solarwinds

eBOOK

EDR vs. AV: What You Need to Know

Introduction

Layered security is the best defense in the face of current and future threats to your customers' networks and end users. Within that model, you'll hear two solutions discussed frequently for endpoint security—antivirus (AV) and endpoint detection and response (EDR). Both offer benefits, but how do you choose between the two? Will EDR come to replace traditional AV? Read on to learn more.

Either—not both

AV and EDR compete for resources, so running the two at the same time can cause problems. For that reason, we don't recommend using both AV and EDR on a given endpoint. It's best to choose one or the other for each endpoint.

When deciding between the two, it's important to consider several factors, including the type of business in need of protection, the end users, and cost. Some customers may need one or the other for their entire user base. Others may want to strategically deploy EDR for some users while using AV for the rest of their employees. Because of this, SolarWinds MSP offers both.

AV: solid protection at a great price point

AV protects customers against malware. SolarWinds® RMM lets you centrally manage AV protection across your customer base from a single dashboard, next to other layers. With AV, you can handle automatic program updates and virus definition updates on your customers' behalves—so user intervention isn't necessary. When a virus or malware is discovered, it's immediately quarantined. This has been the standard form of protection for many years, and the benefit is that most people understand what AV is, often making it simpler to sell.

AV does require regular definition (virus signature) updates though—and therein lies the rub. The protection afforded by the program is only as good as the vendor's most recent updates. New threats arise daily, and ensuring updates get pushed out in a timely fashion is truly a best-effort scenario. Threats can sometimes be discovered after the damage is done.

On top of this, AV solutions only protect against viruses and malicious software. However, there are more threats to endpoints than viruses. For starters, attackers increasingly use fileless attacks that simply can't be caught by AV programs. Plus, cybercriminals increasingly use evasion techniques to slip past AV. For instance, cybercriminals often use packers to encrypt malware and make them hard to detect or develop malware that changes its signature on a set cadence to avoid detection based on the existing virus signature database. In many ways, AV is a known quantity that criminals have worked for years to beat. This doesn't mean AV's powerless by any stretch of the imagination (many vendors still provide excellent coverage for a good portion of threats), but there are gaps to be aware of.

Given these critical issues, why choose to deploy managed AV at all? First, despite these issues, AV protection still offers protection against cyberthreats. So it still offers some benefits to end users. Plus, if you manage their AV protection for them, they won't have to think about doing it themselves. However, the biggest reason to choose MAV may be cost. MAV costs less per seat than EDR, so price-conscious customers may opt for AV. But it's worth noting that your margins on selling AV may become slimmer. Plus, as we'll mention in the EDR section, the upfront expense of EDR may be worth it compared to the significant costs associated with a successful attack or breach.

Here are some additional benefits for managed AV in SolarWinds RMM:

- **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. This can help prevent insider threats from users trying to install malware, but it also helps prevent someone from accidentally deleting or messing with their AV software.
- **Easy 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.

These benefits also apply to EDR, but you can offer them at a lower price point with AV.

EDR: taking endpoint security to a new level

EDR is a multifaceted solution that does everything MAV can do, but takes things a step further—providing greater security and (most importantly) peace of mind. 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 AV and other point solutions. This is where the distinctions between MAV and EDR come into sharp focus.

EDR focuses on endpoint protection, but detects more threats than just malware. Comprised of monitoring software and endpoint agents, integrated machine learning and advanced artificial intelligence (AI) allows EDR to identify suspicious behaviors and address them before they cause harm, rather than simply focusing on files.

While AV does a fantastic job of preventing malware, cybercriminals could attack endpoints via fileless methods. For example, if a hacker finds an open RDP port, they could use that vulnerability to create a new admin user on the machine, gain persistence on the machine, and make changes to the endpoint without the MSP or IT administrator being any the wiser (until it's too late). Traditional AV simply isn't designed to catch this style of attack. Or let's say several files start being modified all at once (and this is atypical for the endpoint); EDR solutions can flag that behavior, alert the administrator, and allow them to take action. And beyond this, it can help for emerging threats that haven't been discovered by the wider security community yet. A signature-based AV product can leave a gap in coverage here; EDR's signatureless approach prevents that gap.

If you use SolarWinds® Endpoint Detection and Response (EDR), processing occurs 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. Doing this allows you to detect threats faster and recover from threats even more quickly. You can rapidly recover, in an automated fashion.

It's not enough to accept a threat has done damage—you want to ask yourself how and why the endpoint arrived at this point. This is where EDR really shines with active root cause analysis. SolarWinds EDR provides true context via a "visual storyline." You can see what process spawned the attack as well as how it replicated and spread. You'll also find answers to how the threat is constructed. This provides actionable information you can use to help improve your customers' security posture.

The storyline unfolds in real-time as an attack occurs, but with EDR, you're far from defenseless. Your recovery options include killing, quarantining, and remediating (rolling back) the attack—depending on how you've set up the agent for each end user. Think of the EDR agent as your personal SOC (security operations center) analyst. You can literally undo the damage done, rendering ransomware useless.

Additionally, we mentioned earlier that AV may cost a little less per seat. While this may seem true at first, the potential downside of less robust protection could be enormous. For example, ransomware attacks are far more than nuisances—you have to factor in the productivity time, the cost of restoring endpoints, the reputational hit due to downtime, or even potential compliance fines under data breach laws. These costs can far outweigh the upfront cost. As threats continue becoming more dangerous and costly, EDR may eventually become the industry standard.

So to sum up, EDR solutions offer many of the same benefits as AV, but also offer:

- **Proactive detection:** While AV solutions require signature updates and scheduled scans, EDR solutions use AI and machine learning to detect potential threats, preventing a potential gap in coverage.
- **Wider protection:** EDR goes beyond detecting viruses and malware, offering protection against malicious traffic and fileless attacks.
- **Root cause analysis:** SolarWinds EDR, in particular, offers a visual attack storyline for suspicious behaviors. This gives you greater insight into the attack and allows you to adapt security processes and controls to prevent the issue from recurring.
- **Fast remediation:** You can also quickly remediate these threats in almost an instant. For example, when it comes to ransomware, you can roll back an endpoint to a known safe state straight from the EDR solution.

SolarWinds RMM with integrated EDR

SolarWinds RMM offers both managed AV and SolarWinds EDR from the same web-based dashboard. SolarWinds EDR uses AI and machine learning to detect threats and offers policy-driven remediation to help respond to threats on your behalf. It can even roll back an endpoint quickly to a known safe state after an attack, saving your customers significant time, money, and headaches due to ransomware.

And with SolarWinds EDR integrated in RMM, you can now offer your customers enhanced threat detection, monitoring, and fast remediation using SolarWinds EDR from the same solution you use to monitor and manage the rest of their IT infrastructure. With other integrated security layers, including patch management, email protection, web protection, and integrated backup, you can offer your customers greater security without stretching your team beyond their limits.

Learn more today about the SolarWinds EDR integration within SolarWinds RMM: solarwindsmsp.com/products/rmm/endpoint-detection-and-response

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.

solarwinds

For additional information, please contact SolarWinds at 866.530.8100 or email sales@solarwinds.com.
To locate an international reseller near you, visit http://www.solarwinds.com/partners/reseller_locator.aspx