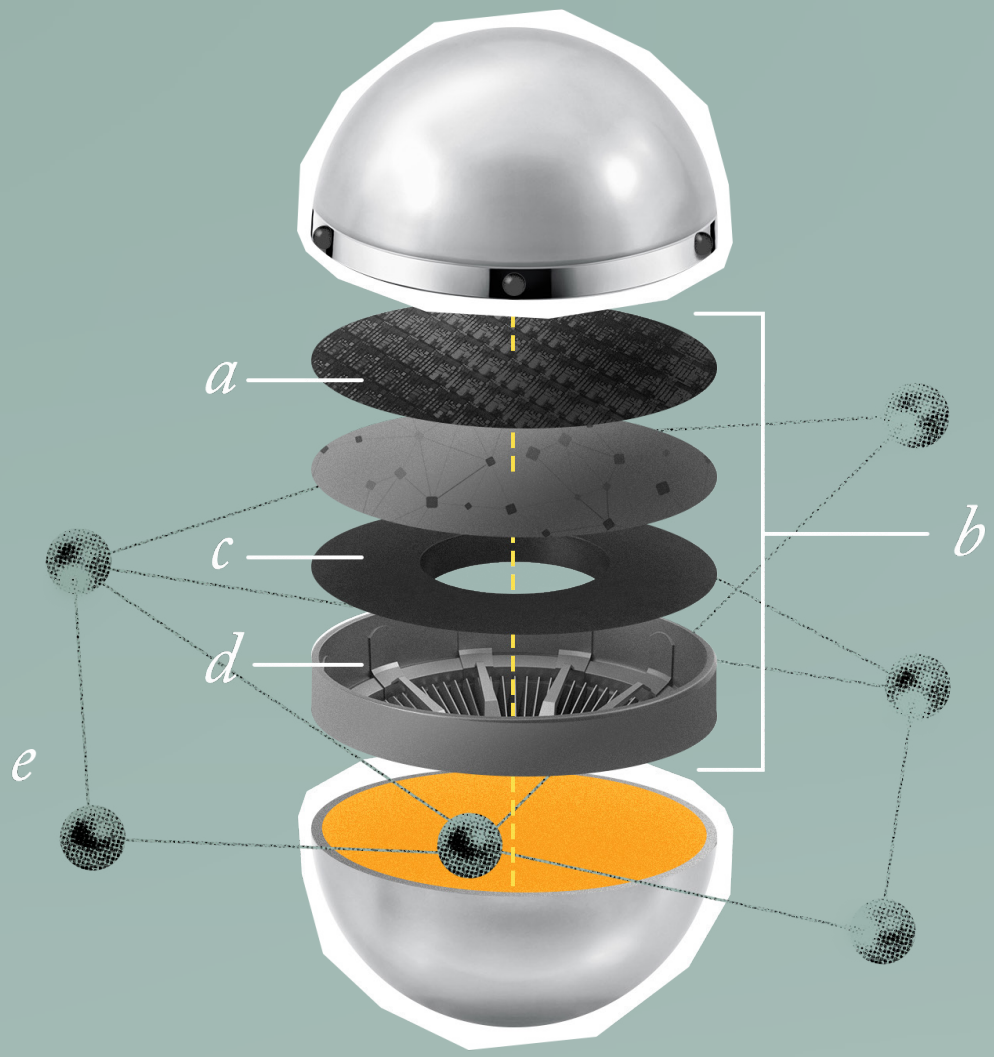
solarwinds msp



eBOOK

Endpoint Detection and Response Demystified

Ransomware. Zero-day malware. Fileless attacks. Phishing and privilege escalation.

These all represent clear and present dangers to your customers' networks, businesses, and personally identifiable information (PII).

For years, antivirus (AV) solutions were the major players on protecting customer endpoints. But as the threat landscape has shifted, we've seen the emergence of newer solutions built to deal with some of the problems inherent in AV.

You may have heard the term "endpoint detection and response (EDR)" crop up over the past few years. These solutions were put on the market specifically to adapt to the evolution of the threat landscape (and to recognize it will continue to evolve faster than humans can often keep up). You may be curious about what these solutions are and why they stand apart.

We'll demystify these solutions today and, hopefully, show you why they're so integral to the future of cybersecurity.

WHAT EXACTLY IS EDR?

Anton Chauvin of Gartner® originated the term "endpoint detection and response," using it to describe a, "family of new tools focused on visibility, and from prevention to detection for the endpoint."[1] EDR is a multifaceted solution that can best be described as expanding AV into a whole new realm.

Everything modern AV can do, EDR takes 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

Whether it's from using artificial intelligence (AI) to monitor for new threats or suspicious endpoint behavior or automated roll back after a ransomware event as a part of threat responses, EDR solutions have developed multiple responses to increase the depth of protection IT providers and IT professionals can offer their users.

Let's take a closer look at this new weapon made for your cybersecurity arsenal.

[1] "A Short History of EDR," Reed Exhibitions Ltd. infosecurity-magazine.com/opinions/history-edr/ (Accessed September 2020).

EDR'S PLACE IN THE CYBERSECURITY UNIVERSE

EDR centers on protecting endpoints. Given the number of threats that spawn daily, AV and other traditional endpoint security products can fall short for managing attacks across large numbers of endpoints. When we talk about traditional AV, it's typically from a passive standpoint. AV can only detect and quarantine known threats—those that have been previously identified.

Many AV solutions operate on traditional virus signatures. When a file gets discovered as malware, it generates a hash that then gets added to a virus signature database. AV programs then scan for files that match a known virus signature in their database, then quarantine the file.

Therein lies the rub—AV requires regular signature updates. This means there is often a gap in coverage between when a virus is discovered and when your customers become protected. Plus, threats that haven't yet been discovered can operate in the wild before you can even get an update. *It's a reactive approach.*

In contrast, EDR is proactive. Comprised of monitoring software and endpoint agents, EDR solutions use integrated machine learning and advanced artificial intelligence (AI) to identify suspicious behaviors and address them regardless of whether there's a signature. For example, if several files change at the same time, chances are it's more likely a result of an endpoint attack rather than user error.

AV can only detect and quarantine known threats—those that have been previously identified.

Cybercriminals themselves have been proactive. Many cybercriminals have developed methods of evading traditional AV solutions. Some might develop malware that changes signatures regularly to avoid matching a known signature in an AV database, while others may use fileless attacks and set up a new admin account on an endpoint with strong privileges. An EDR solution looks for unusual behaviors on an endpoint (compared to a baseline), then takes action accordingly. This allows you to meet proactive cybercriminals with proactive defenses.

THE ONLY CONSTANT IS CHANGE

The world is in a constant state of flux, and technology is no different. The cloud has changed our lives in immeasurable ways, from the rise of ecommerce to enterprise-based solutions that billions of individuals rely on daily. Yet, as technology advances, cybercriminals find new ways to exploit these changes and compromise company data. Data is arguably your customers' greatest asset—so how do you help safeguard that asset?

Like the cloud, artificial intelligence and machine learning promise to change much of the way we do business and live our lives. AI and machine learning power EDR solutions, acting as the engine that fuels greater threat protection and allows it to recognize and deal with advanced threats.

An EDR solution uses machine learning to establish a baseline of behavior for an endpoint. From there, EDR discovers behaviors that veer from the baseline. This is where EDR excels—asking questions like:

- Has this endpoint performed this activity before?
- Does this file or behavior exhibit unusual patterns?
- Why are secured files being looked at or hit?

In essence, EDR solutions use AI to discover indications of a compromise without having to rely on known indications of compromise (which can be subverted). Advanced polymorphic viruses (those that can generate modified versions of themselves to counter detection) and zero-day threats (which target and exploit a previously unknown vulnerability) will slip by solutions that can't ask and answer these questions. EDR not only asks these questions; it also provides the answers we need to address the threats—with options to kill, quarantine, remediate, and roll back.

HOW EDR SOLUTIONS CAN RESPOND TO THREATS

EDR solutions don't just detect threats—they can also act on them. When an endpoint agent discovers a threat, a good EDR solution springs into action via the central monitoring system. The central monitoring system analyzes and correlates threats. Depending on which EDR solution you use, you can even visually trace the genesis of the threat and its path to the endpoint. SolarWinds® Endpoint Detection and Response (EDR), for example, lets you see this attack timeline so you can understand the lifecycle of the attack. You can use this information to help you prevent future threats, but it's also extremely helpful in showing tangible proof of the value of your security services to customers.

While AV and disk encryption are valid ways to secure your endpoints, EDR offers capabilities that help futureproof your users' machines. These include near real-time file analysis and alerts, detailed forensics, offline protection, the ability to disconnect from the network to help prevent further spread, and the killer feature—infected file rollback.

In fact, let's look at how a solution like SolarWinds EDR can help with ransomware. The common drill with ransomware goes as follows: someone opens an attachment or email, or visits a webpage with malicious script,

and they're greeted with a notification that all their files are encrypted. The cybercriminal will only return their files after they pay a princely sum in Bitcoin or another cryptocurrency—except there is no guarantee they will get their data back. Many corporations are unwilling to risk paying a ransom because of this lack of a guarantee.

It can happen to anyone, and the facts are staggering:

- Businesses experienced an average of 16.2 days of downtime at the end of 2019 due to ransomware[2]
- One business will be hit every 11 seconds by a ransomware attack by 2021, according to some predictions[3]
- The predicted cost of damages due to ransomware in 2021 is $20 billion[4]

SolarWinds EDR offers ransomware rollback to help you offer the greatest value to your clients. This feature uses advanced technology to take "snapshots" of the endpoint at regular intervals (set at the administrator's discretion). If ransomware hits, it only takes a few clicks to roll back the endpoint disk image to a previous point in time, helping save your customers significant time and money.

IS AN EDR SOLUTION RIGHT FOR YOU AND YOUR CUSTOMERS?

Before you deploy EDR, you should consider your own capabilities and the needs of your customers. As we've mentioned before, EDR is not the only way to secure an endpoint. Look at your data and the use cases. While EDR is perfect for someone who manages sensitive human resource data (which often includes PII), it may not be necessary for someone who simply stores personal files in the cloud or has a solid backup client combined with disk encryption and AV.

However, even if you have price-sensitive customers who want to fall back on other solutions, it's worth having a conversation with them about EDR. It's up to you, but you may want to consider strongly recommending (or even requiring) the use of EDR for your customers. For starters, the ransomware rollback feature could be worth its weight in gold. If someone gets hit by a ransomware attack, SolarWinds EDR could detect it, stop it cold, restore the endpoint in seconds, and prevent it from spreading across the network. This could help prevent a major downtime event and save the end customer a significant amount of time and money. Plus, EDR offers more complete protection than an AV solution can on

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

[3] "Global Cybercrime Damages Predicted to Reach $6 Trillion Annually by 2021," Cybercrime Magazine. cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ (Accessed September 2020).

[4] "Global Cybercrime Damages Predicted to Reach $6 Trillion Annually by 2021," Cybercrime Magazine. cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ (Accessed September 2020).

its own. EDR isn't the only way to secure a customer, but it's worth having the conversation and potentially pushing for more complete protection.

SOLARWINDS EDR AND SOLARWINDS RMM

SolarWinds EDR uses artificial intelligence and machine learning to detect endpoint threats. Not only can it detect suspicious behaviors at the endpoint level, it can also respond to those threats on your behalf based on set policies. You can even set it to automatically roll back endpoints to a known safe state after a potential attack and show you full attack timelines that let you show your customers in a *tangible*, clear way that you've protected them from threats.

Plus, SolarWinds EDR is integrated within SolarWinds RMM, our remote monitoring and management platform designed to help get up and running fast and start monitoring devices in minutes. This means you can monitor and manage your customers' endpoints and networks from the same dashboard as their endpoint security. Plus, SolarWinds RMM offers multiple other security layers available from the same dashboard, including patch management, email protection, web protection, backup, and disk encryption. It's easy to get started—and it's built to grow with you.

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

solarwinds msp

Learn more today at ***solarwindsmsp.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.