Moving from a Reactive to Preventative Approach

5 Critical Steps in

# YOUR ENDPOINT SECURITY STRATEGY

BeyondTrust

# CONTENTS

**Overlooked Step*

# ENDPOINT SECURITY

Overview & Benefits

**In 2019, 70% of successful breaches started at the endpoint.*** And now, with the large-scale shift to remote working due to COVID 19, the explosion of end user devices, BYOD and endpoints working outside of the network, many organizations are still trying to determine the best security strategies, giving attackers time to take advantage and capitalize on the uncertainty.

Traditional Endpoint Security is the process of securing devices such as mobile devices, laptops, desktops, servers, IoT, and POS and ensuring that those devices comply with certain criteria before they are granted access to network resources. The goal of endpoint security is to limit the attack surface by blocking unauthorized entry and safeguarding the network from malicious threats.

Threats to endpoints can come in the form of external attacks as well as insider threats, which may be either malicious or unintentional in nature. **A compromised endpoint can give an attacker a foothold within an environment, enabling them to launch further attacks on systems to access data and compromise additional endpoints via lateral movement.**

Since a corporate IT network is essentially a linkage of endpoints, endpoint integrity and security should be prioritized before implementing other security solutions at the application layer. As we evolve into modern management of endpoints, the focus should shift to access to corporate data and cloud applications that may not be connected to a corporate environment.

> *We have seen a*
> **30,000%**
> *increase in malware directly attributed to COVID 19*
>
> *—Zscaler**

*IDC, "Do You Think Your Endpoint Security Strategy Is Up to Scratch?", October 2019

*www.zscaler.com/blogs/research/30000-percent-increase-covid-19-themed-attacks

> *Removing admin rights is not just about security—it will also allow your computers to run faster, better and longer.*
>
> *—SAMI LAIHO*
> *Microsoft MVP & Ethical Hacker*

## Benefits of Endpoint Security

- **Improved Security:** Removing admin rights, enforcing least privilege, applying "Just-In-Time (JIT)" access control, and employing signature-based tools like antivirus drive down the risk of security incidents and data breaches from threats targeting endpoints.
- **Enhanced Endpoint Performance:** Eliminating superfluous privileges and hardening devices translates into fewer misconfigurations, incompatibilities, security incidents, and other issues that may cause disruption, and protects against endpoint instability.
- **Simplified Compliance and Audits:** The more tightly an endpoint system is integrated, managed and controlled, and the better the visibility across the entire enterprise, the more straightforward the path to regulatory compliance.
- **Operational Excellence:** The right security tools allow IT to support more types of endpoints and confidently pursue business-enabling changes to the environment, including the roll-out of new technologies and ensuring standardization for monitoring and change control.

# CHALLENGES

## With Traditional Endpoint Security

In today's threat environment, breaches seem inevitable. While the risk of a breach can be significantly mitigated with detection measures, the risk can never be reduced to zero. Having solutions in place to prevent users from performing actions that could result in malware, ransomware, and phishing are just as important. **With 70% of breaches starting at the endpoint, traditional endpoint security needs to evolve to more proactively manage modern threats.**

Evolving cyberthreats, increasingly complex and diverse endpoint environments, corporate misalignment of security technologies to threats, and ever-more stretched IT and InfoSec teams are just some of the many converging factors that put an organization's universe of endpoints at risk, and therefore, the entire network.

Traditional endpoint security tools like antivirus prevent *known* attacks and known attack vectors but **miss an average of 60% of modern endpoint attacks.** And, while Endpoint Detection and Response (EDR) solutions are a valuable safety net in a defense-in-depth security strategy, they rely on statistical analysis and machines models that may not always correctly recognize the difference between threats and acceptable behavior leading to false positives or unacceptable delays in response time.

On the other hand, Endpoint Privilege Management (EPM) solutions prevent attacks from breaching endpoints using a different strategy. They prevent threat actors from penetrating an environment by removing the privileges needed to compromise a host. This mitigates risks at the application layer by controlling which applications are actually permitted to execute, and most importantly, with what privileges. This model solves a critical problem in preventing lateral movement across networks in search of sensitive data to compromise.

**350,000**

pieces of new malware are detected every day*

*www.av-test.org/en/statistics/malware/

# How can organizations shift to a more preventative approach to endpoint security?

Evolving To A

# MODERN MANAGEMENT APPROACH

## Endpoint Security is an Ecosystem, Not a Single Solution

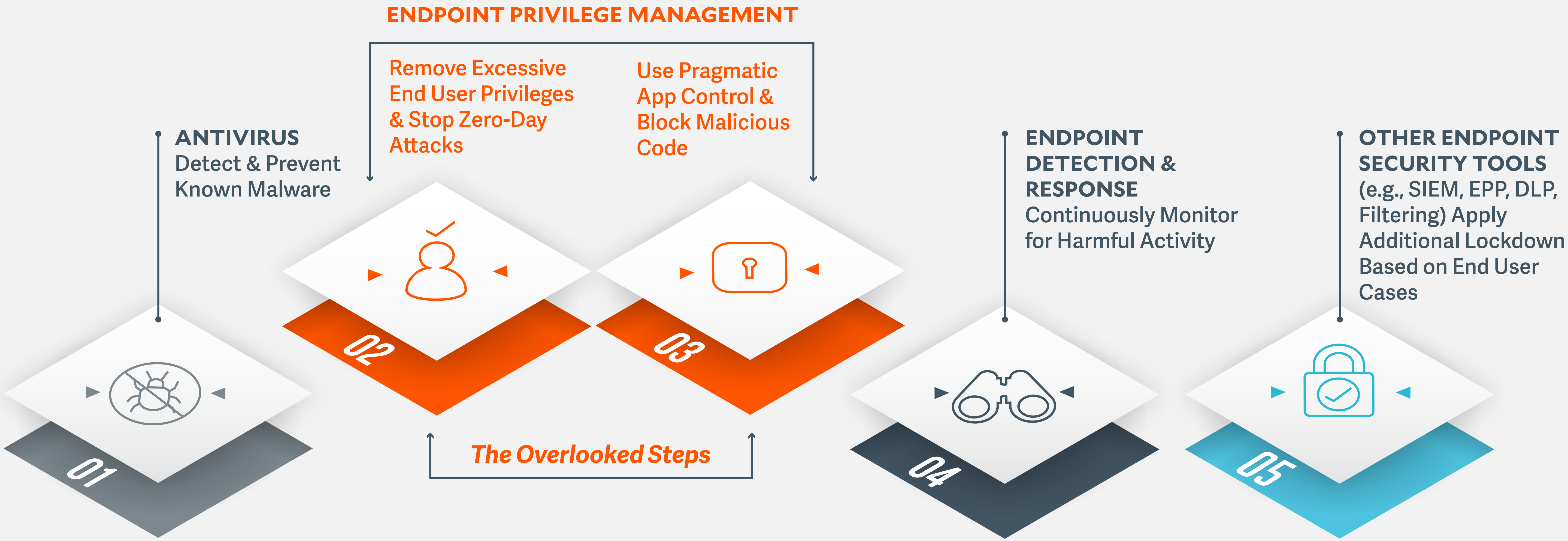
Endpoint security has evolved considerably over the last several decades—from simple, signature-based antivirus software to a holistic, technology stack designed to protect against known or unknown threats to endpoints. Today, endpoint security is necessary to prevent, detect, respond, and mitigate external and internal threats, and scale to meet the growing diversity of devices used by employees, vendors, and third parties, whether on-premises or remote.

It also needs to be adaptable and achievable so it can accommodate an evolving IT and threat environment. Endpoint security is not just one solution—it is an ecosystem that should have prevention as a foundational element rather than only on reactive remediation.

This Quick Guide outlines **5 Critical Steps** to enabling a comprehensive, preventative approach to protecting all of the endpoints in your organization.

# 5 CRITICAL STEPS OF COMPLETE ENDPOINT SECURITY

A Preventive Approach To Endpoint Security



ENDPOINT PRIVILEGE MANAGEMENT

Remove Excessive End User Privileges & Stop Zero-Day Attacks

Use Pragmatic App Control & Block Malicious Code

**ANTIVIRUS**
Detect & Prevent Known Malware

**ENDPOINT DETECTION & RESPONSE**
Continuously Monitor for Harmful Activity

**OTHER ENDPOINT SECURITY TOOLS**
(e.g., SIEM, EPP, DLP, Filtering) Apply Additional Lockdown Based on End User Cases

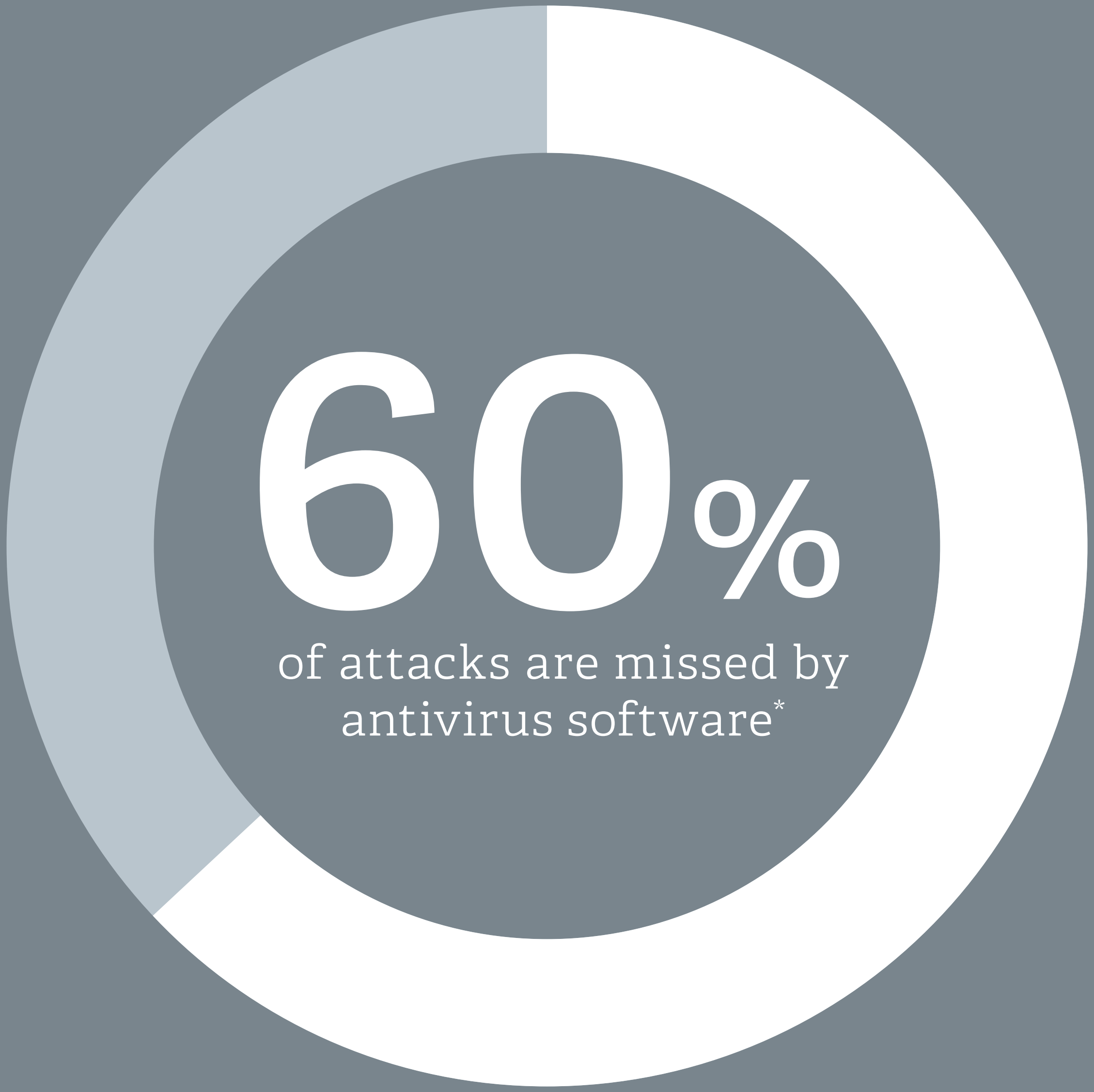
*The Overlooked Steps*

Antivirus

# DETECT & PREVENT

Known Malware

## Antivirus



Typically, antivirus (AV) software is the first endpoint security tool deployed as it defends against common and known threats and is a generally well-accepted and pervasive toolset. **However, AV is clearly not bulletproof with upwards of 60% of attacks missed by antivirus**—due to *unknown* threats, or evasive techniques that exploit 'trusted' applications. Therefore, based on regulatory compliance and well-defined security best practices, antivirus should be considered as just one component of a more complete endpoint security strategy.

Much more effective measures, that are traditionally not considered as part of endpoint security, should be used to compliment AV and statistically improve the effectiveness of endpoint security. This includes features such as restricting the use of admin privileges and controlling which applications can execute. The combination of least privilege and application control will block traditional malware and ransomware attacks. **This becomes a critical portion of Step #2.**

*Ponemon Institute, "*The Third Annual Study on the State of Endpoint Security Risk*", January 2020

Endpoint Privilege Management

Overlooked Step

# REMOVE EXCESSIVE PRIVILEGES

For End Users & Stop Zero Day Attacks

Overlooked Step

With perimeter security now stronger than ever, end user devices are heavily targeted by threat actors. Most users have unrestricted access through web browsers and can be manipulated through email, making it easy for a hacker to "lure them in" using social engineering techniques. If the user has local admin rights when they open an infected attachment or link, the "payload" can execute with their privileges, giving the hacker control of the machine by silently installing backdoors and reconfiguring (or disabling) other security controls.

**Many end users still have full administrative rights, secondary admin credentials or even temporary/shared admin accounts to do their jobs.** Admin users can also uninstall or disable other security tools on their systems which, intentionally or not, could introduce further risk.

By removing admin rights, the user can no longer download or execute malicious software that triggers ransomware or malware attacks. This dramatically reduces the attack surface and severely limits what threat actors that bypass AV can do – the vast majority of exploits and payloads will fail. With no infection present, they do not have the ability to move laterally to compromise sensitive data. **Removing admin rights would have mitigated 77% of Microsoft vulnerabilities.***

With least privilege management, users can perform admin tasks without using root or administrator credentials – giving the privileges themselves to the application, and not the user. This 'Passwordless' administration approach allows organizations to implement true least privilege, giving users just enough rights to do their jobs.

*BeyondTrust, "*2020 Microsoft Vulnerabilities Report*"

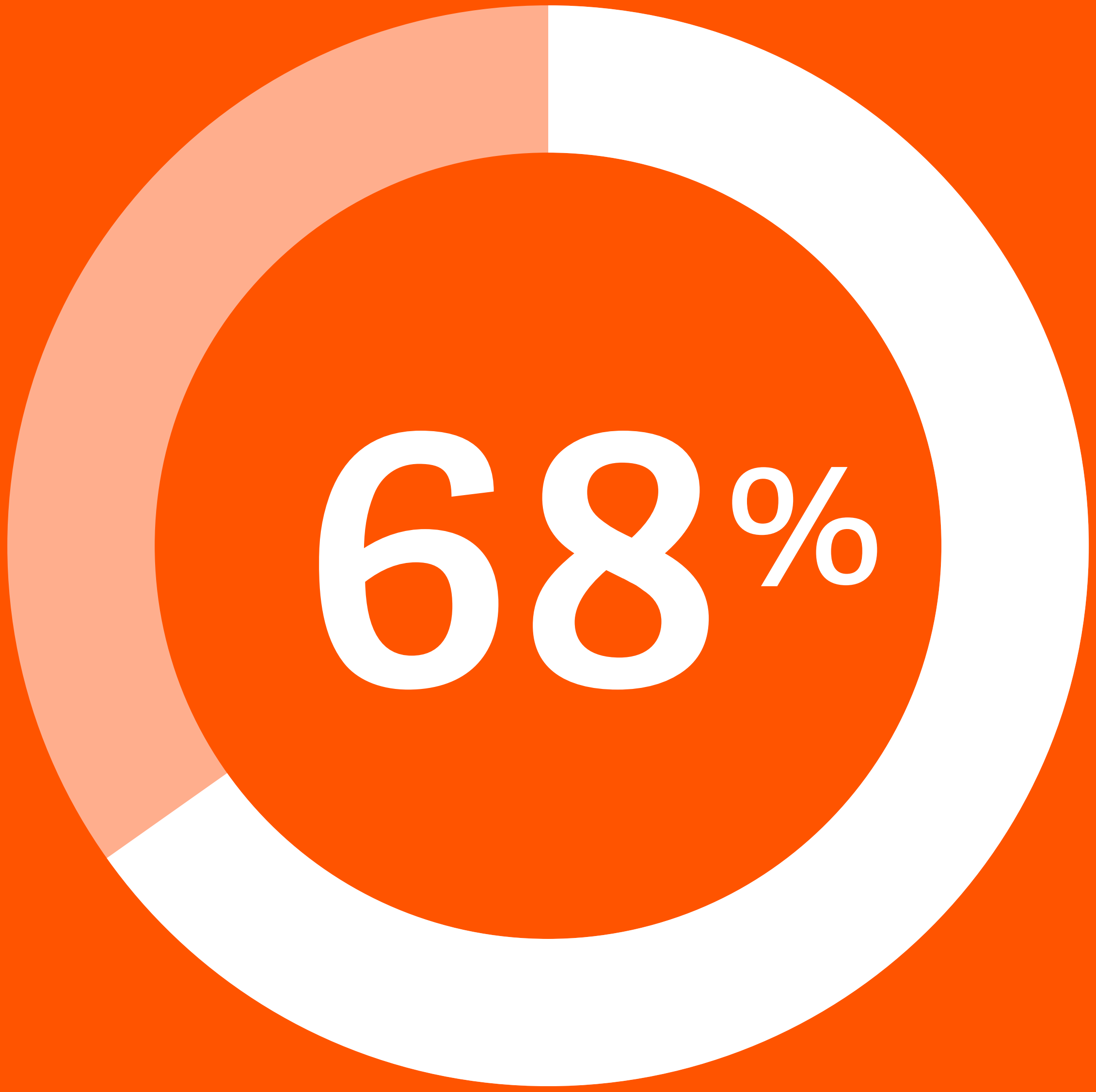
> ***Removing admin rights from end users is one of the single most effective ways to improve overall security posture, and more granular privilege management can achieve this goal without impacting productivity.***
>
> ***—DAN BLUM***
>
> *Cybersecurity Strategist & Author of*
> *Rational Cybersecurity for Business*

Endpoint Privilege Management

Overlooked Step

# USE PRAGMATIC APPLICATION CONTROL

& Block Malicious Code



of organizations have been hit by one or more endpoint attacks in the past year*

Overlooked Step

Not all endpoint attacks need to leverage privileges to compromise a machine, and this is where application control steps in. Application controls stops users, threat actors, and other applications from executing any inappropriate commands or applications on an endpoint.

**Adversaries will typically target and exploit trusted applications to allow long-term access to a system.** By compromising key applications, malicious code can be injected or tied to the applications undetected. Email and web-based applications are often targeted in this manner.

Application Control decides what applications a user can run, regardless of privileges, and allows organizations to define good and bad applications based on business needs and reputation-based models. By using application control, security teams can bolster the security of the system, making it much more difficult for an adversary to cause harm.

Traditionally, Application Control is seen as difficult and was reserved only for the most static of environments. However, by layering Application Control on top of Privilege Management, critical functionality in the operating system is trusted by default (users without privilege cannot introduce new code to directories like Program Files, Windows, System32, or Drivers). This makes it a pragmatic approach because it only needs to be applied to specific directories and files, where threat actors typically 'drop' and execute their payloads.

**Using an Endpoint Privilege Management solution as the second and third layer of endpoint security provides not only a model for least privilege, but also for robust application control.** The combined result is a drastic reduction in the endpoint risk surface. Additionally, application control is a requirement of a number of compliance mandates and frameworks.

*Ponemon Institute, "*The Third Annual Study on the State of Endpoint Security Risk*", January 2020

Endpoint Detection & Response

# CONTINUOUSLY MONITOR

For Harmful Activity

Since every risk will not be mitigated by antivirus, removing administrative rights or application control, it is also important to have endpoint security detection and response.

**Endpoint Detection and Response (EDR) solutions are designed to help organizations identify and react to threats that have bypassed their other defenses.** EDR runs locally on user workstations or servers to monitor processes, scheduled tasks, applications, logged in users and, more importantly, to determine if malicious or unauthorized activity is present on the system. This compliments EPM by acknowledging and alerting of possible attacker activity on a system outside of EPM's scope as a privilege management tool. EDR alerting can include network related activity, known malicious applications, attempts to use built in programs maliciously, and other activity. And, if EDR does detect an event, the confidence of the attack is much higher because privileges and potentially malicious applications have had their execution mitigated by EPM. The number of false positives will decrease, reducing the time needed to review event data and anamolies.

It is important to remember that an EDR solution alone does not give your organization complete monitoring capabilities. Well-trained security professionals and sound processes are needed to maximize your EDR investment and truly improve your security. Without the right team and time commitment, EDR products can amass data and alerts, which can in turn increase your resource costs.

> *EDR alone* ***does not*** *give your organization complete monitoring capabilities.*

Other Endpoint Security Tools

# APPLY END USER LOCKDOWN

Based on End User Cases

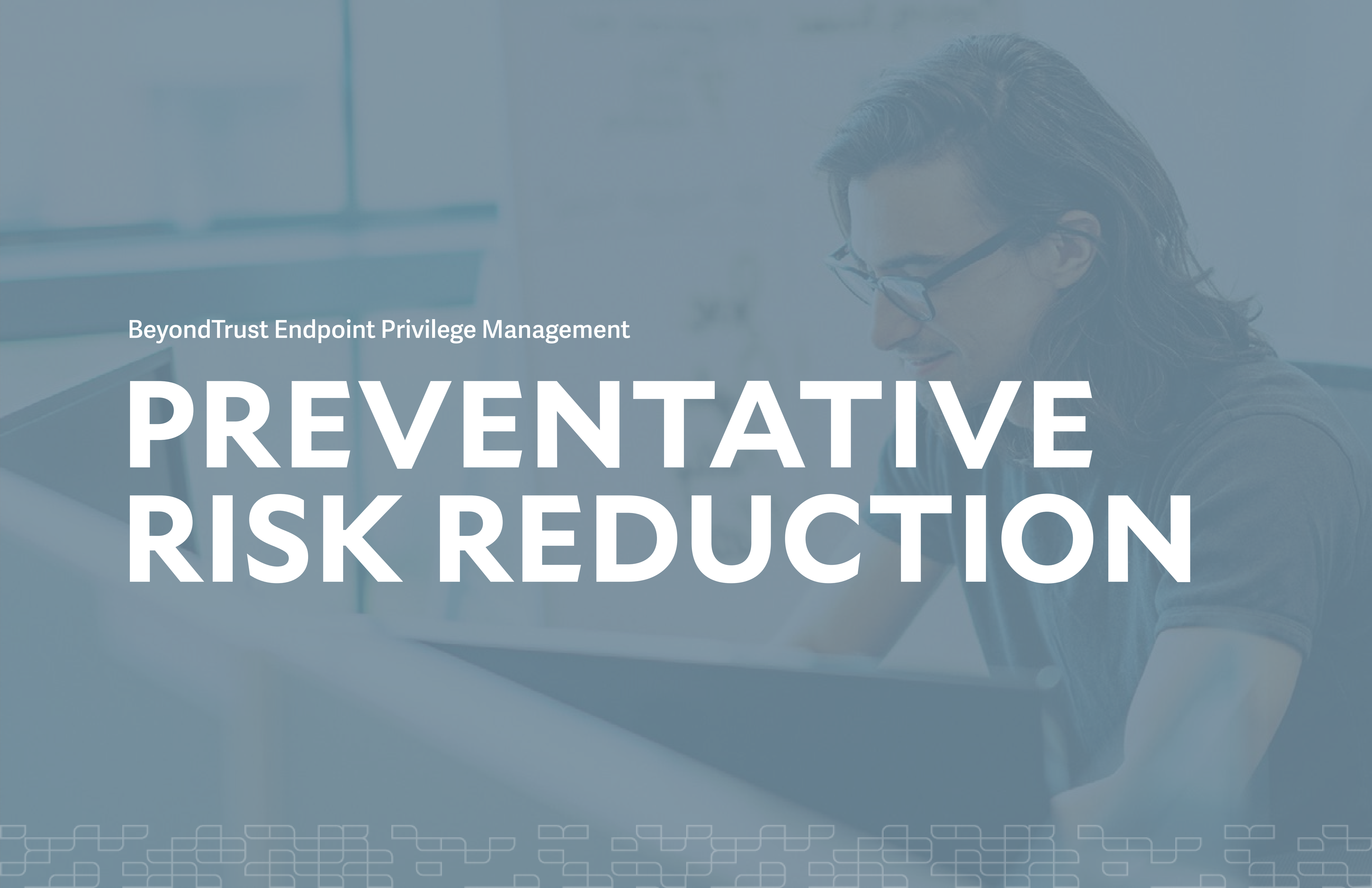
***Endpoint Privilege Management** makes all other Endpoint Security tools more effective by reducing the noise and minimizing the attack surface.*

Endpoint security strategies are not all one-size-fits-all. After your organization has implemented **Steps 1-4**, it's imperative to review specific use cases and evaluate other endpoint solutions based on needs.

**Some types of endpoint security tools to consider include:**

- Endpoint analysis solutions such as vulnerability assessment, log monitoring, and Security Information and Event Management (SIEM) solutions, are enhanced by Endpoint Privilege Management by ensuring only approved and patched applications get to run—reducing the noise in logs, and enriching data with privileged activity.
- Detection and response solutions including Endpoint Protection Platforms (EPP) and Web and Email Filtering applications also are complemented by EPM by preventing a significant portion of malicious activity from even occurring, allowing these tools to focus on a smaller amount of activity.

Additionally, there are many different types of Endpoint Security prevention tools that could also be considered by organizations in their journey to secure their endpoints. These include Data Loss Prevention, Encryption (endpoint and data security), Endpoint Hardening, Patch Management, Secure Configuration, Remote Access, and Web Proxy to name just a few. And, similar to all other Endpoint Security solutions, EPM dramatically reduces the attack surface by removing admin rights and preventing zero-day threats.



BeyondTrust Endpoint Privilege Management

# PREVENTATIVE RISK REDUCTION

## BeyondTrust Privilege Management for Windows & MacOS

A preventative Endpoint Security solution that removes administrative rights, gives users just enough privileges to do their jobs and be productive, and delivers fast, unmatched risk-reduction potential. Simplified deployment models available on-premises or via SaaS drive quick time-to-value and rapid adoption.

## Key Capabilities

**Least Privilege Enablement:** Restrict admin rights for users, accounts, applications, and computing processes to only those resources absolutely required for legitimate activities.

**Passwordless Administration:** Perform administrative functions on an endpoint without the need for privileged or administrator credentials with Just-in-Time (JIT) administration.

**Application Control:** Gain total control over what users can install or run with automated and elegant exception handling.

**QuickStart Templates:** Flexible, out-of-the-box workstyle templates let you implement least privilege policies in days, not months - working effectively for every role and across multiple operating systems.

**Trusted Application Protection:** The pre-built templates stop attacks involving trusted applications, catching bad scripts and infected email attachments - immediately stopping trojan horses, fileless attacks, and more.

**Power Rules:** Use PowerShell scripts to automate workflows, create custom behaviors, or build integrations with ITSM and other tools; integrated ecosystems mean better security positions.

**Enterprise Auditing & Reporting:** Provide a single audit trail of all user activity to streamline forensics and simplify compliance, and use graphical dashboards and reports for fast access.

> *We've got a team of six engineers who manage the entire desktop and mobile estate, so we needed something that was really going to empower them to get the job done in as quick and efficient way as we can, and using Endpoint Privilege Management has really allowed them to do that.*
>
> *—RYAN POWELL*
> *Operations and Response Centre Manager*

## Conclusion

The 5 Critical Steps to Endpoint Security enable a comprehensive, preventative approach to protecting all of the endpoints in your organization, whether office-based or remote. Enabling least privilege and allowing pragmatic application control are often overlooked but are crucial to achieving complete endpoint security.

BeyondTrust Endpoint Privilege Management solutions significantly reduce your attack surface and mitigate the chances of a breach by removing admin rights and taking a Passwordless approach. Through intelligent whitelisting and custom Power Rules, this can be achieved without hindering end user productivity or impacting your existing security ecosystem.

Using BeyondTrust as part of a layered, preventative approach to your endpoint security strategy ensures a frictionless user experience by giving the right level of access at just the right time.

## Additional Resources

- BeyondTrust Glossary: Endpoint Security
- Guide to Endpoint Privilege Management
- Microsoft Vulnerabilities Report 2020
- Quick Guide: Enable & Secure Your Workforce
- ON DEMAND DEMO: Privilege Management for Windows & Mac
- 2020 Gartner Magic Quadrant for Privileged Access Management

BeyondTrust

## 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 www.beyondtrust.com.