BeyondTrust

Beyond EDR:

Why EPM and Least Privilege are Critical to Endpoint Protection

Learn how pairing EPM and EDR provides a blended endpoint defense against ransomware, malware, insider threats, and more.

BeyondTrust

TABLE OF CONTENTS

Executive Summary 3

What is Endpoint Privilege Management (EPM)? 3

- BeyondTrust Endpoint Privilege Management 4

What is Endpoint Detection and Response (EDR)? 6

EPM vs. EDR: Key Differences 6

Security Problems Addressed by EPM and EDR 7

How EPM Enhances EDR 8

Limitations of EDR 9

EDR Bypass Attacks 9

4 Ways EPM Prevents EDR Bypass Attacks 10

Mapping EPM and EDR to the MITRE ATT&CK Framework 11

Next Steps 12

- Multilayered Protection Against Ransomware, Malware, and Other Endpoint Threats with BeyondTrust 12

About BeyondTrust 13

Executive Summary

Today, threat actors are rapidly evolving their techniques to evade detection, while increasing the velocity of attacks. For instance, ransomware attacks surged 50% in early 2025. Threat actors aim to target and compromise endpoints and identities to gain initial access. From there, they can deliver weaponized malware for persistence and potentially ransom and extort sensitive information.

Many organizations lack the protection mechanisms to adequately defend against these escalating threats. A late 2024 red team assessment performed by the Cybersecurity and Infrastructure Security Agency (CISA) found organizations tend to rely heavily on Endpoint Detection and Response (EDR) solutions. However, EDR by itself is failing to protect organizations against privileged attack vectors, leaving them highly vulnerable to ransomware infections, insider threats, and many other risks.

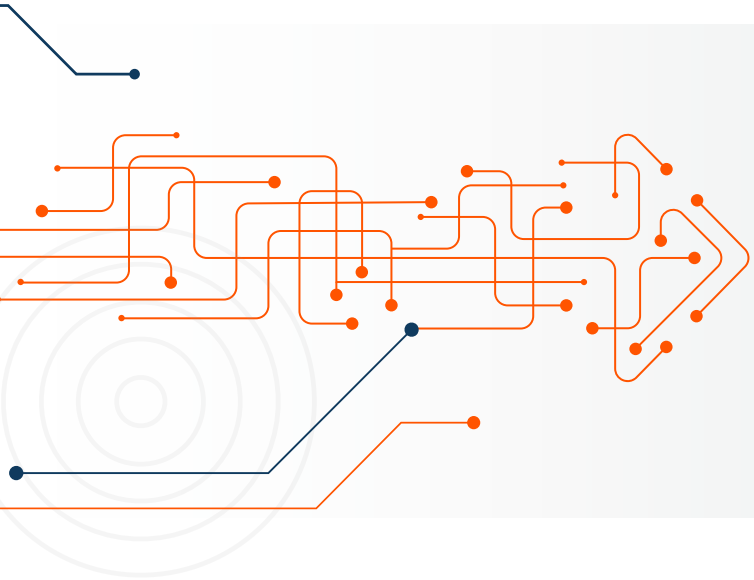
A blended endpoint protection and prevention strategy pairing EDR with Endpoint Privilege Management (EPM) amplifies defenses against a wide array of threats, increases resiliency, and breaks important parts of the ransomware attack chain.

Read on for a detailed breakdown of:

- How EPM protects against ransomware and other advanced cyber threats
- Why EPM is an essential piece of a holistic endpoint protection and prevention strategy
- The gaps threat actors are exploiting within EDR solutions
- How proactive EPM enhances reactive EDR capabilities

What is Endpoint Privilege Management (EPM)?

Endpoint Privilege Management (EPM) solutions control user privileges on endpoints, minimizing the attack surface and preventing unauthorized access to sensitive data and systems. Gartner refers to this discipline as Privileged Elevation and Delegation Management (PEDM), and defines it as a category of tools focused on granting specific, granular privileges to logged-in users. Together, Privileged Account and Session Management (PASM) and PEDM form the two core pillars of traditional Privileged Access Management (PAM).



Get Gartner analysis of the PEDM and PAM use cases that matter, and how BeyondTrust and other vendors are assessed, in the 2024 Gartner® Critical Capabilities for PAM report:

https://www.beyondtrust.com/gartner-critical-capabilities-for-pam-pedm

Endpoint Privilege Management governs privileged access on endpoints, allowing administrators to define who can access what, and under which circumstances. It achieves this by enforcing the principle of the least privilege, which dictates users should only have the minimum amount of privileges to perform their job functions.

BeyondTrust Endpoint Privilege Management

The BeyondTrust Endpoint Privilege Management solution manages privileges at the individual, user group, and application level. In an EPM-driven setup, no end user has privileged access by default. Instead, users are granted elevated privileges on an as-needed basis, with each request going through a workflow to ensure legitimacy. Some standard examples of approval workflows include:

- Elevating privilege, automatically and invisibly to the end user
- Requesting MFA or step-up authentication prior to privilege elevation
- User-justified self-elevation with a selected business reason
- Using an ITSM workflow to gain third-party approval

It's important to note that the BeyondTrust solution never grants privileges directly to the end user. Instead, privileges are granted to the task or application that requires the elevated permissions. BeyondTrust Endpoint Privileged Management can also support just-in-time (JIT) access requests to a tamper-proof and fully local audited local admin account, extending the flexibility of our solution even further.

The BeyondTrust solution offers many important benefits, including:

- **Enforcing Least Privilege and Enabling Zero Trust:** BeyondTrust Endpoint Privilege Management shrinks the attack surface and enhances an organization's security posture by removing local admin rights and standing access to implement a true least privilege model, and support zero trust.

- **Improving Security for Remote Workers:** The BeyondTrust solution allows mobile and remote workers to install software, update applications, and change settings, all while adhering to security policies. This enhances both productivity and security.

- **Endpoint Hardening:** Endpoint Privilege Management enforces least privilege at the OS level, only allowing authorized processes or users to make changes to system settings. By restricting elevated rights and controlling application execution, the solution prevents unauthorized modifications, preserves secure baseline configurations, and reduces configuration drift. Consequently, it upholds baseline integrity, while blocking and logging for review any attempted changes outside approved policies.

- **Pragmatic Application Control:** EPM solutions typically layer on application control capabilities. With the BeyondTrust solution, allow known, legitimate business applications, and block the rest. Achieve broad application control in a sustainable and scalable manner with optimized exception handling capabilities that overcome the productivity challenges experienced with alternative solutions.

- **Malware Protection for Business Apps:** BeyondTrust can block the spawning of child processes from legitimate business applications—a typical attack vector for malware. For example, PowerShell spawned from Word or Excel documents can be detected and prevented. BeyondTrust Endpoint Privilege Management can defend against malware that attempts to obfuscate these child/parent process relationships. This prevention doesn't rely on analysis of the child process behavior, but instead is automatic and based on the parent process belonging to a legitimate business app.

- **Reducing IT Costs:** BeyondTrust Endpoint Privilege Management simplifies automation of tasks like credential rotation and access provisioning. The solution reduces the workload of IT staff and minimizes the risk of human error, such as the misuse of privilege on an endpoint. By acting as a password change agent for loosely connected devices, the solution can rotate passwords on devices when it's offline.

- **Meeting Compliance and Regulatory Requirements:** The BeyondTrust solution also enables organizations to meet key regulatory frameworks and standards, such as GDPR, ACSC's Essential Eight, and ISO 27001 to name a few. It enforces least privilege, implements a unified security policy, and creates an audit trail for all privileged activities. Increasingly, Endpoint Privilege Management is a must-have to qualify for cyber insurance.

What is Endpoint Detection and Response (EDR)?

Endpoint Detection and Response (EDR) solutions monitor endpoint activity to detect and respond to real-time threats, either through automation or manual remediation. EDR solutions provide real-time visibility and use advanced analytics and machine learning to identify suspicious behavior and potential threats, as opposed to the static rules-based nature of traditional antivirus (AV) software.

Organizations can deploy EDR across workstation and server environments to understand and respond to the threat lifecycle. EDR tools help answer what happened, how it happened, where it has been, and what it's doing now. Today, we often see EDR tools / capabilities as part of Extended Detection and Response (XDR) offerings, which include additional telemetry from networks, email, etc.

Key EDR capabilities include:

- **Real-time visibility:** EDR agents on endpoints continuously monitor and capture data, such as running processes, network connections, registry changes, and file access.
- **Threat detection:** EDR solutions analyze the data—usually leveraging AI/ML—to identify patterns and behaviors indicative of potential threats, including malware operation, intrusion techniques, and unusual data access patterns.
- **Response and remediation:** EDR solutions can trigger a response to a detected threat, such as isolating an infected endpoint, stopping malicious processes, or reverting potentially unwanted changes.
- **Threat hunting:** EDR can assist SOC teams in threat hunting with forensic analysis tools that enable deeper endpoint investigations.

EPM vs. EDR: Key Differences

While both EPM and EDR are key endpoint security toolsets, they differ in approaches and goals. See the table below for a breakdown of how EPM and EDR differ from each other, but more importantly, complement each other.

	EPM	EDR
Primary Protection Approach	Prevention	Detection and response
Methodology	Privilege control and application control	Continuous monitoring and analysis

	EPM	EDR
Main Threats Addressed	Unauthorized access, privilege escalation, lateral movement, insider threats, external threats	Malware, ransomware, fileless attacks, zero-day exploits
Other Threats Addressed	Malware, ransomware, zero-day and LOLBin exploits through trusted app protection/app control	Anomaly detection through real-time monitoring
Approach	Proactive	Reactive
Implementation	Policy-based, restricts user privileges	Agent-based, monitors endpoint activity

EDR **detects and responds reactively to threats** that have already bypassed preventative measures. It does so by continuously monitoring endpoint activity, then analyzing the data for suspicious behavior. Then, it provides tools for investigation and remediation.

BeyondTrust Endpoint Privilege Management **focuses on proactive protection** to help prevent and mitigate threats. The BeyondTrust solution shrinks the attack surface and threat windows by limiting user privileges and enforcing least privilege, controlling application execution, removing standing privileges, and preventing unauthorized access to sensitive resources.

Security Problems Addressed by EPM and EDR

EPM and EDR address different types of security problems.

EPM primarily tackles:

- **Unauthorized access:** EPM enforces least privilege and prevents unauthorized users from accessing sensitive data and systems. It does so by controlling application and child process elevation to stop unwanted software, malware, and ransomware from executing.
- **Privilege escalation:** EPM mitigates the risk of privilege escalation attacks. It limits user privileges and also can prevent bad actors from gaining elevated access through vulnerability exploits in third-party software.
- **Insider threats:** EPM minimizes insider threats by controlling access to sensitive data and systems, including control for privileged users. Even those with access to sensitive data can be prevented from taking actions to exfiltrate that data.
- **Application control:** EPM permits only authorized business software to be installed and used. This reduces the risk posed by shadow IT and unwanted software.

- **Remote Code Execution:** Enabling of Least Privilege and Application Control on the endpoint significantly enhances protection against Remote Code Execution, preventing execution of malicious code on a target system from a remote location.

- **Privilege monitoring:** Alongside controlling the use of privilege on the endpoint, endpoint privilege management can audit use of all privileged and non-privileged actions. This in-depth auditing aids incident response and compliance/audit processes.

EDR primarily addresses:

- **Malware attacks:** EDR detects and responds to malware/ransomware by identifying, containing, and helping remediate malicious files and processes.

- **Fileless attacks:** EDR identifies and analyzes suspicious activities on endpoints to detect fileless attacks.

- **Zero-day exploits:** EDR aims to uncover zero-day exploits by leveraging threat intelligence and detecting anomalous behaviors.

- **Reduced dwell time:** EDR can slash dwell time to minimize the potential damage incurred from endpoint exploits.

A properly configured EPM offers many similar benefits to an EDR, and more. For example, a well-maintained allowlist can make malware, ransomware, and zero-day exploits harder to execute. However, EDR can catch a zero-day exploit or vulnerability in allowed software that EPM wouldn't uncover.

How EPM Enhances EDR

BeyondTrust Endpoint Privilege Management complements and enhances EDR in several ways to create a more robust defense:

BeyondTrust Endpoint Privilege Management Benefit	Impact on EDR
Reduces noise by limiting user privileges and application execution.	Fewer false positives and improved accuracy in threat detection.
Limits the scope of potential damage.	Faster incident response, allowing EDR to focus on investigating and remediating the specific threat.
Provides context by identifying users and applications with elevated privileges.	Improved threat hunting, enabling security teams to more effectively prioritize and investigate potential threats.
Prevents threat actors from exploiting vulnerabilities that require elevated privileges.	Strengthens defenses against sophisticated attacks, making it more difficult for threat actors to gain a foothold and execute malicious activities.
Prevents tampering with EDR agents through removal of standing privileges and stopping privilege escalation.	Ensures EDR can continue to operate on a compromised endpoint.

Limitations of EDR

Organizations should always implement a layered defense-in-depth approach for endpoint security. While EDR provides significant benefits, it's not a complete endpoint security defense. What's more, recent research analysis highlights shortcomings inherent of EDR in certain attacks. The paper, Decoding the MITRE Engenuity ATT&CK Enterprise Evaluation: An Analysis of EDR Performance in Real-World Environments, demonstrated:

- **Delay / Lack of Protection:** Many EDR systems exhibit delayed protection. Some solutions only react after the malicious behavior has occurred, or fail to react altogether. In some cases, EDR systems require a longer "kill chain" to build confidence before blocking threats. Some toolsets are susceptible to evasion techniques as well.
- **Network Traffic Data Collection:** Most EDR systems primarily collect transport layer network traffic data and tend to ignore application layer protocols.
- **"Living-off-the-Land" Threats:** EDR systems struggle to detect LoTL threats, which involve using legitimate tools for malicious purposes.
- **Contextual Information:** While EDR systems can identify some malicious behaviors and provide context, they struggle with others, such as credentials from password stores and permission group discovery. EDRs also tend to provide less context for activities common in everyday use.
- **Manual Effort:** Detecting techniques integrated with local environments often requires additional manual effort.
- **Linux Protection:** EDR systems generally offer a lower protection rate against attacks on Linux compared to Windows. Some EDR products lack Linux support altogether.

EDR Bypass Attacks

As widely reported, threat actors (including APT / nation-states) are forging ahead in developing more sophisticated techniques to successfully evade EDR technology. Some methods being observed include:

- **Exploiting legitimate tools and resources (such as LOLBins)** already present on the system to execute attacks. The co-option of legitimate tools makes it exceedingly difficult for EDR to differentiate between authorized and malicious activity.
- **Executing Bring Your Own Vulnerable Driver (BYOVD)** attacks to exploit vulnerabilities in legitimate drivers, gain high-level system access, and disable EDR solutions.

- **Launching supply chain attacks to compromise legitimate software or services.** Attackers can then bypass EDR solutions by gaining access to target systems that trust the compromised software.

- **Leveraging specialized tools** like EDRKillShifter, AvNeutralizer, etc. to disable EDR capabilities before or as part of an attack's execution.

4 Ways EPM Prevents EDR Bypass Attacks

A multi-layered security approach that combines EDR with EPM and other PAM solutions helps organizations significantly harden endpoint security and protect against threats, especially those that may bypass EDR.

BeyondTrust Endpoint Privilege Management prevents or mitigates EDR bypass attacks by limiting the privileges and capabilities threat actors can exploit. Here's how:

1. **Enforcing Least Privilege:** The BeyondTrust solution removes local admin rights and enforces least privilege so users, applications, and systems only have the minimum needed. Key points of an attack, such as running malware, dumping credentials, and achieving lateral movement, typically require privilege to execute. So, removing unnecessary privileges not only can prevent threats from gaining a foothold in the first place, but also limits the actions a threat actor or malware can take, if they have compromised a user account or endpoint.

2. **Enabling Application Control:** BeyondTrust Endpoint Privilege Management controls which applications are allowed to install and at what privilege level they can run. Such controls prevent threat actors from executing malicious code or exploiting vulnerabilities in unapproved, but legitimate, applications. The solution also blocks or restricts the use of tools commonly used for EDR bypass, such as LOLBins and vulnerable drivers. This considerably limits threat actors' ability to evade detection.

3. **Preventing Lateral Movement:** By eliminating excessive privileges on an endpoint, BeyondTrust Endpoint Privilege Management makes it more difficult for threat actors to move laterally within a compromised network. This not only limits the potential damage a threat actor can inflict, but also helps buy time for EDR to detect and respond to the initial compromise.

4. **Amplifying EDR Effectiveness:** By limiting privileges and application execution, the BeyondTrust solution reduces the "noise" that would otherwise have to analyze. In turn, this contributes to reduced false positives, while increasing threat detection accuracy.

BeyondTrust Endpoint Privilege Management essentially acts as a proactive layer of defense to complement EDR's reactive capabilities. By also preventing threat actors from gaining the privileges and tools needed to bypass EDR, BeyondTrust strengthens your overall security posture and makes it much more difficult for threat actors to succeed.

Mapping EPM and EDR to the MITRE ATT&CK Framework

MITRE ATT&CK is an ontology and knowledge base of curated threat intelligence of real-world attacks. It provides a structured way to understand adversary tactics and technique. Organizations use this framework to identify mitigations and improve security posture.

The table below demonstrates EPM's core functionality and protection mechanisms against attacks in the wild. These mitigations span various tactics and techniques to harden endpoints, reduce and restrict elevation, enforce least privilege, and minimize the attack surface. Endpoint Privilege Management allows organizations to take a proactive and preventative approach to disrupt threat actors early in the ATT&CK lifecycle. The user and endpoint are known attack vectors, and formalizing these mitigations is essential for endpoint resiliency.

Mitigation ID	Name	EDR	EPM
M1025	Privileged Process Integrity	◖ Controls privilege elevation	● Monitors and blocks unusual activity
M1026	Privileged Account Management	◖ Detects misuse	● Enforces least privilege
M1027	Password Policies	◖ Support monitoring	● Enforces strong auth for elevation
M1028	Operating System Configuration	◖ Detects changes	● Enforces hardening, restricts elevation
M1028	Account Use Policies	◖ Detects policy violations	● Enforces usage restrictions
M1033	Limit Software Installation	◖ Prevention of malicious software install only	● Can prevent installation of any unwanted software
M1038	Execution Prevention	● Blocks execution behaviors	● Prevents unauthorized elevated runs
M1040	Behavior Prevention on Endpoint	● Core capability	◖ Reduces attack surface
M1042	Disable or Remote Feature or Program	◖ Alerts on use	● Restricts access to system tools
M1047	Audit	● Collects telemetry	● Logs privilege elevation events
M1050	Exploit Protection	● Memory protections	◖ Reduces exploit viability via least privilege
M1054	Software Configuration	● Alerts on changes	● Controls app elevation behavior

● Core Feature ◖ Supportive/Complementary Feature

Next Steps

EPM and EDR are essential to achieve a holistic endpoint protection and prevention strategy. Endpoint Privilege Management takes a more proactive and preventative approach by controlling user privileges and application execution. Endpoint Detection and Response, on the other hand, offers reactive controls for detection and response threats that have bypassed preventative measures.

Paired together, EPM and EDR can significantly enhance endpoint security posture, reduce the risk of cyberattacks, and protect sensitive data and systems. This layered approach is critical in today's dynamic threat landscape, where organizations must be prepared to prevent, detect, and respond to a wide range of attacks targeting endpoints.

Multilayered Protection Against Ransomware, Malware, and Other Endpoint Threats with BeyondTrust

As covered in this guide, BeyondTrust Endpoint Privilege Management provides powerful capabilities that reduce the attack surface to prevent and mitigate threats from ransomware, malware, insiders, and external threat actors. The product also improves the effectiveness of EDR, while proactively stopping threats that EDR may otherwise miss.

The leading industry analysts consistently recognize BeyondTrust as an overall leader in the privileged access management (PAM) space. The BeyondTrust Endpoint Privilege Management solution stands out for its breadth and depth of capabilities across Windows and macOS workstations, and Windows and Linux servers.

While BeyondTrust Endpoint Privilege Management by itself can significantly enhance your organization's security posture, improve operations, and help address many regulatory and compliance initiatives, it is just one piece of BeyondTrust's groundbreaking platform approach to identity security. The BeyondTrust Pathfinder Platform provides a single integrated console for all our products, delivering a unified experience for operational agility that brings shared context across all our products. Gain unprecedented risk visibility and control of identities, privileges, and Paths to Privilege™.

With the integrated Pathfinder platform, customers can benefit from the broad and deep capabilities reflected in our multicategory identity security leadership, which spans Privileged Access Management (PAM), Identity Threat Detection and Response (ITDR), Cloud Identity Management, Cloud Infrastructure Entitlement Management (CIEM), and Enterprise Secrets Management. When it comes to ransomware and malware, these capabilities translate into preventing attacks, breaking more parts of the attack chain, and also responding more rapidly, and with precision, to stop or mitigate in-progress attacks.

Learn how BeyondTrust Endpoint Privilege Management, as part of of our unified Pathfinder platform, delivers a **Least Privilege Defense-in-Depth Solution.**

Or, contact us today to chat about how BeyondTrust can help you address your organization's security, compliance, and workforce efficiency needs: **https://www.beyondtrust.com/contact.**

Keep Learning about BeyondTrust Endpoint Privilege Management and Other Solutions

- Guide to Endpoint Privilege Management (guide)
- Buyer's Guide for Complete Privileged Access Management (PAM) (guide)
- Streamlining Security: How L3Harris Technologies Optimized Endpoint Management Post-Merger with BeyondTrust (case study)
- Microsoft Vulnerability Report 2025 (research report)

Gartner®, Critical Capabilities for Privileged Access Management, by analysts: Paul Mezzera, Abhyuday Data, Michael Kelley, Nayara Sangiorgio, Felix Gaehtgens. 9 September, 2024.

>>> About BeyondTrust

BeyondTrust is the global identity security leader protecting Paths to Privilege™. Our identity-centric approach goes beyond securing privileges and access, empowering organizations with the most effective solution to manage the entire identity attack surface and neutralize threats, whether from external attacks or insiders.

BeyondTrust is leading the charge in transforming identity security to prevent breaches and limit the blast radius of attacks, while creating a superior customer experience and operational efficiencies. We are trusted by 20,000 customers, including 75 of the Fortune 100, and our global ecosystem of partners.

Learn more at **www.beyondtrust.com.**