moved from reactive to proactive. PAM is a top cyber security priority and they have automation in place to manage most PAM processes. There is a commitment to continuous improvement of privileged security practices, policies, and tools, and the CISO has strong management support and executive buy-in.
4. Adaptive intelligence phase organizations are all in. They take continuous improvement to a higher level by integrating AI to collect data and adapt system rules on the fly. These organizations have automated the entire PAM lifecycle from provisioning and deprovisioning to reporting and automatic password rotation.


Organizations typically have exponentially more privileged accounts than employees.

## Solving common problems

Most organizations today struggle with cyber security because there is no one-size-fits-all solution that can address every possible attack vector, zero-day exploit, or server misconfiguration error. But there are some very common use cases (aka, problems) to which PAM is particularly well suited. Fixing these security holes in your organization will go a long way towards eliminating some pretty obvious and common threats:

- ☑ Shadow IT: system admins have no idea what programs users are running today or their permissions, leading to a lot of potentially dangerous endpoint activity.

- ☑ Changing roles: users require constantly changing endpoint security policies based on new roles and responsibilities. This shifting landscape is very hard to navigate, track, and manage.
- ☑ Visibility: too many users have unnecessary endpoint admin privileges, but IT has no visibility into who these users are or what they are doing with these privileges.
- ☑ Access control: too many users are overprivileged and have unknown membership in local administrator groups, giving them access to systems they do not need.
- ☑ Password management: Overly restrictive password policies lead users to reuse the same credentials over and over on different applications, services, and endpoints.

# How PAM Differs from Other Tech

PAM is a suite of tools that work together to form a solution that is flexible, extensible, and scalable. While each of the technologies listed below plays a role in endpoint security, individually they cannot provide the same comprehensive level of least privilege security that PAM achieves.

## *PAM vs. group policy objects*

Most organizations running Windows endpoints launch their privilege management strategy using Microsoft's group policy objects (GPO). It's free and effective for small organizations with a limited number of endpoints. But its capabilities are limited and inflexible. As organizational complexity grows, groups change frequently, becoming more diverse and often including third-party endpoints that GPO can't reach. Nor does GPO include a password vault, remote session monitoring, an audit trail, or the discovery tools that PAM provides.

## *PAM vs. Windows 10*

While Windows 10 provides a lot of top-tier least privilege security tools out of the box, implementing them requires piecing together and managing multiple systems by hand.

System admins already are stretched thin so this could prove to be a major obstacle to achieving a viable PAM solution. Also, Windows lacks the in-depth application controls, audit capabilities, and automation necessary to make least privilege work at scale.

## *PAM vs. password managers*

Password managers (aka, password vaults) are great but they are just a first step. This is because credentials move throughout the organization – in memory or in a token representing a password hash – and need to authenticate other people and systems. PAM integrates vault functionality so it can establish automatic connections between people and systems without exposing credentials to users. A big difference between PAM and password managers is that password managers still rely on users to manage and secure passwords.


Advanced PAM solutions serve as a proxy to execute administrative sessions and automatically relay the privileged account password from its vault to the target device or application.

Chapter 3

# Exploring Endpoint Application Control

## In this chapter

- Understand application least privilege
- Learn the components of application control
- See how application control stacks up

## What is Endpoint Application Control?

Endpoint application control (EAC), aka application control, applies the concept of least privilege to applications. Many of the processes that users run every day, including installing printers, updating software, and changing system preferences, require administrative rights. Popular conferencing applications like Zoom and GoToMeeting require users to download and launch small executables. And some programs, processes, ActiveX controls, and user-run scripts break if local admin privileges are suddenly removed.

Application control ensures successful adherence to least privilege policies while still allowing users to access and use the applications they want with no downtime or loss of productivity. This is accomplished by temporarily elevating select application privileges as needed, allowing the application to execute on the endpoint.

### How application control contains threats

There are two ways to implement application control: by temporarily elevating an individual user's privilege so they can run an application or access certain application features and functionality; or by elevating the privilege of the application itself. The first approach briefly elevates a user to a local admin or empowers a hidden admin user stored on the endpoint to elevate privileges when required to run an application or service, such as a software update.

Granting IT admin rights, even for a short period, is never a good idea, however. The second approach, elevating application privilege based on pre-determined conditions, is the preferred and most secure method. It ensures users never get admin rights to the endpoint. Also, it is the most scalable strategy to maintain least privilege as your organization grows, individuals change roles, and business needs dictate new types of applications and processes.


During the application review process, pay special attention to applications that require administrative, root, or elevated rights.

## The Components of Application Control

To implement application control, you first have to know what applications are running on which endpoints. This is a monumental task, but not to worry: automated discovery takes care of it for you. Once this critical step is completed, you can apply the below application control functionality to secure the endpoint.

### Allow/deny known applications

After the discovery phase uncovers all the applications that are running, you can begin to add them to allow and deny lists based on your level of trust in the application. (We will discuss this in greater detail in Chapter 6.) To keep deny lists up to date, application control software utilizes threat intelligence databases like VirusTotal and Cylance to separate bad applica-

tions from good ones. Once these determinations are made, you can build and implement, usage policies and enforce them on all protected endpoints en masse using your EPM management console.

Instead of managing each application elevation request individually, which often leads to a huge backup of requests at your helpdesk, most application control solutions elevate requests automatically. This process is seamless to users and requires no input from IT, which helps improve scalability.

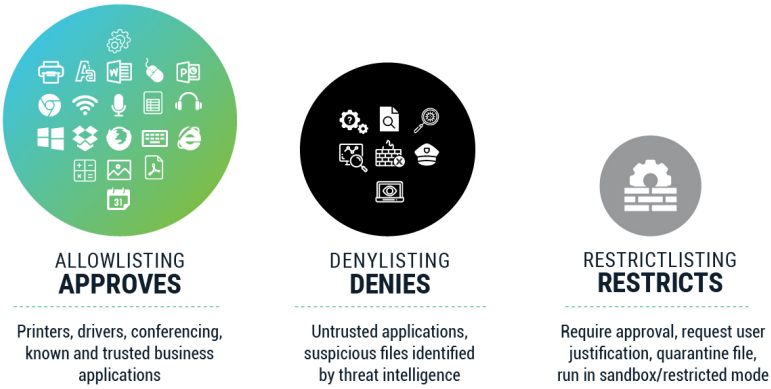


**Figure 3-1:** Allow, deny, and restrict lists.


Allow listing and deny listing are global, top-down strategies set by your IT leadership team.

## Unknown applications

As Figure 3-1 shows, not all applications can be labeled good or bad. That designation can change from hour to hour due to the constantly changing signatures of today's *polymorphic malware*. This is why application control solutions also rely on restrict lists as a way to require approval or user justification and to sandbox unknown applications. Once an application usage policy has been defined and IT has vetted the application, only then can users run them.

Application control also allows system admins to elevate application privileges in a limited way that enables users to do their jobs but does not give them or the application

permission to touch, for example, system folders or the underlying OS. Restrict listing also keeps unknown applications from doing things like looking for updates or accessing a system's desktop, display settings, registry, clipboard, handles, or hooks.

## Policies

Application control tools give you the power to customize policies to match your organizational needs. A good example is only allowing processes to run on certain types of endpoints used by specific organizational groups in select geographic regions or domains during certain times of the day. In that way, if the application tries to run outside of those parameters, it can be flagged as a possible intrusion or malware.

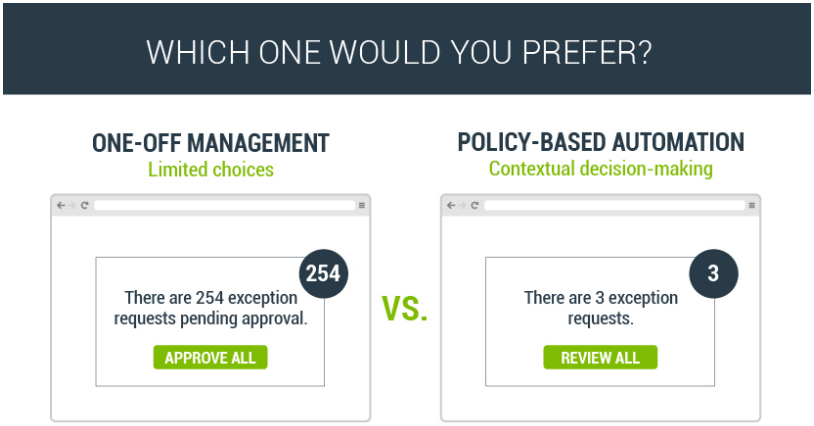


**Figure 3-2:** Which would you prefer? Manual or automated request control?

## Child processes

It is imperative that processes spawned by a parent application, called child processes, do not inherit administrative privileges that would allow them to get around the parent application's least privilege settings. Application control will let you decide whether to allow child processes, such as executing macros within a spreadsheet or Word document, or not.

### *Non-domain endpoints*

Application control also works on your universe of contractor, partner, or other third-party endpoints with network access. By default, these machines are not part of your domain, but they are connected nonetheless and are potent threat vectors. EPM tools should work with Windows and Mac devices, as well as domain-joined and *non-domain*-joined endpoints, to give you more visibility and control.

### *Just-in-time (JIT) escalation*

JIT privilege escalation is an essential part of EPM. It gives IT admins the ability to elevate privileges – but only for a defined amount of time. When privileges are escalated with no time limit, IT admins often forget to reduce those privileges, diluting the effectiveness of EPM defenses. JIT privilege escalation is particularly useful for managing dev and operations teams because they often need to run unknown applications with privileges as they build and test new software.

Although not specifically application control, JIT also can be used to control non-domain endpoints, giving third parties like contractors access to just the network resources they need for just the time they need it.

## How Application Control Stacks Up

When it comes to tech, there is always more than one way to do everything. This holds true for application control as well. Access control lists, for example, have long been used to rein in application privileges. But this old-school method struggles to keep up with today's rapid pace of change and ever-expanding network edge.

More recently, IT security teams have begun to implement network micro-segmentation as a means of boxing in endpoints. Should they become compromised, the damage is limited to the endpoint and data that resides on it. While this approach is highly effective at isolating endpoints on a network, it cannot be applied to a single endpoint. This is because one of the endpoints in the newly created network sub-domain needs to be connected to a network server. Still, it is a sound means to achieving a similar end.

## Application control vs. access control lists (ACLs)

Application control and ACLs serve similar functions: to limit access. But the similarities end there. ACLs are aimed at controlling access to Active Directory objects, which can be individual users, groups, computer accounts, domains, organizational units, or single files or file directories. ACLs use manually configured and maintained Yes/No decision trees to apply access rules to Active Directory objects.

Application control is policy based and can be automated so it can be applied across many systems with consistent results. In contrast, ACLs are complex and hard to manage in large organizations because of the sheer number of Active Directory objects. They also demand a lot of local resources to run; the more complex the ACL, the longer it takes to execute.


Application control works at the kernel level, whereas ACLs work at the file and folder level.

## Application control vs. network micro-segmentation

Like application control, network micro-segmentation serves to control privileged access. Microsegmentation takes the idea of network segmentation to the next level by setting up privileged domains on a network that allow only authorized endpoints to access other endpoints in that domain and nothing more. This approach could, for example, be employed by organizations that use a lot of contractors. Once contractors log into the organization's network, they are only allowed to access certain areas, applications, and data, limiting the potential damage they can do to your organization if one of their endpoints is compromised or their users act maliciously.

Chapter 4

# Integrating EPM into Your Existing IT Security Ecosystem

## In this chapter

- See what systems integrate with EPM solutions
- Learn the layers of strong endpoint security
- Understand the difference between EPM and other endpoint security technologies

## How EPM Works with Existing Endpoint Security Tools

Even though least privilege is recommended as a best practice by Microsoft and other endpoint and OS providers, EPM focuses on those threats aimed at your endpoint's credentials and privileges. As outlined in Figure 4-1, endpoints require a defense-in-depth strategy made up of different tools to create overlapping rings of security. Your endpoints should sit at the logical center of these rings.

EPM works both independently and in concert with these must-have endpoint security technologies to reduce attacks and to help clean things up if they occur. The goal of integrating your EPM tools with these technologies is to make it easier for you to manage the entire security tool stack while enhancing the effectiveness of each component. In this instance, the whole is truly greater than the sum of its parts.

## Anti-virus (A/V)

As perhaps the oldest (and certainly the best known) first line of defense for endpoints, anti-virus tools don't integrate with EPM solutions since they solve for fundamentally different problems. Like endpoint firewalls, A/V software is aimed at spotting and stopping malware at the perimeter, while EPM is all about "boxing in" the endpoint so malware can't escape.

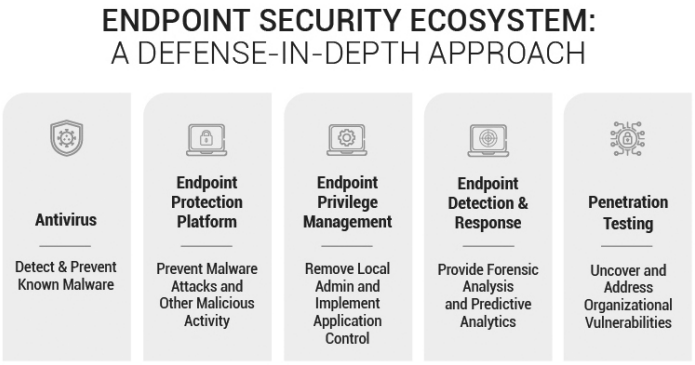


**Figure 4-1:** The key security tools used to secure endpoints.

## Endpoint detection and response (EDR)

By continuously collecting and analyzing data from all endpoints managed by an organization, EDR systems can provide surveillance, alerting, and reporting. The data they collect can be used to monitor current user behaviors and conduct forensic analysis after a breach has occurred.

Like EPM solutions, EDR systems keep exploits that slip past A/V or are launched by an unwitting user contained to the endpoint, denying cyber criminals the lateral network movement they crave.

EDR tools also provide data about endpoint usage that aids in understanding the root cause of an attack and determining if it has expanded beyond the endpoint.


Restricting privileges is the best way to contain and limit the damage caused by a malicious user, aka an insider attack.

## Data loss prevention (DLP)

Fundamentally, DLP is focused on data and EPM is focused on privileges. DLP stops data breaches and leaks using policy-based controls, data encryption, and real-time activity monitoring. It alerts your security teams when red flags appear, such as copies being made or data being transferred to an external drive or USB stick. EPM enables DLP with the appropriate privileges to scan endpoints for sensitive data, thereby increasing DLP success.

Like EPM systems, DLP tools can respond automatically to contain incidents before they get out of hand and provide audit trails in the event a data breach does occur.

## Endpoint protection platform (EPP)

You can think of an EPP as A/V on steroids. These solutions support the same goal of recognizing and stopping attacks by blocking malware before it launches. Advanced EPP solutions rely on many detection technologies, from static indicators of compromise to behavioral analysis, to spot suspicious activity. Like A/V, EPM complements EPP solutions with least privilege capabilities, reporting, and incident response.

## File integrity monitoring (FIM)

FIM is a critical tool in the cyber security tool chest. It is used to make sure that if files (not applications) are changed, alerts are generated, or some other action is taken. FIM tools take regular snapshots of the endpoint and then compare that snapshot with any changes to the file to look for suspicious activity.

FIM also tracks parameters, such as what changes were made, by whom, and when. If it spots anything fishy, such as a sudden change in file size or access by an unauthorized user, the FIM software can alert your IT security team or, depending on the solution, take action itself. EPM solutions, while offering similar functionality when it comes to users, applications, and services, work alongside FIM solutions to keep endpoints safe.

## Reputation engines

Just like A/V software, EPM solutions integrate with reputation engines like VirusTotal and Cylance to perform real-time reputation checks so applications that are known to be malicious can't execute. If an application is not listed and is unknown, your EPM solution can sandbox or restrict list it until it can be vetted by IT.

## Multi-factor authentication (MFA)

MFA is an essential tool for fighting cyber crime. In a nutshell, MFA works to authenticate users by verifying that the person logging into the endpoint is who they say they are. This is done using various methods, such as SMS, RSA tokens, email, or other means, by which the user verifies they are a human (and not a *bot*) by responding to the MFA system in real time, typically by entering a temporary code.

EPM can integrate with MFA tools so users are required to verify their identity before privileges are elevated via EPM tools like a JIT privilege escalation manager.

## System Center Configuration Manager (SCCM)

Commonly referred to as SCCM, this Microsoft tool is used to push out new software, software updates, and patches to endpoints. EPM solutions can integrate with SCCM tools to verify that the new software, patches, and updates your sys admins deliver adhere to your least privilege policies and enable deployment of software updates to use EPM privileges to successfully install.

## Ticketing systems

EPM systems can integrate with ticketing management solutions so that when users ask for privileges to be escalated, that request goes through the existing end user support workflows you've already set up.

### Over privileged and out of control

Organizations have exponentially more privileged accounts than employees. This happens for a lot of reasons: young companies grow fast; M&A drives up the number of endpoints exponentially overnight; proper controls are never put into place or maintained, or the organization's cyber teams haven't given the issue the time and attention it deserves. Another reason is the use of golden images to set up endpoints. With these images, the same hidden passwords find their way onto the stored memory of every endpoint.

Another cause is using Active Directory controls to change a user's status. It's all too easy to add a local user to the wrong group or fail to remove them if their status, role, or employment changes. Or, IT may have elevated a user to an admin status for a one-time request but forgot to change the user's status back. Regardless of the cause, endpoints and users with elevated privileges run unchecked across most organizations even today.

## Exploring What EPM Can and Can't Do

As you've learned by now, EPM gives CISOs and their security teams a way to lock down privileges so that compromised devices cannot be used to launch attacks against the corporate network, act as bots in a *botnet*, exfiltrate data, or carry out other nefarious activities that can harm your organization, its reputation, or your employees.

### *What EPM does well ...*

Properly configured EPM solutions:

- ☑ Keep exploits confined to users' devices
- ☑ Use allow/deny/restrict lists to help control shadow IT and manage application privileges
- ☑ Apply least privilege to human users and non-human applications and services
- ☑ Contain child processes

- ☑ Work across the organization, including on third-party endpoints with network access
- ☑ Stop lateral network movement via privilege escalation and *pass-the-hash* attacks
- ☑ Automate local admin password rotation and group enforcement
- ☑ Serve as a key technology in a zero-trust cyber security strategy
- ☑ Contain insider threats by limiting access to sensitive data and applications
- ☑ Provide real-time application analysis via reputation checking
- ☑ Provide an audit trail for compliance with myriad government and industry regulations and standards
- ☑ Sandbox suspicious applications
- ☑ Reduce the cyber security burden on IT
- ☑ Reduce the burden on help desk personnel

## *And what it doesn't*

EPM can't, however:

- ☒ Protect the data on the endpoint from being exfiltrated
- ☒ Remove malware from an endpoint
- ☒ Manage endpoints remotely
- ☒ Replace EDR, A/V, EPP, or identity and access management (IAM) solutions
- ☒ Quarantine infected endpoints
- ☒ Authenticate users at login
- ☒ Replace endpoint firewalls

Chapter 5

# Common EPM Pitfalls and How to Avoid Them

## In this chapter

- See why maintaining user productivity is paramount
- Understand the keys to a successful EPM rollout
- Learn a few change management best practices

It's simple: any EPM implementation that hinders user productivity will fail. Users will defeat IT every time if the security controls IT imposes are too restrictive. And with easy access to cloud resources and applications that bypass traditional IT processes and controls, there are just too many workarounds available. Therefore, it's critical to create an EPM strategy that restricts user and application privileges without preventing employees from doing their jobs.

## The Keys to EPM Success


Applying the principle of least privilege should be a foundational element of any organization's cyber security strategy. As such, least privilege is not something that can – or should – be set up overnight. It takes planning, collaboration, communication, change management, and the right tools to meet the diverse needs of security teams, IT admins, desktop support personnel, and users.


For the best chance of success, EPM enforcement should operate in the background without users even knowing it's there. This can be achieved manually through resident OS functionality and scripts, but an automated EPM solution will ensure

least privilege policies run with minimal disruption to users and IT. With proper planning, executive support, and budget, users will go about their day unaware their privileges are being actively managed.

## Selective least privilege enforcement

Automation is key to strong enforcement of least privilege. There are many instances where privileges need to be escalated for just a short period. Submitting a help desk ticket to get this escalation is just not practical or desirable.

A commercial EPM solution solves this by defining policies and applying security controls selectively. EPM platforms allow organizations to elevate privilege on demand, offer one-time passwords, and increase and decrease privileges based on dynamic needs, risks, and threats. EPM ensures users and applications aren't over-privileged any longer than they have to be.

## EPM is a process, not a "solution"

Even though the word "solution" gets thrown around a lot in technology circles, in very few instances does a single technology, method, approach, or schema yield all-inclusive results. A successful EPM strategy includes elements like cyber security awareness training for users. It also requires the use of many overlapping endpoint security protection tools like those outlined in the previous chapter.

## Don't ignore the elephant: change management


Change is hard and often unwelcome. Implementing sound change management practices will help everyone in the organization acclimate to your new least privilege environment. Many companies fail at change management for a few familiar reasons: they start too late; they underestimate organizational impact; they outsource the function; or they "bolt on" changes without department-level buy-in. To increase your chances of success, make sure you assign senior leaders with change management experience to this task and hold them accountable.

## Communicate, communicate, communicate

One of the keys to a successful roll-out of your least privilege strategy is regular communication about your intentions, the process, and the reasons for the changes you are making. Managers and users also need to know that support for these changes comes from the top. A sound communication strategy that flows from the C-suite will help accomplish that.


During the early days, set expectations and provide notifications to employees of potential changes, such as popups asking why they want to run a new application or explaining why some existing applications now require admin approval to execute. Your job is to educate users on the value of least privilege – while reassuring them that they can continue to do their jobs securely.

## Integrate into existing workflows

As we've said, to be successful your least privilege policies must have minimal impact on employee productivity. That means adapting least privilege controls to suit your organization's specific needs.

For example, using JIT privilege escalation for exception management is a great way to allow authenticated users to run new applications without having to wait for IT. After a fixed amount of time, those privileges expire and their credentials for that session are retired. Or you can use application control to elevate application rights when specific predetermined conditions are met.


Today's automated EPM solutions offer a variety of ways to make sure that user productivity needs do not take a back seat to security.

## Ongoing training and education

Ongoing cyber security awareness training and education are keys to a successful least privilege strategy. The value of least privilege is best understood in the context of the damage cyber criminals can do. Unfortunately, most organizations fail at this critical task. Too few provide any training for users on privileged access management or the principle of least privilege.

To change this dynamic, take advantage of your organization's workforce development team and budget, if you have one. If not, make formal training a part of your least privilege program to educate both IT professionals and users about least privilege and encourage them to act in the organization's best interest.

## Nothing breeds success like success

To get your EPM program off the ground, start small, do some pilot projects to show it is working and leverage the reporting capabilities of your EPM solution to prove it.

That way, when your CEO wants to know if your organization has dodged the latest malware bullet, you can pull up a report that details how your policies prevented a full-blown attack. To do this, experts recommend you maintain a thorough audit history of what applications were run, by which user, and on which machine.

Based on the audit trail, you can create reports that highlight how many endpoints and applications are protected by least privilege management; how applications are governed by application control; and the type and number of attacks you have prevented.

Chapter 6

# Getting Started

## In this chapter

- Take the first steps on your EPM journey
- Learn which applications require least privilege
- See how the State of Indiana does it

## The Lay of the Land

A sustainable least privilege strategy is not something that can be set up overnight. It takes planning, collaboration, and the right tools to meet the needs of cyber security teams, IT, desktop support, and most importantly, users.

You'll first need to take an inventory of your organization's existing cyber security strategy, the cyber tools already in place, your teams' capabilities, your future plans (like any acquisitions or divestitures), and your organization's overall risk profile and footprint. Once you have the lay of the land, you can begin setting the foundations for rolling out your EPM strategy.


Cybrary offers a great line-up of endpoint security courses at https://www.cybrary.it/catalog/refined/?q=endpoint

### *Identifying critical assets*

You can't protect what you can't see. That's why you have to inventory all of your endpoints to understand who is using them, what applications are running on them, where they are in the world (on prem, in the cloud, in the hands of remote employees or contractors, etc.), and what level of business risk they represent.

To do this, use an automated discovery tool to:

- ☑ Uncover the applications, services, and users that have admin rights
- ☑ Understand what applications need admin rights
- ☑ Identify the employees and developers who install software frequently
- ☑ See who is using legacy applications
- ☑ Surface third-party and non-domain accounts

Even if you have some visibility into the applications that are managed and approved by IT, users are always doing new things and downloading new software, such as SaaS tools, which are not on anyone's lists. Unaccounted-for systems running unknown and unmanaged applications (aka, shadow IT) are among the most common security vulnerabilities. That's why ongoing, automated scanning is required to keep these lists up to date.

## Identifying the riskiest applications and services

Risky applications and service accounts typically have elevated privileges, like access to the endpoint's *BIOS* or the ability to update the OS. These applications are all over your organization. They call home for updates. They back up data, change endpoint settings, schedule tasks, and run batch jobs. They interface with other applications and services to share data and functionality. And they often run in the background, so most users don't even know they exist. To avoid application downtime, service account privileges are often set too high, are never changed, and never expire. These common practices create dangerous vulnerabilities.


Endpoint agents apply least privilege policies at application runtime to grant, elevate, restrict, or deny privileges.

## Identifying the riskiest users

Not all users are created equal. That's why, like applications, they have to be placed into categories based on risk. The

category is determined primarily by the role they play in the organization. Typically, the higher up the food chain, the more risk they represent.

But two groups, in particular, are always super high risk: IT admins and developers. These two groups can't function without very high privileges. Admins run IT so they need access to everything. Developers need unfettered access to new tools and services like software libraries and test environments that mirror production system functionality. IT admins in particular are notorious for sharing and reusing the same passwords within administrator groups. For their part, developers often forget to shut down temporary test environments, leaving open huge back doors into your network.

## Setting policies

To set effective privilege policies that do not hinder user productivity, flexibility is key. Rather than setting simple, blanket policies, EPM allows you to be more lenient in some areas and stricter in others. You can restrict some privileges or application functionality, like running macros, so users can do their jobs, but maintain security by not allowing the application to access any system folders or OS configurations. This approach effectively isolates the system from malicious behavior.


You can find least privilege policy templates online, so you don't have to start from scratch.

## Creating allow/deny/restrict lists

There are three categories into which you will place applications based on risk: low, high, and unknown. Low-risk applications can be added to an allow list. High-risk applications should be immediately placed on a deny list. Applications in the unknown category go on a restrict list so they can be sandboxed and only allowed to run after they have been vetted by IT.

Regardless of risk category, controls should always be in place to limit the application's privileges. Email is a great example of an allow list application that should also have its privileges tightly curtailed, given its position as the number-one threat vector in every organization.


Allow, deny, and restrict lists are great examples of application policies in action. But you can get much more granular than these simple lists using automated application control.

## Finally getting a good night's sleep

By integrating its EPM solution with Active Directory, the State of Indiana ensures that service accounts have the appropriate privileges and are securely managed. The IT team eliminated mistakes by centralizing and automating EPM account creation. And the state now uses EPM to manage privileges for third parties and software developers.

"We used to have shadow sessions … in the middle of the night where we had to get up and share our screen with a developer so they could fix a problem in production," said Indiana's system administrator. "Now I'm able to go in and elevate applications using their user group, and it just automates the process. And that's been a huge, huge value for our team."

The IT staff even set up a simple, form-based process for new application requests that lets them know when users want to run new executables in advance.

"I throw it straight into a policy, I turn it around, I throw it right back at them and say, 'Here you go, you can go ahead and install this stuff. You don't need my help.'"

Chapter 7

# Selecting the Right EPM Solution

## In this chapter

- Learn the elements of a robust EPM solution
- Understand what to avoid in an EPM solution
- See why automation is critical

## What to Look for in an EPM Solution

Above all else, your EPM solution must be usable. Complexity kills, so your least privilege software solution must be policy driven, flexible, and automated. Otherwise, you'll never be able to maintain enforcement and you'll end up with just more *shelf ware*.

From a features and functionality standpoint, look for the following capabilities, so you can achieve simplicity and ease of use without impacting effectiveness or productivity. Make sure any solution you choose is customizable, scalable, and extensible, so it changes to meet your organization's needs, not the other way around.

### *Application restricting and sandboxing*

You need an EPM solution that allows restricting and *sandboxing* of unknown applications. This capability will enable your IT security teams to investigate and vet applications before they run. This goes double when those applications

require admin rights for certain processes like installing updates.

With restrict lists, you can elevate application privileges so users can do their jobs without allowing the application to touch any system folders or underlying OS configurations, registry files, or settings. You can also require IT approval or user justification prior to elevating the application.

With endpoint sandboxing, even if a malicious application does execute, damage will be contained on the endpoint. There is no access to privileged credentials that could allow a threat actor to progress laterally across your organization via a *privilege escalation attack*.

## Management of non-domain endpoints

Your network extends well beyond the borders of your organization today. This will not change. In fact, the "edge" of the network, already porous, will become non-existent in the coming years. A robust EPM solution must allow you to extend least privilege to non-domain endpoints. Because these machines are not joined directly to a domain managed by your IT department, they are potent threat vectors into your organization.

## Integrated threat intelligence

There are literally hundreds of millions of new exploits and variants released into the wild every year. That's why your EPM solution must utilize threat intelligence to perform real-time reputation checks for all unknown applications. This will keep your allow, deny, and restrict lists up to date and your employees productive and safe.


Make sure your EPM solution can scale as your organization grows.

## Integration with common ITSM tools

In the interest of making your EPM solution as easy to use as possible, it should integrate with your IT service management toolset. Look for a solution that integrates with popular ITSM platforms like ServiceNow so support requests and

IT responses can be managed, tracked, and reported via the ticketing system itself.

## Automated discovery

With so many privileged accounts spread across your organization, there is simply no way to find them all on your own – no One Ring, as it were. Spreadsheets of privileged accounts become outdated as soon as they are written. Canvassing every endpoint using tools like those available in Windows and Active Directory only gives you a one-time snapshot into domain-attached accounts.

Look for an EPM solution that automates the privileged account discovery process. This way, all privileged accounts on all endpoints are continually surfaced as roles change, people come and go, and assets and applications are added and removed.

## Automated reporting and analytics

Today, almost all boards of directors are demanding accountable action to stop cyber security threats. Your organization's compliance teams also need insights into these efforts. Spreadsheets don't cut it. They are hard to work with and can't provide the timely answers people are looking for. Dashboard-based automated reporting and analytics are key to keeping strategic decision makers informed and for tracking the effectiveness of your EPM strategy.

## Automated privilege elevation

For an EPM solution to be successfully adopted en masse, the vast majority of application elevation requests must be managed automatically. Because of the granular, contextual policies put in place at the beginning of the process, most applications are either approved or denied without any work from IT. This leaves only specialized or custom applications for hands-on review and approval by your security teams – shrinking your queue and creating more time for other priorities.


Training and education are key so that security risks are made clear and the value of least privilege solutions is apparent.

## Multiple deployment options

This one's pretty straightforward: look for EPM solutions that can be deployed on prem, in the cloud, or as a managed service, based on your organizational needs.

## Regulatory compliance

Your EPM solution must demonstrate compliance with multiple requirements from a variety of regulations, such as PCI-DSS, HIPAA, and SOX, which require least privilege to ensure system security. Your solution should align with the specific compliance standards your organization must meet.

## Child process control

Child processes are easily overlooked because they execute from within a file, such as a PDF or Word document. But they are frequently used to deliver malware to an endpoint. Look for an EPM solution that allows you to prohibit execution of child processes to ensure unknown executables don't run.

### Eyes open and head up

Because EPM can fundamentally change not only your approach to cyber security but the relationship your employees have with IT and their jobs, you have to go into your EPM journey with your eyes open and your head up.

It starts by modifying your EPM strategy to fit the needs of your organization and then educating users on how least privilege will empower them to do their jobs without putting the organization at risk. You can also stress that this approach means they will no longer have to worry if they are doing something they shouldn't with unapproved software and services.

It also means communicating the value of least privilege and engaging in a robust change management process, so employees feel like part of the solution, not the problem. If you don't, then, like so many big initiatives before, EPM could well become just another control that employees actively undermine and work around. With the plethora of cloud tools at the ready and discretionary budgets in every department just waiting to be spent, this is easier than ever.

Because "complexity kills," your EPM solution must be simple and policy driven. Otherwise, you'll never be able to maintain enforcement. But even with automated, policy-driven solutions, you should expect some manual policy maintenance. Give administrators the flexibility to set and update policy rules as needed and appropriate.

# What to Avoid

All technology solutions are incomplete. That doesn't mean they are ineffective. However, design decisions early in the build process can lead to end-product limitations that will hamper your ability to secure your organization. Therefore, it is important to avoid solutions that are narrowly based on just Active Directory or GPO.

## *Dependence on Active Directory*

It is critical to deploy an EPM solution that integrates with Active Directory or Azure Active Directory as its identity authentication and authorization service – but does not depend on it. Some least privilege solutions that rely solely on Active Directory only enforce least privilege on new accounts or those that are active at the time of implementation.

This means local users can be added and re-added to a local administrator group without the EPM tool's awareness or ability to fix the privilege creep this represents.

Look for solutions that import users and groups on an ongoing basis so you can assign one or more Active Directory users to a privilege manager role, such as an admin, or have privilege levels automatically assigned, elevated, or reduced.

## *Dependence on GPO*

With Microsoft's Group Policy Object (GPO) you can set local account password requirements, but you cannot automatically set, retrieve, or rotate local admin credentials. With EPM solutions that are reliant on GPO to manage passwords, the burden for creating, remembering, changing, and sharing passwords falls to IT.


Your IT admins are often the worst at properly managing passwords.

Another issue is that GPO doesn't work with centrally secured and managed password vaults for local accounts. Because of this, IT admins can't remotely monitor sessions, require check-out, or execute other advanced features that lower the risk of privileged credential abuse.

By relying on GPO for enforcement, you lose the ability to create granular policies for application control. Therefore, every time users need to access an unapproved application, they have to ask IT for permission. Also, there is no management or automation of those privileged credentials once they're in the wild.

## So, that's it...

At this point in your EPM journey you should understand the basics of least privilege and how you can apply it in your organization. As part of a zero-trust cyber security framework, least privilege acts as a cornerstone technology that, when combined with an defense-in-depth endpoint security strategy, will let your CISO and everyone else in the C-suite sleep better at night. The best security solution is a usable security solution.

# Glossary

**BIOS:** Basic input/output system. BIOS is firmware used by the computer at startup to enable basic functionality like keyboard, monitor, mouse, and other hardware, as well as services like the system clock, before the operating system is launched.

**Bot:** An autonomous program, typically malicious, which can interact directly with systems, applications, or users.

**Botnet:** A group of computers taken over and used by cyber criminals to launch attacks, send out spam, act as proxies, and propagate viruses, worms, and Trojans.

**Domain:** A group of Windows computers with one or more acting as a server, called a domain controller, which is used by network administrators to manage the other computers in the domain.

**Endpoint Privilege Management (EPM):** The process of actively managing the privileges (aka, access rights or permissions) of users, applications, and services on endpoints that run Windows, Mac, Linux, or Unix operating systems.

**HIPAA:** The Health Insurance Portability and Accountability Act of 1996, which created U.S. national standards to protect sensitive patient health information.

**Least privilege:** In cyber security, the concept of limiting user, application, and service access to privileged accounts to only what is required through various controls and tools without impacting productivity.

**Non-domain endpoint:** An endpoint that is not part of a defined Windows domain but has access to your network.

**Non-human account:** An account used to run services or applications.

**Pass-the-hash attack:** A type of attack that relies on stealing the stored hash of an IT administrator. When computers store plain text credentials in memory, they do so using a hash, a mathematical version of the password, instead of the password

itself. Once an attacker acquires the hash, they can move about the network using it, instead of the actual password, to gain entry into systems and data stores.

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

**Polymorphic malware:** Malware that constantly changes its characteristics to evade detection.

**Privilege escalation attack:** Access by a cyber criminal to elevated privileges, such as those of a system administrator, to launch an attack, steal data, or learn more about the organization's network while remaining undetected.

**Sandboxing:** Using a sequestered area set aside and isolated from the main system to safely launch and run suspicious applications and check for malware.

**Shelf ware:** Applications or software that are purchased but never used to any great extent.

**Shell program:** A powerful program that allows humans to communicate directly with the endpoint's operating system through a command-line interface.

**SOX:** The Sarbanes-Oxley Act of 2002, which cracks down on corporate fraud.

**Superuser:** Someone who has system administrator-level privileges.

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

thycotic

# How many of your users have local admin privileges?

## Find out with Thycotic's Free Least Privilege Discovery Tool

A simple first step to implementing endpoint security and a least privilege policy. A quick scan of your environment indicates which accounts may be overprivileged and, therefore, vulnerable to insider threats and malware attacks.

**DOWNLOAD NOW:**
**www.thycotic.com/leastprivilegediscoverytool**

**Discover how endpoint privilege management dramatically reduces your cyber security footprint by empowering a zero trust approach to your most vulnerable assets.**

Because over-privileged endpoints are a prime target of an organized, for-profit malware industry that pumps out hundreds of millions of new variants every year, CISOs need to deploy every tool they have to combat this scourge. Among the most effective tools is EPM. By automating the rollout and management of privileged access, EPM stops cyberattacks before they start.

- Explore the concept of least privilege — learn how least privilege prevents attacks and contains them if they do
- Learn the different components of EPM — explore the many tools in the EPM toolset
- See how EPM fits into your endpoint protection strategy — learn why EPM is just one component of a robust defense-in-depth endpoint protection strategy
- Uncover common pitfalls — learn how to deploy EPM so everyone benefits and no one is left behind
- Get started with EPM — discover the first steps you'll need to take on your EPM journey
- Learn the essential elements of EPM — uncover the must-have features and functions of every EPM solution

***About the Author***

Allen Bernard is a veteran technology journalist, editor, and content creator. He has written, assigned, and edited thousands of articles focused on the intersection of business and technology. As well as developing books and content for some of the world's best-known brands, he has written for TechRepublic, TechTarget, CIO.com, the Economist Intelligence Unit, and NetworkWorld.

CYBEREDGE PRESS

Not for resale

ISBN 978-1-948939-17-1