N-ABLE™

Endpoint Detection and Response Demystified

eBook

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 for 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 might 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 evolving threat landscape—and in the recognition that the landscape will continue evolving faster than humans can keep up. You might be curious about what these solutions are and why they stand apart.

Here, we'll demystify these solutions and explain why EDR is 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 expands AV into a whole new realm. Everything modern AV can do, EDR takes a step further, providing greater security and peace of mind. EDR features include, but are not limited to:

- Monitoring
- Threat detection
- The ability to list and deny/exclude listing
- Threat response
- Integration with other cybersecurity solutions

EDR solutions have developed multiple responses to increase the depth of protection IT providers and IT professionals can offer their users—from the use of artificial intelligence (AI) to monitor and detect new threats or suspicious endpoint behavior, to automated rollback after a ransomware event.

[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 focuses 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. Traditional AV is passive—it can only detect and quarantine known threats that have been previously identified.

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

In contrast, EDR is proactive. Comprising 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 the result of an endpoint attack rather than user error.

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

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

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 e-commerce 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 about 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 viewed or hit?

In essence, EDR solutions use AI to discover indications of a compromise without having to rely on known indications of compromise that 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, can slip by traditional AV solutions. EDR not only asks all the right 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. Seeing the attack timeline helps you understand the lifecycle of the attack. You can use this information to help prevent future threats. It's also extremely useful for providing 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—most significantly—infected file rollback.

Let's look at how EDR can help with ransomware. A common ransomware scenario goes as follows: someone opens an attachment or email or visits a webpage with malicious script. Suddenly, 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. Of course, there's no guarantee they'll get their data back, which is why many corporations are unwilling to risk payment.

EDR with ransomware rollback capabilities offers huge 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 already noted, EDR is not the only way to secure an endpoint. Look at your data and use cases. Although EDR is perfect for someone who manages sensitive human resource data (which often includes PII), it might 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. You might want to consider strongly recommending (or even requiring) the use of EDR for your customers. For starters, a ransomware rollback feature could be worth its weight in gold. If someone gets hit by a ransomware attack, EDR could detect the attack, stop it cold, and restore the endpoint the endpoint in seconds, preventing the ransomware from spreading across the network. This could help prevent a major downtime event and save the customer a significant amount of time and money. Plus, EDR offers more complete protection than an AV solution can on its own. EDR might not be the only security option, but it's worth having the conversation with your customers and potentially pushing them toward more complete protection.