

01001 000 001 001 1100 1001




eBOOK

EDR or Antivirus: Which Solution Is for You


EDR or Antivirus: Which Solution Is for You?

There are some significant differences between antivirus (AV) solutions and endpoint detection and response (EDR) tools. They may both protect endpoints from cyberthreats, but the way they do so differs. We've gone into detail in other eBooks on the stark differences, but we let's quickly recap them here.

Antivirus solutions:

- 
- Protect against malware and viruses. This typically requires a file to scan.
 - Rely on virus signatures, traditionally. This means the AV vendor must have discovered the malicious software, pushed a signature update to the user base, and the end user must have their virus signatures up-to-date.
 - Require the administrator to run scans on a regular basis.
 - Cost less than AV in general.

EDR solutions:

- 
- Protect against multiple threat vectors—including fileless attacks, malicious documents, and malicious scripts launched outside of a scan window—by using AI to focus on behavior.
 - Actively look for potential threats, rather than relying on scans. If it detects suspicious activity, it will alert you in near real time (if the alert is warranted).
 - Automate responses to potential threats. SolarWinds® Endpoint Detection and Response (EDR) even allows you to roll back Windows software-based endpoints to known safe states in an instant after a ransomware attack.
 - Cost a little more per seat than traditional AV.

When we talk about traditional AV and EDR, it might seem like EDR should be the only option, as it provides more comprehensive coverage and offers some upgrades on remediation options. However, there's room for both solutions in today's world. SolarWinds MSP offers both options so you can decide which works best for your customers. But how do you choose?

A risk-based approach

Offering the more comprehensive coverage afforded by EDR solutions can certainly improve a customer's security posture. If possible, you should sell this solution to your customers since it offers greater endpoint protection. Plus, you can charge more for the solution to offset the per-seat cost to your business.

But not every customer will want to pay the higher price tag. So, it's worth developing a pragmatic approach, and that means understanding customer risk and developing plans accordingly. While risk-based approaches often happen to conserve security and technology administrative resources or to offer a less intrusive user experience for end users (think strategically employing multifactor authentication for executives or sysadmins), risk can guide your decisions for financial resources as well.

Ultimately, you'll need to consider the users you're protecting, the access they have to sensitive data, and the consequences of losing that important data.

For context, consider these personas:



- **Human resources manager:** This person likely has personally identifiable information (PII) on their machine that needs to remain confidential. They will have access to payroll records, social security numbers, addresses, and potentially sensitive information on work histories. If a cybercriminal accessed this PII during a breach, individuals and businesses could experience catastrophic damage. As a result, an HR manager probably needs more robust protection than AV can offer—including being able to automatically kill a process, quarantine a file, and take the endpoint off the network to prevent the spread of the threat. In this case, EDR is the obvious choice. The risk and potential cost of a successful attack will justify the additional expense.



- **Graphic designer:** This individual probably has important files and documents, but probably doesn't have a significant amount of PII on their machine. Plus, their work may not be as time-sensitive as those in other roles, so if they needed to wait a few hours for you to reimage a disk, it would be a pain, but business wouldn't grind to a screeching halt in the way it might for a customer-facing service role. For this reason, a combination of antivirus, backup, and disk encryption provides a solid, layered defense. While EDR would offer great coverage, antivirus can still provide exceptional defense at a lower price point for this lower risk user.



- **C-suite or other executive:** This person may present the greatest risk if a breach occurs. For starters, they could easily have access to PII on their systems as well as highly valuable company data and intellectual property. Not only do you need to protect that data, you need to be able to recover it quickly with a rollback function. But consider another possibility. Imagine they remotely connect to the CEO's computer and either install spyware that's hard to detect or create a superuser admin account without the CEO knowing. This could give the cybercriminal significant power, potentially using access to further compromise the rest of the company. An EDR solution can help prevent these types of threats. Ultimately, for a high-risk user like someone in the c-suite, protecting their machines with EDR is a far safer bet.

When it comes down to it, you aren't locked into either solution. While EDR may offer better protection, if you need to make compromises, you can do so strategically.

The cost objection

To be objective, we need to address the issue of cost. EDR does cost more per license than traditional antivirus. In SolarWinds RMM, the per-seat cost for EDR may be higher than antivirus, but not prohibitively so. Some customers may balk at the additional expense, particularly if they feel everything's going well already. However, cybercrime continues increasing in both ubiquity and damage. Organizations may be unaware of the threats they face or the damage a successful attack could cause. For example, a ransomware attack could spread throughout a network very quickly, requiring significant time investments to rebuild the infrastructure from scratch. When EDR prevents an attack like this, it more than justifies the cost.

If your customer doesn't have endpoint protection in place at all, it's worth counseling them to take advantage of the EDR value proposition. Your customer 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 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 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. This can help you take countermeasures to prevent similar threats in the future, allowing you to offer robust proactive security services and truly be the consultant they need.

Finally, while AV certainly can still play a role, it's important to consider the risk to your own business of not pushing for the additional protection. If you face a breach, there's a definite possibility you may lose the customer. Your customers look to you as experts. Even if they're concerned with price, they do want you to solve their problems, including security. If you aren't pushing for more complete protection, you may risk a breach that could have you lose the customer. Some cost-conscious customers may simply not sign up for EDR protection and you may need to stick with AV to earn their business, but it's worth noting that your customer relationships may come down to offering more comprehensive protection.

The last word

There's certainly room for both antivirus and EDR. However, with the innovation offered by EDR and the way it meets the current threat climate, don't be surprised to see EDR solutions eventually replace AV as the industry standard. The cost differential is small enough that the gains may easily justify more widespread use of EDR solutions.

Finally, while the rollback feature in SolarWinds EDR can help in terms of ransomware, EDR does not replace a good cloud-based backup. Backing up data off-site and regularly testing recoverability should be part of any good cyberhygiene practice. Backup solutions protect against more than just these threats—they also protect against accidental or malicious data deletion by insiders, software and hardware failures, and acts of God, like natural disasters. Plus, rollback currently only works with Windows software-based PCs and laptops.

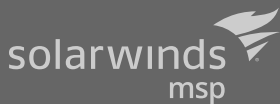
In the end, you have options on which solution you choose—EDR or antivirus. You can even mix and match as needed to meet customer demand. Regardless of what you choose, SolarWinds MSP can help.

SolarWinds N-central with integrated EDR

SolarWinds RMM offers both managed antivirus and SolarWinds EDR from the same web-based dashboard. Whether your customers want the expanded capabilities of EDR or they simply need antivirus, you can deliver those services across your customer base from the same web-based dashboard you use to monitor and manage their IT infrastructure. Plus, you can access other integrated security layers—including patch management, email protection, web protection, and integrated backup—to offer your customers greater security without stretching your team beyond their limits.

If you'd like to learn more about our SolarWinds EDR integration, visit:

solarwindmsp.com/products/rmm/endpoint-detection-and-response



Learn more today at
solarwindmsp.com

SolarWinds (NYSE:SWI) is a leading provider of powerful and affordable IT management software. Our products give organizations worldwide—regardless of type, size, or complexity—the power to monitor and manage their IT services, infrastructures, and applications; whether on-premises, in the cloud, or via hybrid models. We continuously engage with technology professionals—IT service and operations professionals, DevOps professionals, and managed services providers (MSPs)—to understand the challenges they face in maintaining high-performing and highly available IT infrastructures and applications. Targeted for MSPs, the SolarWinds MSP product portfolio delivers broad, scalable IT service management solutions that integrate layered security, collective intelligence, and smart automation. Our products are designed to enable MSPs to provide highly effective outsourced IT services for their SMB end customers and more efficiently manage their own businesses.

© 2020 SolarWinds MSP Canada ULC and SolarWinds MSP UK Ltd. All rights reserved.

The SolarWinds and SolarWinds MSP trademarks are the exclusive property of SolarWinds MSP Canada ULC, SolarWinds MSP UK Ltd. or its affiliates. All other trademarks mentioned herein are the trademarks of their respective companies.

This document is provided for informational purposes only. SolarWinds makes no warranty, express or implied, or assumes any legal liability or responsibility for the information contained herein, including for the accuracy, completeness, or usefulness of any information.