



Traditional Antivirus (AV) vs. EDR (Endpoint Detection and Response)

Introduction

One every 11 seconds: the predicted frequency a business will fall victim to a ransomware attack by 2021.¹

Cyberthreats continue to rise, with COVID-19 creating an additional opportunity for would-be attackers to exploit. As an MSP, layered security is undoubtedly the best defense in the face of current and future threats to your customers' networks and end users.

Within that model, there are two solutions available to help protect the end user: traditional antivirus (AV) and endpoint detection and response (EDR). Both offer benefits to MSPs, but they do so with different levels of protection. Neither is a one-size-fits-all solution, with both solutions addressing different issues.

When deciding between the two, it's important to consider several factors, including the type of business in need of protection, the end users, cost, etc. SolarWinds MSP offers both solutions to help you provide the best level of service to your customers. We'll delve into each. If you would like a quick snapshot of the differences, we've included a summary chart at the end of this document.

¹"Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate," Coveware. <https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate> (Accessed September 2020).

AV: solid protection, ease of use, and lower cost

With AVs, MSPs handle automatic program updates and virus definition updates—so user intervention isn't necessary. When a virus or malware is discovered, it's immediately quarantined. It's a simple, straightforward first line of defense for employees—it doesn't require any technical knowledge and does a good job of turning away many threats.

However, AV does require regular definition (virus signature) updates. The protection afforded by the program is only as good as the vendor's updates. New threats arise daily, and ensuring updates get pushed out in a timely fashion is a best-effort scenario. Often, threats are discovered after the damage is done.

Given this critical issue, why choose AV? Clearly, ease of use is at the top of the list. Zero intervention on your customer's part makes this one less thing for them to worry about. It's a good value proposition at an affordable price point. Some additional benefits include:

- » **One management source:** The customer can look to the MSP as the single source for deployment, management, definition updates, and threat debriefings. This puts the MSP in a great position of trust, which can lead to additional revenue in other areas.
- » **"Locked-down" security:** AV program policy allows for zero intervention from the end user. They can't force an update or uninstall the program without the proper permissions.
- » **24/7 monitoring:** You set the scan schedule, update the software, and push out definition updates. Again, it doesn't require any intervention from your customers or end users.
- » **Fast remediation:** You can triage threats as they occur.
- » **Cost:** AV is less expensive per seat than EDR. This is the second biggest selling point for AV behind the effective protection aspect. But as we'll point out, the margins are becoming slimmer. And given the threat environment we face today, your customer might find themselves in a position where they can't afford not to pay for EDR.

EDR: major-league prevention and protection

EDR is a multifaceted solution that does everything AV can do but takes things a step further—providing greater security and (more importantly) peace of mind. These include, but are not limited to:

- » Monitoring
- » Threat detection
- » Whitelisting/blacklisting
- » Threat response
- » Integration with other cybersecurity solutions
- » Moving beyond threat detection and quarantine

Like AV, MSPs manage EDR without requiring any input from the end user. Given the number of threats that spawn daily, managing large numbers of endpoints can be more difficult with antivirus and other point solutions. *This is the point where the differences between AV and EDR come into sharp focus.*

EDR is proactive. Comprised of monitoring software and endpoint agents, integrated machine learning and advanced artificial intelligence (AI) allows EDR to identify threat vectors that exhibit suspect behavior and address them before they're acknowledged as harmful. Instead of relying on definition updates, it looks for abnormal behavior. For example, if several files change at the same time, it's likely due to an endpoint attack.

If you use SolarWinds® Endpoint Detection and Response (EDR), processing is done locally on the endpoint—unlike some other EDR vendors that require a resource and time-intensive uploads to the cloud for threat analysis and processing. You can recover quickly, in an automated fashion.

It's not enough to accept a threat has done damage—you want to ask yourself how and why we arrived at this point. This is where EDR really shines, with active root cause analysis. SolarWinds EDR provides true context via a “visual storyline” (see Figure 1).

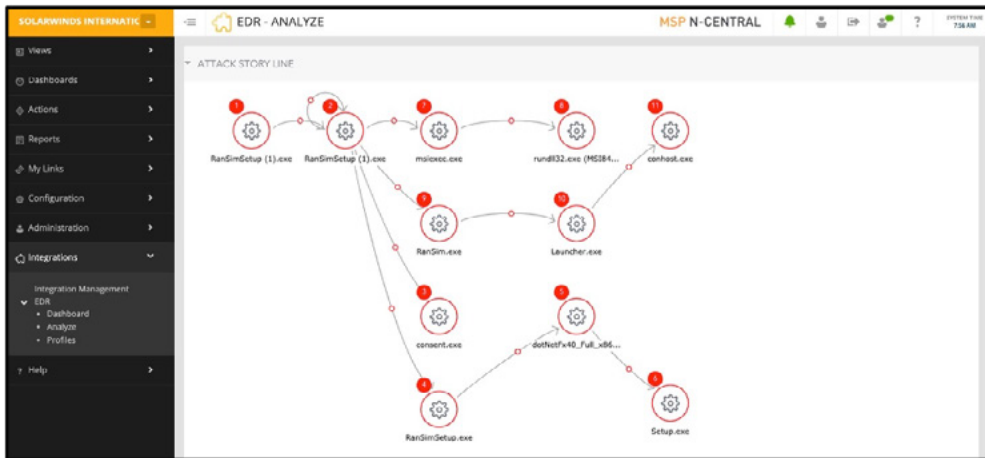


Figure 1: Visual storyline

You can see what process spawned the attack and how it replicated and spread. You'll also find answers to how the threat is constructed. This will drive actionable information to help the end user understand their part in allowing the threat to slip through, if applicable.

The storyline unfolds in real-time as an attack occurs, but with EDR, you're far from defenseless. Think of the EDR agent as your personal security operations center (SOC) analyst. Your recovery options include killing, quarantining, remediating, and rolling back the attack (see Figure 2)—depending on how you've set up the agent for each end user. In the event of a ransomware attack, you can restore an infected endpoint to its pre-attack state (Windows® OS only).

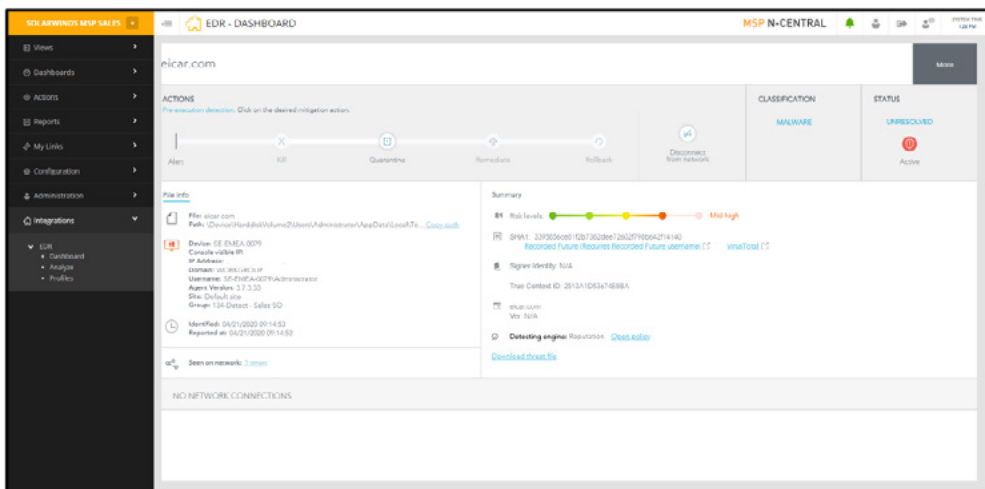


Figure 2: Kill, quarantine, remediate, and rollback actions

Protecting your devices: who are your users?

SolarWinds MSP offers both AV and EDR because one simple question determines which one you need. What kind of end users do you serve? For context, consider these personas:

- » **Human resources manager:** This person likely has personally identifiable information (PII) on their machine, which is confidential. If a cybercriminal accessed the PII during a breach, individuals and businesses could experience catastrophic damage. This is why we need to stop attacks in real-time, before they take hold and cause a lot of damage. EDR is the obvious choice for this type of end user. The risk and potential cost justify the additional expense.
- » **Marketing manager:** This individual probably has important files, but probably doesn't have customer PII on their machine. For this reason, a combination of AV, backup, and disk encryption provides a solid, layered defense. Choose AV for this end user and enjoy the lower cost since most users fall into this category.
- » **C-suite or other executive:** This person presents the greatest risk for a breach because both PII and highly valuable data to the business are likely stored on their machine. Not only do you need to protect that data, you need to be able to recover it with a rollback function. EDR wins.

The bottom line

To be objective in our assessment, we need to address the issue of cost. EDR does cost more per license than traditional AV—but not prohibitively so. Many customers may balk at the additional expense, but they may be in a position where they can't afford not to use EDR. If you'd like to read an example of the potential business costs to a customer who chooses to go without EDR, take a look at a recent [case study](#).

If your customer doesn't have endpoint protection, we recommend the EDR value proposition. They won't incur upgrade costs moving from AV to EDR down the line, and the added peace of mind more than justifies the choice. And for your servers, treat them the same as the high-value assets they host—EDR is your best choice.

If you do encounter resistance to EDR based on cost, consider focusing not on what the customer is losing by moving to EDR, but instead on what they are gaining—time. It typically takes less than a minute to do a rollback versus four to six hours to reimage each device—and you gain insight into what happened. Finally, if a breach does occur, there's a very real possibility you'll lose that customer.

One final point to note: EDR is not a substitute for backup. Without question, backing up your data and storing it off site remains a cyberhygiene best practice. Together, they're an incredibly effective one-two punch.

AV vs. EDR: at a glance

	AV	EDR
Context and forensic threat data available	Limited	Complete
Kill, quarantine, remediate, and rollback options	Kill/quarantine only	All
Leverages common vulnerabilities and exposures (CVE) system	No	Yes
Offline user protection	Requires updated definitions	Yes
Policy to allow/block USB devices by vendor/class/serial/product	No	Yes
Policy to contain threats by disconnecting from the network	No	Yes
Policy to control endpoint firewall settings	No	Yes
Resource-intensive	Moderate	Light
Helps defend against wrapper/variations/obfuscator threats	Requires updated definitions	Yes
Helps defend against fileless attacks	No	Yes
Helps defend against unknown and zero-day threats	Requires updated definitions	Yes
Uses signature-based detection	Yes	No

ABOUT SOLARWINDS

SolarWinds (NYSE:SWI) is a leading provider of powerful and affordable IT infrastructure management software. Our products give organizations worldwide, regardless of type, size, or IT infrastructure complexity, the power to monitor and manage the performance of their IT environments, whether on-prem, in the cloud, or in hybrid models. We continuously engage with all types of technology professionals—IT operations professionals, DevOps professionals, and managed service providers (MSPs)—to understand the challenges they face maintaining high-performing and highly available IT infrastructures. The insights we gain from engaging with them, in places like our **THWACK** online community, allow us to build products that solve well-understood IT management challenges in ways that technology professionals want them solved. This focus on the user and commitment to excellence in end-to-end hybrid IT performance management has established SolarWinds as a worldwide leader in network management software and MSP solutions. Learn more today at www.solarwinds.com.



For additional information, please contact **Form IT Solutions** on **01582 57 27 27** or email sales@formits.com

© 2020 SolarWinds Worldwide, LLC. All rights reserved

The SolarWinds, SolarWinds & Design, Orion, and THWACK trademarks are the exclusive property of SolarWinds Worldwide, LLC or its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks or are registered or pending registration. All other trademarks mentioned herein are used for identification purposes only and are trademarks of (and may be registered trademarks) of their respective companies.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of SolarWinds. All right, title, and interest in and to the software, services, and documentation are and shall remain the exclusive property of SolarWinds, its affiliates, and/or its respective licensors.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NON-INFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.