BeyondTrust

# 5 CRITICAL STEPS TO COMPLETE ENDPOINT SECURITY

*Karl Lankford*

*RVP, Solutions Engineering EMEIA*

# What is Endpoint Security?

**TRADITIONAL ENDPOINT SECURITY**

The process of securing mobile devices, laptops, desktops, servers, IoT, and POS and ensuring that they comply with certain criteria before being 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

- A compromised endpoint can give attackers **a foothold within an environment**, enabling them to launch further attacks on systems to access data and compromise more endpoints via lateral movement

- The traditional model has **multiple challenges** associated with achieving complete endpoint security

# 70%

## of Successful Breaches Started at the Endpoint in 2019

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

# Challenges with Traditional Endpoint Security

These factors leave organizations at risk of being ‘left behind’ when it comes to endpoint security:

- Continually evolving and more **advanced cyber threats**
- Increasingly complex and **diverse endpoint** environments
- Corporate **misalignment of security technologies** to threats
- Resource challenged **IT and InfoSec** teams that continue to be stretched thin

**350,000**

pieces of new malware are detected every day

## Consider This…

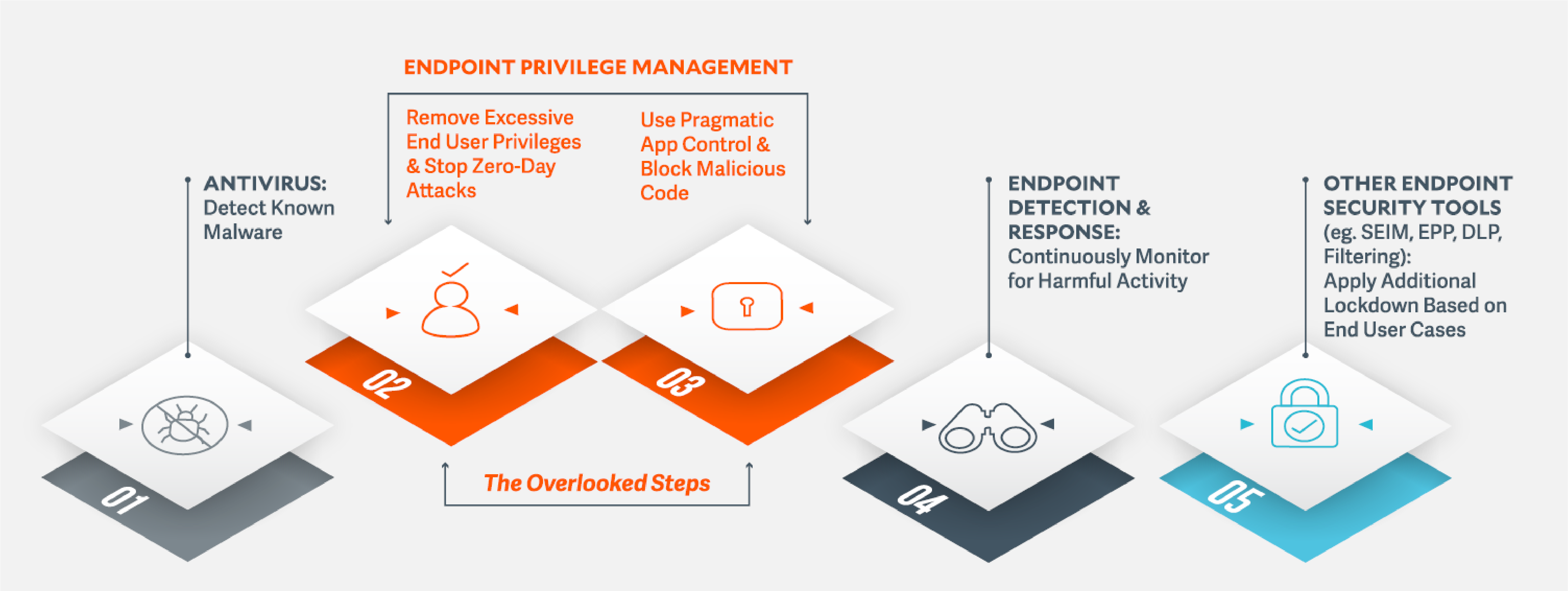
The year 2020 has been an unprecedented time, with the pandemic and ”new normal” for remote workers, creating a *perfect storm for privilege abuse* and changing the cybersecurity landscape forever

av-test.org

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

# 5 Critical Steps of Complete Endpoint Security

a preventive approach to endpoint security



ENDPOINT PRIVILEGE MANAGEMENT

**ANTIVIRUS:** Detect Known Malware

Remove Excessive End User Privileges & Stop Zero-Day Attacks

Use Pragmatic App Control & Block Malicious Code

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

**OTHER ENDPOINT SECURITY TOOLS** (eg. SEIM, EPP, DLP, Filtering): Apply Additional Lockdown Based on End User Cases

*The Overlooked Steps*

# ANTIVIRUS

Detect Known Malware

# 1. Antivirus: Detect Known Malware

- Many **companies still use antivirus alone** to secure their endpoints, but only catch 40% of known attacks
- For the threats that do bypass AV, some companies will **utilize Endpoint Detection and Response (EDR)** solutions to detect and then react to threats
- However, starting with combination of **Least Privilege** and **Application Control**, most malware and ransomware attacks will be blocked

60%
of attacks
are missed by
antivirus software

# ENDPOINT PRIVILEGE MANAGEMENT

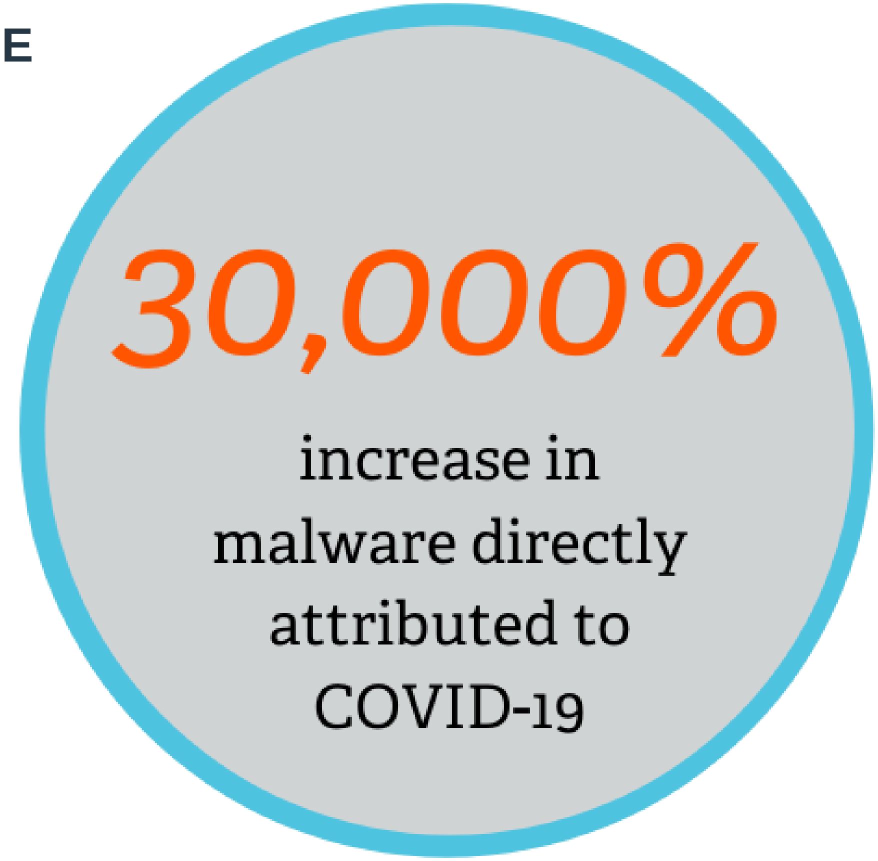
Remove Excessive End User Privileges & Stop Zero Day Attacks

Overlooked Step!

# 2. Remove Admin Rights & Stop Zero Day Attacks

## REDUCE THE NOISE EDR AND SHRINK THE ATTACK SURFACE

- With 40% of known threats covered by AV, it’s time **remove admin rights** from end users and give them *just enough* privileges to do their jobs
- Perimeter security is stronger than ever, making **end user devices heavily targeted** by threat actors
- Modern EDR will be optimized and **noise reduced** when layered on a **solid foundation of zero-admin rights**



30,000%

increase in malware directly attributed to COVID-19

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

# ENDPOINT PRIVILEGE MANAGEMENT

Use Pragmatic Application Control & Block Malicious Code

Overlooked Step!

# 3. Use Pragmatic Application Control & Block Malicious Code

- Not all malware needs admin rights
- Control what applications a user can run regardless of privileges by **defining good and bad applications**
- App Control improves security, compliance, and licensing management
- With admin rights removed, you can now trust critical operating system functionality making it easier to implement modern Application Control

**By layering Modern Application Control on top of Privilege Management, critical functionality in the operating system can now be trusted making Application Control easier and greatly reducing the attack surface**

# ENDPOINT DETECTION & RESPONSE

Continuously Monitor for Harmful Activity

# 4. Endpoint Detection & Response

**You have now successfully removed excessive admin rights and implemented and application control.**

## Now it's time to consider… EDR

- Designed to help organizations **identify and react to threats** that have bypassed their other defenses.
- Runs locally on user workstations or servers to monitor processes, applications, logged in users and **determines if malicious activity is present** on the system.
- Using EDR with EPM as the foundation prevents the execution of applications that need elevated privileges, allowing EDR tools to focus on a smaller amount of endpoint data

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

# OTHER ENDPOINT SECURITY TOOLS

Apply End User Lockdown Based on End User Cases

# 5. Other Endpoint Security Tools

- Endpoint security solutions are not one-size-fits-all
- Depending on your industry, compliance mandates, and systems – there are dozens of other endpoint security tools that should be considered
- It’s imperative that organizations review specific use cases based on specific needs

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

# KEY TAKEAWAY

Removing privileges and implementing application control with Endpoint Privilege Management makes all other Endpoint Security tools

***more effective***

by reducing the noise and minimizing the attack surface