Learn how to protect your organization from cyberthreats by implementing least privilege

BeyondTrust

A Guide to **Endpoint Privilege Management**

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In this guide, you will learn what endpoint privilege management is and how using it to implement and enforce least privilege across Windows, macOS, and Linux endpoints significantly enhances enterprise security and operational performance.

Read on for an overview of:

- The current cybersecurity landscape
- How endpoint privilege management helps simplify the compliance process
- The benefits of application control
- How endpoint privilege management works to seamlessly secure organizations
- How endpoint privilege management enhances user productivity and operational performance

Understanding the Modern Cyberthreat Landscape

To better understand endpoint privilege management and how it protects organizations, let's first explore the threats organizations face.

The Modern Threat Landscape

According to an IBM report, **83% of organizations** have had more than one security breach. Identifying and containing a breach is a complex and costly process. In 2023, it took organizations a mean time of **204 days to identify** that they had been breached and an additional **77 days** on top of that to contain the breach.[1]

The majority (83% in 2023) of breaches were perpetrated by external threat actors. However, insiders also pose a major threat in two different ways, accounting for 19% of data breaches in 2023. Some insiders are malicious and intentionally harm the organization, but insiders are also twice as likely to harm the organization through inadvertent mistakes that jeopardize sensitive data (such as via exposure of cloud buckets) or critical systems.[2]

[1]SOURCE: 2023 Cost of a Data Breach Report. IBM. July 2023
[2]SOURCE: 2023 Data Breach Investigations Report. Verizon. June 2023

How are external threat actors *able to gain access* to so many organizations?

Malware, including ransomware, poses a serious threat. **71% of companies** were affected by malware in 2022[3], and it contributed to more than **20% of breaches in 2023.**[4]

Identities are also a huge factor. **90% of organizations** reported one or more identity-related security incidents in 2023.[5] Stolen credentials often play a role. **More than 45%** of data breaches in 2023 were perpetrated using stolen credentials, which are frequently acquired via social engineering campaigns like phishing, smishing, or pretexting.[6]

Cloud identities, which are proliferating across platforms like AWS, Azure, and Google Cloud, also pose substantial risks. **In 99% of pentesting cases** conducted by IBM's X-Force Red, cloud identities were found to be over-privileged. This excess privileged attack surfaced enabled these pentesters to quickly compromise client cloud environments.[7]

The most common endpoint type that threat actors target are servers, allowing them to gain access to the critical applications and processes as well as the sensitive data that organizations often host on them. In 2023, more than **80% of breaches** affected a server, demonstrating how important a strong security posture is for server deployments.[8]

>>> These are just a few data points that provide a glimpse of the modern threat landscape, and should illustrate the importance of securing both endpoints and identities.

[3]SOURCE: 2023 State of Malware Report. Malwarebytes. April 2023
[4]SOURCE: 2023 Data Breach Investigations Report. Verizon. June 2023
[5]SOURCE: IDSA 2023 Trends in Securing Digital Identities. IDSA. June 2023
[6]SOURCE: 2023 Data Breach Investigations Report. Verizon. June 2023
[7]SOURCE: X-Force Cloud Threat Landscape Report 2023. IBM. Sept 2023
[8]SOURCE: 2023 Data Breach Investigations Report. Verizon. June 2023

Windows Vulnerabilities *and* Threats

In 2022, reported total Microsoft **vulnerabilities rose to 1,292, hitting an all-time high.**

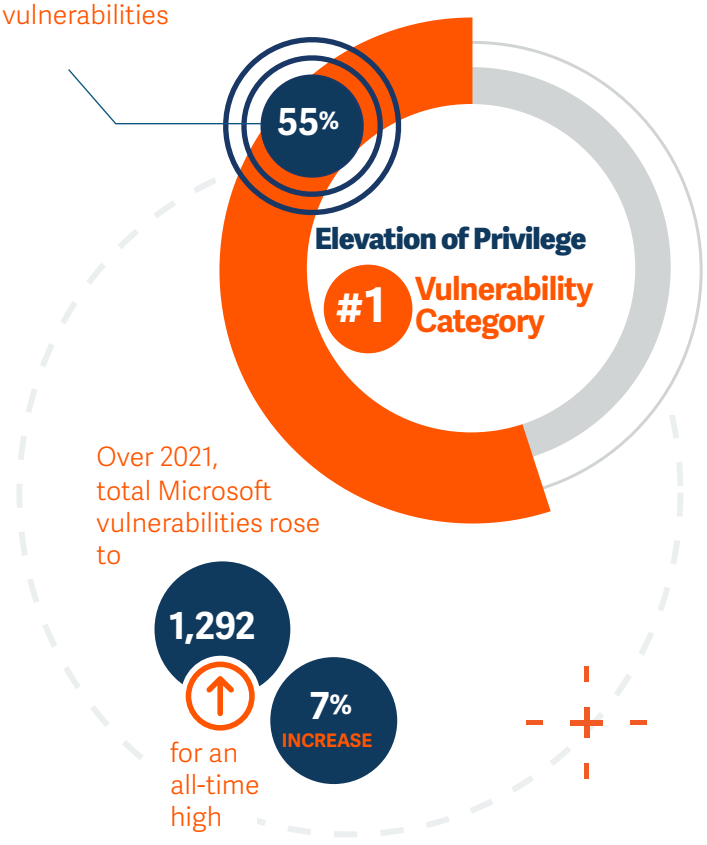
However, it's not just the number of vulnerabilities that should be of concern, **but also the unique threat and impact** posed by individual vulnerabilities.

1. The **Elevation of Privilege category dominated** the Microsoft vulnerability landscape for the third year in a row and continues its rise.

2. Microsoft Azure and Dynamics 365 are not only generating the biggest financial gains for Microsoft; they are also **propelling the biggest gains in number of vulnerabilities.**

Key Findings & Data Highlights

Elevation of Privilege accounts for **55% of the total** Microsoft vulnerabilities



macOS *and* Linux Threats

Many organizations focus their security efforts on their Windows estates, assuming that macOS and Linux endpoints are immune to the threats that plague Windows endpoints. While it may have once been true that attackers paid little attention to macOS or Linux endpoints, that is no longer the reality.

Mac usage in enterprise settings is growing rapidly, with some research firms estimating it will increase by as much as **20% in 2024**.[9] Those Mac endpoints are often used by two types of risky users:

- High-level executives,
- And highly technical developers and engineers.

Attackers are increasing their focus on macOS endpoints, as evidenced by Mac malware detections growing by **31% in enterprise** settings in recent years.[10] Without a strong security posture, organizations risk attackers breaching their high-value macOS endpoints.

Linux endpoints present an even more dire enterprise threat. Once considered inherently secure, Linux is an increasingly attractive target for attackers.

Critical applications, processes, and systems, as well as sensitive data, are often hosted on Linux servers, making them some of the highest-value targets for threat actors. From 2022 to 2023, Linux ransomware attacks increased by 62%[11]. If attackers succeed in compromising an organization's Linux endpoints, it can spell out severe consequences.

[9]SOURCE: (IDC) Worldwide Quarterly Personal Computing Device Tracker. IDC. Aug. 28, 2023
[10]SOURCE: 2021 State of Malware report. Malwarebytes. Feb 2021
[11]SOURCE: The Linux Threat Landscape Report. Trend Micro. Aug 2023

The *'Least Privilege'* Concept

To fully understand endpoint privilege management and the protection it provides in the fight against cyberattacks, it's helpful to first grasp the foundational concept that forms the basis of it: the principle of least privilege (PoLP), which is also a cornerstone of zero trust security strategies.

When a user has local administrator rights or unrestricted access to root, that means they have 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 or installing updates, and executing commands. With local admin rights, a user can also create additional user accounts and change their passwords.

Many organizations auto-provision users with local admin rights on their desktops / laptops, or provide unrestricted access to root, because it's convenient. Users are happy and productive because they can install or run any software they want.

However, this laxness in doling out broad privileges and entitlements greatly expands the attack surface, opens the doors to attackers, can negatively impact compliance, and leaves the organization extremely vulnerable to security breaches. Moreover, excess privilege often generates far more service desk tickets due to the security and operational issues that inevitably emerge.

Least privilege is a fundamental, security-conscious approach to managing user privileges in a way that mitigates the risk of breaches, while supporting workforce productivity. A least privilege access approach requires that users and programs receive the least amount of permission required to complete specific tasks. Ideally, privileges are elevated dynamically according to a just-in-time (JIT) access model. This means standing, or persistent/always-on privileges, are eliminated. In this model, privilege is only active for the finite moments, and within the proper context, it is needed.

Although the least privilege approach was conceived over 40 years ago, it remains arguably the most essential security measure for organizations seeking to protect their estate against modern and legacy cyberthreats.

Endpoint Least Privilege + Application Control

Endpoint least privilege works most effectively when combined with application control, and vice versa. Application control is the proactive practice of restricting and regulating the software applications that users can install or run on endpoints.

At the most basic level, application control is enacted via the creation of allow and deny lists, which enable organizations to specify indexes of applications that are either permitted on an endpoint or prohibited. This ensures only authorized and trusted applications are allowed to run, thereby preventing the execution of potentially malicious or unauthorized applications. Some mature application control technologies can exercise granular control around which specific application subfunctions and processes can run, and in what context.

The synergy of tightly integrating least privilege and application control is where endpoint privilege management comes into force.

What is Endpoint Privilege Management?

Endpoints are devices where users log on and applications run. This includes Windows, macOS, and Linux computer systems, laptops, desktops, and servers, as well as IoT devices, operational technology (OT) systems, networking devices, and more.

Endpoint privilege management solutions, sometimes referred to as privilege elevation and delegation management (PEDM) solutions, allow organizations to control exactly what actions can and cannot be performed by users on any given endpoint. These solutions should combine privilege management, application control, and centralized administrative control that incorporates robust monitoring features for all privileged activities. With endpoint privilege management, organizations can remove standing local admin rights without sacrificing any user productivity.

In many organizations, some (or all) users have full local administrative rights, which in essence means they have limitless privileges to execute, install, run, or change anything on their endpoint. A considerable downside is that this also means malware can run with elevated privileges, security controls can be bypassed, and software can be installed and executed with no control or visibility, by a threat actor. It also means a user could inadvertently make changes that have big security or operational implications, potentially even at massive scale, depending on their role.

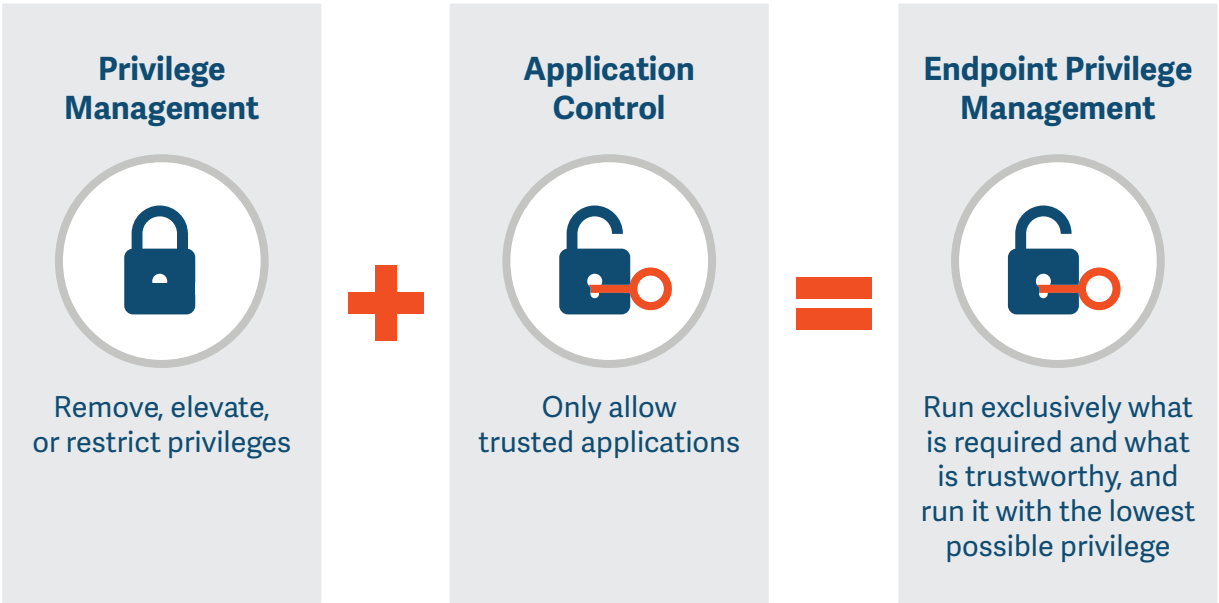
Organizations tend to assign local admin rights to employees on a company-wide basis, to ensure their users are productive and to head-off any potential future access requests of IT Support. This practice dangerously bloats the attack surface, not only providing potential entry points for attackers to gain an initial foothold, but also opening up pathways that enable attackers to advance their attack via lateral movement.

Cloud and multicloud environments have further exacerbated the problem of excess privilege, while also obfuscating the level of privilege identities may have at any given moment. There are over 40,000 permissions across key cloud infrastructure platforms that can be granted to identities. An estimated 50% of cloud identities are high-risk and have Super-Admin-like privileges.[12]

Endpoint privilege management is the process of providing users just enough access, at just the right time to remain productive in their roles—without giving them full administrative rights over an IT system.

Removing local admin rights and adopting a least privilege approach has historically mitigated 75% of Microsoft's critical vulnerabilities. Not only does endpoint privilege management mitigate vulnerabilities, it also protects against dangerous zero-day threats.[13]

With enterprise endpoint privilege management solutions, access is provisioned on an application basis, rather than on a user basis. Importantly, from a security standpoint, this approach ensures employees are granted the exact level of permissions that are required for their role—nothing more and nothing less.



[12]SOURCE: 2023 State of Cloud Permissions Risk Report. Microsoft. March 2023

[13]SOURCE: 2023 Microsoft Vulnerabilities Report. BeyondTrust. March 2023.

Benefits of Implementing *an* Endpoint Privilege Management Solution

1. Endpoint privilege management **drastically enhances security** by reducing the cyberattack surfaces for endpoints and applications. In enforcing least privilege and granular control, these solutions provide foundational protection against many of the most common attack vectors, thereby safeguarding sensitive data and systems from potential breaches.

2. Endpoint privilege management **improves operational efficiency** by streamlining access controls and reducing the burden on IT and security administrators. Such solutions allow for more effective management of user permissions.

   Many organizations attempt to use sudo to manage privileged access on their macOS and Linux desktops and servers, but it has critical shortcomings that leave organizations with painful challenges. Endpoint privilege management enables centralized, policy-based management of privileged access, drastically reducing the workload on IT and security administrators.

3. Endpoint privilege management **helps organizations maintain compliance** with regulations and standards by providing detailed audit logs and enforcing least privilege principles.

   In contrast to native or open-source alternatives, such as sudo, endpoint privilege management solutions are purpose-built for the enterprise and enable far more detailed auditing of all privileged user activity. This makes responding to audits and maintaining compliance far more streamlined.

4. Endpoint privilege management products **help organizations qualify for cyber insurance** by specifically addressing some of the most common eligibility questions such as, *do your users have local admin rights on their laptops or desktops?* And, *do you enforce least privilege across your environment?*

Evaluating & Implementing a Solution

Balancing security and user productivity is one of the central struggles at the heart of many security technologies, including PEDM. You need to strike the right balance to keep your endpoint estate secure, while also maintaining operational productivity. Achieving one without the other doesn't result in long-term success for anyone.

The right endpoint privilege management solution will not only help you minimize the attack surface, but also improve admin efficiency—without sacrificing the experience of all the end users across your enterprise.

Introducing BeyondTrust Endpoint Privilege Management

BeyondTrust Endpoint Privilege Management enables organizations to eliminate unnecessary privileges, implement zero trust controls, satisfy specific cyber insurance qualification requirements, and solve some of the most critical and foundational security challenges across Windows, macOS, and Linux endpoints. The solution works seamlessly across cloud and on-premises environments, and also can enforce security best practices across your DevOps and CI/CD workflows.

Customers rely on BeyondTrust Endpoint Privilege Management to:

1 Remove unnecessary privileges to achieve least privilege

Endpoint Privilege Management empowers you to remove local admin rights, control root access, and implement true least privilege and zero trust security across Windows, macOS, and Linux desktops and servers—all without compromising end-user productivity.

2 Control the applications users can install or run

BeyondTrust Endpoint Privilege Management empowers you to proactively restrict which applications users can install or run through fine-grained, policy-based controls. This helps prevent the installation or execution of unauthorized or potentially harmful applications.

3 Protect against external cyberthreats

Endpoint Privilege Management safeguards against common cyberattack vectors by enforcing least privilege, limiting the risk of lateral movement by an attacker, preventing unauthorized execution of malicious code, and enabling the restriction of common attack chain tools. The BeyondTrust solution includes advanced controls that can even intelligently thwart tricky fileless attacks and sneaky living-off-the-land (LotL) exploits.

4 Protect against internal threats and errors

Endpoint Privilege Management helps your users work better. The BeyondTrust solution protects against internal threats by enabling true least privilege. End users will have just enough access, at just the right time, to only the appropriate application or process. The solution also enhances security by reducing errors. For instance, the product has a policy language that can elevate Linux commands just-in-time and inspect all the options and switches (including what is embedded in scripts). This allows it to identify malformed or inappropriate commands.

5 Pass audits and achieve compliance with regulations

Endpoint Privilege Management equips you with the tools needed to simplify the audit process and ensure compliance to diverse regulatory requirements. Granular access controls, a single unimpeachable audit trail of all privileged user activity, and secure central management do the heavy lifting, so you won't have to.

6 Integrate other critical security solutions

Endpoint Privilege Management seamlessly integrates with a customer's existing security technology solutions, enhancing overall visibility and operations, thereby improving the effectiveness of existing solutions. Seamless, out-of-the-box integrations include ITSM, SIEM, MFA, BeyondTrust Active Directory Bridge, BeyondTrust Password Safe, and more

BeyondTrust Endpoint Privilege Management is native and specifically optimized to manage and protect endpoints across Windows, macOS, and Linux endpoints. Here are some features of Endpoint Privilege Management that address operating system-specific use cases and challenges.

Endpoint Privilege Management for
Windows and Mac Features

Privilege Management: Remove local admin rights fast, improve the end-user and admin experience, and greatly reduce IT service desk tickets.

True Least Privilege: Give just enough access, at just the right time, to only the appropriate application or process.

Application Control: Gain control over what users can install or run—without impacting productivity or creating management overhead.

Trusted Application Protection: Stop attacks from taking advantage of email attachments, bad scripts, and malicious websites, with built-in, context-based security controls.

Reporting & Visibility: Monitor your users' activity through customizable dashboards and reports; and seamlessly update policy based on user activity to continuously bolster your security posture.

Rapid Deployment: Use pre-built quick-start policies informed by insights from thousands of deployments to make rapid, high-impact leaps in risk reduction.

Endpoint Privilege Management for
Linux Features

Auditing & Governance: Monitor user activity with centralized capture and management of event logs, including privilege elevation events and full session recordings.

Sudo Replacement: Fine-grained, policy-based control of privileged access replaces sudo with a streamlined, centralized solution.

Dynamic Access Policy: Utilize factors such as time, day, and location to make automated, intelligent privilege elevation decisions.

Policy & File Integrity Monitoring: Audit and report on changes to critical policy, system, application, and data files.

Centralized Management: Centralize the management of your Linux estate, including all user activity data, policies, upgrades, updates, and deployments.

Fine-Grained Least Privilege: Control root access and dynamically elevate privileges for standard users through fine-grained, policy-based controls.

Remote System & Application Control: Enable users to run specific commands and conduct sessions remotely based on rules—without logging on as admin or root. Enable organizations to implement multiple layers of security, protecting against both external attackers and internal mistakes.

High Availability: Reduce daily maintenance and errors, and achieve advanced fail-over and load-balancing by managing policy configurations for Linux hosts.

Integration & Scalability: Automate tasks, seamlessly integrate with your other systems and tools such as SIEM or ServiceNow, and scale simply to meet enterprise needs.

How to Operationalize Endpoint Privilege Management, Fast

With BeyondTrust Endpoint Privilege Management, you can implement the solution in a matter of days and make rapid leaps in risk reduction. Our pre-built, out-of-the-box QuickStart policy templates help you achieve fast time-to-value on Windows and Mac endpoints.

Based on learnings from thousands of Endpoint Privilege Management deployments, QuickStart policy templates cover the majority of enterprise requirements and have helped complex organizations with over 100,000 endpoints deploy Endpoint Privilege Management in just weeks.

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 climb the security scale without impacting user productivity. No other endpoint privilege management product offers this level of convenience, flexibility, and speed during deployment.

How Does QuickStart Work?

The BeyondTrust QuickStart policy templates allow organizations to apply three common workstyles to the users and endpoints in their estate. You can choose a workstyle based on the necessary flexibility of the user's job role:

Low flexibility (i.e. sales, marketing, etc.)

Users under the low flexibility workstyle are allowed to run approved applications and operating system functions. However, if an unknown application tries to run, or if an application requests admin rights, the user is prompted to contact support to obtain a challenge-response code that can only be generated by IT.

Medium flexibility (i.e. sales engineers, IT, etc.)

Users under the medium flexibility workstyle must authenticate and provide a business reason before they can run unknown applications. This helps to add an extra layer of security and an immutable trail of user activity between potentially harmful installations and your environment.

High flexibility (i.e. developers, engineers, QA, etc.)

The most flexible of all workstyles, these users are prompted to simply provide a business reason to install unapproved applications or make system changes. This ensures that highly technical users are able to remain productive, while capturing an immutable record of their activity.

QuickStart policy templates enable BeyondTrust customers to get up and running with Endpoint Privilege Management overnight and make substantial security gains. Once you've implemented this baseline, you can continually build onto it thanks to detailed, intuitive user activity tracking.

Endpoint Privilege Management allows you to closely monitor user activity. This includes what applications they're trying to install or run, what operating system settings they're trying to change, and common areas where their productivity could be getting blocked. This data is served as intuitive insights, which you can seamlessly apply to update your policies, helping continuously strengthen your security posture as your organization changes.

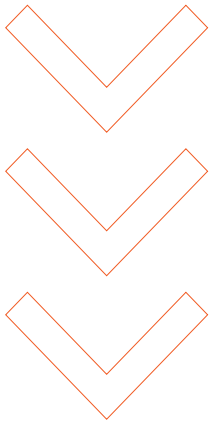
Fast Time-to-Value for Linux Privilege Management

On Linux servers and desktops, Endpoint Privilege Management can also be operationalized and scaled quickly. Start by simply downloading and deploying endpoint agents to all your Linux endpoints across on-premises, hybrid, and cloud environments. Endpoint Privilege Management empowers you to address your core security gaps quickly with role-based policies. These lightweight, easy-to-implement policies deliver huge leaps in risk reduction, fast. After filling your core security gaps, these policies can be updated continuously to keep pace with your changing environment.

Why BeyondTrust

BeyondTrust has paved the way for innovation with 25+ years in the Endpoint Privilege Management and Privileged Access Management (PAM) spaces. In 2023, we release 100+ new features for our Endpoint Privilege Management solution. We are also annually named by the top-tier industry analysts as a PAM leader and are recognized for the strength of our endpoint privilege management capabilities.

By uniting privilege management and advanced application control, BeyondTrust Endpoint Privilege Management empowers organizations to protect against cyberattacks, while still maintaining user productivity.



Hear from Our Customers: **What They Like About BeyondTrust Endpoint Privilege Management**

"Competitor solutions were bulky and had difficult processes to set up and apply. BeyondTrust Endpoint Privilege Management seamlessly integrated with our internal process and created an exceptional outcome."

Vikas Vijaywargiya, CIO, Zensar

"Everybody tries to sell you the world and then gives you a little bit. BeyondTrust is different. They have given us more than we even knew was possible."

Tommy Green, VP Information Systems & Technology, Amoco

"If you are looking for a solution that allows you to quickly and easily eliminate admin rights, I have no hesitation recommending [Endpoint Privilege Management] to any organization."

Application Support Manager, Seyfarth Shaw

"BeyondTrust provides a powerful platform that allows us to streamline and standardize application control and privileged management across our entire organization. Our people are smarter and better protected, and that's great news for our business."

Dan Bartlett, Senior Consultant, Ramboll

"BeyondTrust pushes us to be better... From sales to support to engineering, BeyondTrust has always extended dedicated care and attention to our projects."

David Lokke, Senior Systems Administrator, PREMIER Bankcard

"We did an extensive review of the different offerings in the endpoint privilege management space and BeyondTrust was the clear winner. We didn't have to do any training with the software itself, and we were able to roll it out quickly with minimal impact on our users."

Richard, Zecurity Manager, Global Software Developer

Next Steps & Resources

Hopefully this guide has shed light on how endpoint privilege management works, highlighting the quick wins and long-term benefits implementing least privilege and application control can provide your organization.

Contact BeyondTrust today to learn more about **Endpoint Privilege Management.**

- Gartner Magic Quadrant for Privileged Access Management
- Cybersecurity Insurance Requirements Checklist
- Microsoft Vulnerabilities Report
- Endpoint Privilege Management for Linux Solution Brief
- Endpoint Privilege Management for Mac Use Cases
- Buyer's Guide for Complete Privileged Access Management (PAM)
- Endpoint Privilege Management Case Study: Ramboll
- Investec's Journey to Zero Trust: from Theory to Practice

BeyondTrust is the worldwide leader in intelligent identity and access security, enabling organizations to protect identities, stop threats, and deliver dynamic access. We are leading the charge in innovating identity-first security and are trusted by 20,000 customers, including 75 of the Fortune 100, plus a global ecosystem of partners.

beyondtrust.com