WHITE PAPER

A GUIDE TO ENDPOINT PRIVILEGE MANAGEMENT

Learn about least privilege and discover the business benefits

BeyondTrust

SYNOPSIS

BeyondTrust is the worldwide leader in Privileged Access In this whitepaper you will learn what endpoint privilege management is and how an effective approach significantly enhances an organization's security against rising cybercrime. We cover the origins of the least privilege concept, the benefits of application control, the current cyber threat landscape and how endpoint privilege management works to combat this seamlessly and with minimal disruption to user productivity.

We will also take a closer look at deployment offerings, including both on-premise and SaaS (Cloud) - providing you with a comprehensive understanding of the benefits and ease of rolling out an EPM solution in your organization.

TABLE OF CONTENTS

1 Understanding the Cyber Security Landscape

To better understand the role endpoint privilege management plays in the wider security landscape, we must first understand the current cybersecurity climate. Before we delve into how it works and what the benefits are, let's look at some of the most recent and credible industry research in order to paint an accurate picture of the landscape in 2019 and beyond.

McAfee Labs

In its December 2018 Threat Report, McAfee Labs identified 63 million new malware samples – a record high.1 As a result, the total count in their sample database has now surpassed 837 million.

Raj Samani, McAfee's Chief Scientist, explained that "attackers continue to benefit from the dynamic, benign capabilities of platform technologies like PowerShell, a reliable recklessness on the part of individual phishing victims, and what seems to be an equally reliable failure of organizations to patch known vulnerabilities with available security updates."

In the Threat Report, McAfee drills down into the most vulnerable sectors when it comes to cyber-attacks. While the overall number of reported incidents fell by 12%, Public Sector incidents rose by 150% since the previous quarter, and Finance rose by 64%.

Other key takeaways from McAfee's December 2018 Threat Report include the fact that new JavaScript malware continued to rise throughout 2018 and isn't showing signs of slowing down. Globally, mobile malware increased by 46% last year, reaching 24 million samples, and ransomware samples grew by 45% to surpass 18 million.

It is evident that cybercrime is still on the increase, with criminals leveraging new and harder to detect methods of committing a breach. When you consider that 80% of security breaches involve privileged credentials, the danger of admin rights cannot be ignored.

> *The $100 billion growth in cybercrime is due to cyber criminals quickly adopting new technologies, the ease of engaging in cybercrime— including an expanding number of cybercrime centers— and the growing financial sophistication of top-tier cyber criminals.*
>
> **ECONOMIC IMPACT OF CYBERCRIME, NO SLOWING DOWN, MCAFEE, FEBRUARY 2018**

Figure 1: Malware Statistics 2016-2018 (McAfee Labs Threat Report Dec. 2018

2 The 'Least Privilege' Concept

In order to determine the effect of endpoint privilege management solutions in the fight against cyber attacks, we must first consider the underlying security principle of least privilege.

Having local administrator rights means a user has privileges to perform most, if not all, functions within an operating system on a computer. These privileges can include such tasks as installing software and hardware drivers, changing system settings, installing system updates. They can also create user accounts and change their passwords. While many organizations assign local admin rights to ease the need for IT Support, they are leaving themselves at high risk of a security breach.

A common approach to managing privileged user accounts, the least privilege model is the practice of assigning users and programs the least amount of permission required to complete specific tasks.

> *Organizations should exercise the principle of least privilege for local administrative access. The vast majority of users do not require local admin access in the modern Windows OS. When an application or service requires administrative privilege, the end user should log on as a standard user, and privilege should be elevated according to policy.*
>
> **REDUCE ACCESS TO WINDOWS LOCAL ADMINISTRATOR WITH ENDPOINT PRIVILEGE MANAGEMENT, OCTOBER 20, 2017**

The least privilege concept is not a new phenomenon. It was born in October 1974, when Jerome H. Saltzer and Michael D. Schroeder submitted a paper entitled 'The Protection of Information in Computer Systems.' The paper explores the mechanics of protecting computer-stored information from unauthorized use or modification and, in doing so, outlines the earliest design principle of least privilege:

"Every program and every user of the system should operate using the least set of privileges necessary to complete the job. Primarily, this principle limits the damage that can result from an accident or error. It also reduces the number of potential interactions among privileged programs to the minimum for correct operation, so that unintentional, unwanted, or improper uses of privilege are less likely to occur."

Although the least privileged approach was conceived over 40 years ago, it remains the fundamental security measure for organizations looking to mitigate against the growing number of malicious attacks. This is primarily achieved by removing local admin rights from users.

Least privilege works most effectively when combined with the concept of application whitelisting. Whitelisting is the practice of specifying an index of approved software applications that are permitted to be present and active on a computer system. The goal of whitelisting is to protect computers and networks from potentially harmful applications.

An efficient solution will set a handful of broad rules based on trusted application types, automatically stopping unapproved applications from running. The integration of these two approaches is where endpoint privilege management comes into force.

Methods of achieving least privilege have evolved somewhat since the concept's inception, as users look for ways to implement best practices, and make deployment easier than ever and deliver rapid time-to-value.

As such, it is now possible to take significant steps towards a least privilege environment via software-as-a-service (SaaS) based solutions, which delivers all of the above benefits from the cloud as a subscription model. This something we will cover in more detail in the next section.

3 What is Endpoint Privilege Management?

Endpoints are devices where users log on - Windows or Mac computer systems, laptops, desktops, and even servers - and applications run. Endpoint privilege management technologies allow organizations to control exactly what actions can and cannot be performed by any given endpoint.

In many organizations, some (or all) users have full administrative rights, which enables them to execute unknown applications. This means that malware can run with elevated privileges, security controls can be bypassed, and software can be installed and executed with no control or visibility.

Organizations tend to assign local admin rights to company-wide employees in order to ease the headaches for IT Support and productivity losses. In doing so, they've placed their company's confidential data at a high level of risk, putting it on a plate for any able hacker to steal.

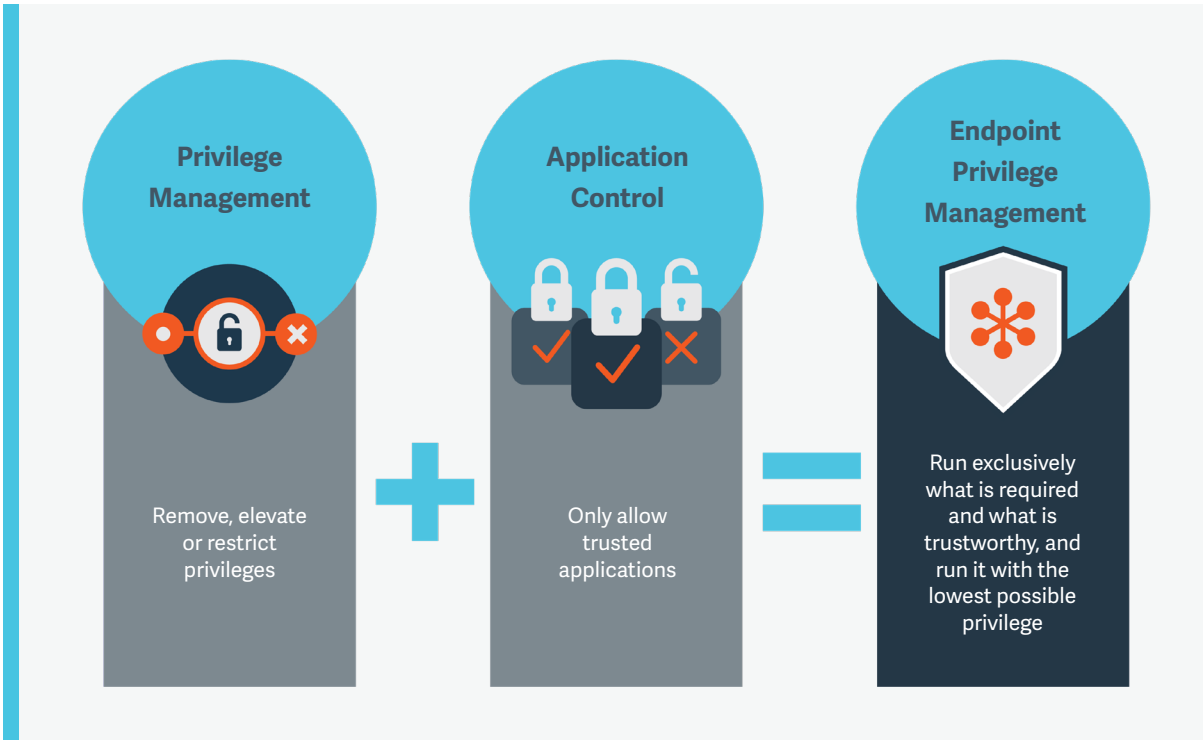

Figure 2: Better Together, Privilege Management and Application Control

In her whitepaper, Gartner Analyst Lori Robinson clearly defines endpoint privilege management as the combination of privilege management and application control:

"Endpoint privilege management (EPM) technologies combine application control and privilege management to ensure that only trusted applications run, and that they run with the lowest possible privilege. With EPM, organizations can remove local admin access with minimal impact on end users."

"By utilizing on-demand privilege elevation, EPM automatically provides users with the privileges necessary to run trusted applications and carry out authorized tasks. Self-service, workflow and self-elevation features further protect and enable end users by empowering them to get access to operations for which they were not previously approved."

According to Gartner, endpoint privilege management "utilizes privilege management and application control to determine first, whether an application can run, and second, how (under what privilege conditions) it can run."

Endpoint privilege management is the process of allowing your employees enough access to remain productive in their roles, without giving them full administrator rights over your IT system.

Access is given on an application basis, rather than on a user basis. This means that employees are not granted permissions for more than, and crucially less than, what is required of their role.

Using Endpoint Privilege Management to Prevent Attacks

Application control and least privilege prove an effective combination in the prevention of malware.

In Architecting Privileged Access Management for Cyber Defense, Gartner Analyst Homan Farahmand highlights that "the privileged access threat landscape is growing with a higher risk of enabling cyber attacks and severe consequences. Technical professionals must architect privileged access control capabilities to defend against exploitation scenarios and to resist advance persistent attacks."

Gartner's Lori Robinson explains that "If abused or misused, local admin access can result in compromised security, loss of data, high support costs and poor user experience... users with unfiltered local admin rights have full control of the endpoint, including the ability to:

- Install or run unauthorized processes or applications
- Install malware that exploits privileged access (intentionally or not)
- Disable security and system settings
- Perform file system changes
- Change standard desktop configuration setting"

And while local admin rights may not be as powerful as domain or server-level privileges, it does not mean they can be ignored. Attackers can exploit local admin rights to gain access to further network controls (like domain or application access).

> *Excessive employee access is one of the fastest growing unmanaged risks for organizations and it's because most organizations don't know where to start.*
>
> ROBERT HERJAVEC, CEO AND FOUNDER OF HERJAVEC GROUP

The most recent Microsoft Vulnerabilities Report revealed that, on average over the past five years, 83% of all Critical Microsoft vulnerabilities discovered could have been mitigated if admin rights were removed.

Finding & Implementing a Solution

Endpoint privilege management is vital to a company's security stack but is historically perceived to be challenging to deploy and without due consideration, can result in a higher volume of IT support desk calls as users encounter issues accessing documents or applications they need.

In a recent study of nearly 200 security professionals across multiple sectors, 61% of respondents either already had an EPM solution in place, were preparing to implement one, or expressed that EPM would be a good fit for their business' security needs.

Gartner's Robinson highlights that "Reducing access to local admin rights is one of the best things you can do to improve Windows security. However, balancing access restrictions with user experience is a challenge that many users fail to get right."

Exception handling capabilities are crucial to ensuring that users remain productive, even in the context of a standard user account.

A popular method of handling new and unknown requests is offering up a simple code prompt, and the user is required to ask IT Support for an authentication code to continue. This provides an extra layer of security, as the IT professional is then able to determine whether such action presents a level of risk, or if the action should in fact be whitelisted for the future.

"Endpoint privilege management technologies can be used to seamlessly elevate, manage and control users' access. The most lightweight solution for Windows privilege management is the native User Account Control (UAC), but it lacks the fine-grained controls and reporting capabilities of other commercial EPM solutions."

4

Leveraging EPM from the Cloud (SaaS)

Deploying Endpoint Privilege Management from the Cloud makes it even easier for customers to eliminate unnecessary privileges and stop malicious attacks by enforcing least privilege on their Windows and Mac systems.

A competent SaaS-based EPM solution can deliver the same high availability, security, access, and scalability of an on-prem offering, while removing the overhead of managing infrastructure.

For organizations looking to reduce privileged access risks without adding administrative and financial burdens on their organization, SaaS solutions feature rapid deployment and make managing privileged access easier and more cost-effective. A SaaS offering is available in a subscription model, allowing customers to pay only for what they need and allow it to expand with their business.

In the aforementioned study, when asked whether a SaaS Solution for EPM would be an attractive prospect, 58% of respondents agreed, while 33% said it would make no difference to them.

The top six reasons that were cited as benefits of a SaaS EPM solution included:

- Improved ease of management
- Better scalability and more flexible
- Improved end-user experience
- Enhanced productivity/efficiency
- Reduced workload for IT Staff
- Solution will be updated more regularly

> *If the least privilege principle was well implemented and the user does not use admin privileges for daily work, the attacker would have to put in much more effort to escalate privileges and perform traversal movement to other machines.*
>
> PAULA JANUSZKIEWICZ, CYBERSECURITY EXPERT

5

Introducing Endpoint Privilege Management by BeyondTrust

With our Endpoint Privilege Management solution, you can eliminate unnecessary privileges and elevate rights to Windows, Mac, Unix, Linux and network devices without hindering productivity.

We've combined best-in-class privilege management and application control, making admin rights removal simple to ensure compliance, security, and efficiency. It deploys in hours and leverages more than two dozen validation criteria to elevate applications securely and flexibly, and elegantly scales to meet the demands of even the largest and most complex organizations. A powerful rules engine and comprehensive exception handling features help minimize the impact on end users and IT teams alike.

Six key features of our Endpoint Privilege Management solution include:

1. **Achieve Least Privilege**

   Elevate privileges to applications for standard users on Windows or macOS through fine-grained policy-based controls, limiting attack surfaces by providing just enough access.

2. **Seamless Application Control**

   Deliver trust-based application whitelisting, with a flexible policy engine to set broad rules, choose automatic approval for advanced users - protected by full audit trails - or utilize challenge-response codes.

3. **Auditing & Reporting**

   Provide a single, unimpeachable audit trail of all user activity, speed forensics and simplify compliance with complete reporting for multiple stakeholders.

4. **Privileged Threat Analytics**

   Correlate user behavior against asset vulnerability data and security intelligence from best-of-breed security solutions to provide an overall picture of end-user risk.

5. **Flexible Deployment Options**

   With both on-prem and SaaS offerings, users have a choice of deployment methods to suit their unique needs and adapt as they grow, without the need to compromise on feature offerings.

6. **Security Ecosystem Integrations**

   Built-in connectors to third-party solutions, including help desk applications, vulnerability management scanners, SIEM tools, and more, ensure rapid time to value and return on security investments.

This is by no means an exhaustive list, but Endpoint Privilege Management can mitigate the following attack vectors:

- Installation of spyware and adware
- Access to data belonging to other users
- Replacing OS and other program files with Trojan application
- Disabling/uninstalling anti-virus virus
- Creating and modifying user accounts
- Resetting local passwords
- Rendering the machine unbootable
- Exposure of entire networks to malware, viruses, and denial-of-service (DOS) attacks
- Data corruption or manipulation
- System wide configuration changes
- Leakage of sensitive data
- Disabling security features/products

If a comprehensive endpoint privilege management solution is applied, then not only will the above threats be mitigated, but productivity will not be compromised in the process.

6 Additional Benefits of Endpoint Privilege Management

The key benefits that come with endpoint privilege management include mitigation of internal and external threats, assistance in meeting compliance requirements, and significantly improving operational efficiency.

Aside from these primary benefits, there are several other positive effects that come with deploying BeyondTrust's Endpoint Privilege Management.

1. **Extra Visibility of Privileges**
   An effective solution will ensure that you have control and visibility over activities within your business. You see which applications are being used and installed, which tasks and applications require privileges, and how many users are running with local admin rights. Enterprise reporting capabilities assist with visibility and auditing. Graphical dashboards and reports with drill-down options provide fast access to as much detail as you need.

2. **Legacy Systems/Applications**
   Old software and outdated applications create vulnerabilities and are used as a target for hackers, particularly where admin rights are needed for them to run. According to Kenna Security's Remediation Gap report, most companies take an average of 100-120 days to patch vulnerabilities, and many companies have critical vulnerabilities that go unpatched altogether. Endpoint Privilege Management by BeyondTrust allows you to create pragmatic whitelists to manage trusted applications and block unauthorized or old versions of software.

3. **Remote Workers**
   Home or mobile users typically require flexibility to change settings, install software and update applications regardless of their location. Having a policy approach based on low/medium/high flexibility allows you to grant the privileges needed based on job role, ensuring productivity and security.

4. **Third Party Access**
   Granting admin rights to external users is a security risk. A well-developed endpoint privilege management solution ensures third parties can just do the job they need to (on only the servers required) using approved applications and processes, during a specific timeframe, from an approved location.

7 How to Deploy an Endpoint Privilege Management Solution

Traditionally, deploying an endpoint privilege management solution has taken months. Configuring the solution to fit an individual organization's needs has been a laborious task, requiring large amounts of implementation effort. By leveraging years of deployment scenarios, BeyondTrust have created out-of-the-box workstyles to cover the majority of enterprise requirements.

This means that you can operationalize Endpoint Privilege Management overnight to make quick security gains that can be refined over time. This secure baseline allows you to significantly move up the security scale without impacting user productivity. No other product can offer this level of convenience, flexibility, and speed during deployment.

The Quick Start policy allows organizations to apply three common workstyles, depending on the necessary flexibility of the role:

Low flexibility (i.e. interns, temps, contractors)
Users are presented with a 'challenger-response', meaning that they must enter an IT-generated PIN code. This allows a relevant and knowledgeable IT professional to verify any software installation or system change as being high or low risk beforehand.

Medium flexibility (i.e. front-office, sales)
With medium flexibility, authentication is required – meaning users must provide their credentials in order to install applications. This helps to add an extra security layer between potentially harmful installations and your network.

High flexibility (i.e. engineering, IT, QA)
The most flexible of all workstyles, these users or given a prompt to simply provide a business reason to install applications or make system changes. Their role requires such access in order for it to be adequately performed.

BeyondTrust gathers accurate user behavior data, with trend analysis to identify which applications require elevated privileges, which are executing from within the user's profile area, and which are being installed. Then this data is used to build tailored workstyles that fit your enterprise, as you continue to refine your deployment. This means you only need to elevate the applications each user requires, ensuring that only trusted applications are able to run.

8 Summary

Hopefully this whitepaper has shed some light on how endpoint privilege management works, highlighting the quick-return and long-term benefits it gives to organizations large or small. While the term itself is relatively new, the concept has been around for some time - making it a widely used, tried and tested method.

By combining privilege management and application control, Our Endpoint Privilege Management solution can help organizations to minimize the risk of a security breach, without minimizing productivity. If you're interested in learning more about how BeyondTrust can help you manage and monitor your privileged accounts, sign up for a free demo today.

9 Next Steps & Resources

By addressing unmanaged admin rights, you can quickly achieve endpoint security while eliminating security gaps and meeting compliance requirements, without hindering user productivity.

Contact BeyondTrust today to schedule a demo of Endpoint Privilege Management and view these additional resources.

Whitepaper

- Microsoft Vulnerabilities Report 2020

Case Study

- How the University of Derby Secure their Endpoints with BeyondTrust

Video

- A Two-Minute Overview of our Endpoint Privilege Management Solution

Datasheets

- Privilege Management for Windows & Mac
- Privilege Management for Unix & Linux

ABOUT ENDPOINT PRIVILEGE MANAGEMENT

BeyondTrust Endpoint Privilege Management elevates privileges to known good applications that require them, controls application usage, and logs and reports on privileged activities

using security tools already in place.

With granular application control, multiple deployment options, and a unique Quick Start feature, achieving least privilege without impacting user productivity has never been easier.

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 70 percent of the Fortune 500, and a global partner network. Learn more at

beyondtrust.com