N-ABLE™

AV to EDR

What You Need to Know

eBook

Introduction

Your customers want their networks and end users protected. The best defense? Layered security. But don't worry, unlike an onion these layers prevent you from crying. Antivirus (AV) and endpoint detection and response (EDR) both help keep your customers' software safe, but in their own unique way.

So how do you know which one you'll need? And will EDR ever replace AV?
Don't stress, the answers are simple.
Read below to find out.

AV:
A protection only as good as its updates

Simply put, AV protects customers against malware and helps you update automatic programs and virus definitions so your customers don't have to. So, if malware or a virus ever pops up, they're automatically quarantined. That's why AV has been the standard for virus protection for years, and why customers know all about it.

But that doesn't mean it's without flaw. While AV helps protect against viruses and malicious software, these are only a few of the many endpoint threats. And though AV is currently top dog, it still requires regular definition (virus signature) updates. That means that your customers' AV is only as good as its most recent update, and crafty cybercriminals frequently use evasion techniques to slip past. Sadly, most threats that do get past AV are identified after the damage is already done.

Following are five types of attacks using evasion techniques.
Read through them to understand what you're up against more clearly.

Five evasion attack techniques that can slip past your AV

1 Polymorphic malware

Though useful, AV programs may not be as bulletproof as you might think. Many traditional AV programs rely heavily on signature-based detection. That means it compares a file against a known entry (or signature) in a database of known threats, key word: "known".

In order to function correctly, the AV user needs the most recent list of signatures which requires frequent updates on their part. But if that user hasn't kept their virus definitions current, they'll be defenseless against newer files. That's why it's crucial the AV company knows about the signature before they can flag it to their user base. Cybercriminals know this and that's why they create malware that avoids AV detection.

A favorite of cybercriminals? Polymorphic malware. A method specifically designed to exploit these AV blind spots. Even just a simple gap in coverage can cause malware mayhem. Let's say your AV program detects the malware. That's great, but the attack will still regenerate itself using new characteristics that purposely don't match the signatures your AV is reliant upon. Now the infection is underway.

2 Weaponized documents

Cybercriminals sometimes prefer this death by papercut method because they can weaponize your own documents against you when they manipulate the code (script). It's a stealthy attack that doesn't just fly by AV but runs in the background without the user ever knowing.

Cybercriminals can use documents like Adobe® PDFs with embedded JavaScript® to execute operating system commands or download executables to compromise the devices and networks they access.

They can also use embedded scripts to execute PowerShell® commands. This is important because these commands are built-in to the Windows® operating system and can infect not only endpoints but entire networks. These tactics can also expose XML, HTML, and Office® documents and slip right by AV solutions that compare executable signatures. AV only scans the initial document, not the malicious code the document launches.

3 Browser drive-by downloads

Ever download something from your browser but see a flurry of downloads right after? That's where cybercriminals can thrive. These are called "drive-by downloads", a tactic where harmful files are downloaded to the endpoint through browser vulnerabilities. And it's not as obvious as avoiding sketchy websites because legitimate websites could have a compromised script or ad service too. These downloads can come from all angles. Emails, social phishing, or hidden pop-up links can lure users to a website. Once the criminals find a way in, they'll leverage exploits in browsers or plugins to download malware and attack.

4 Fileless attacks

AV needs files to inspect to keep your system secure, but what if there were no files to detect? Cybercriminals can use fileless attacks to sneak by AV without being detected. Crazy right? And they don't even need to install an actual payload on a system. These attacks can infect machines in the endpoint's memory using PowerShell, rundll32.exe, or other built-in systems.

Yet these fileless fakes have even more tricks up their sleeves. For example, when a computer uses remote desktop protocol (RDP), it opens a listening port on the machine that allows someone to connect. Now hackers can run malicious processes like downloading actual file-based malware, changing the registry, or stealing data.

5 Obfuscated malware

AV companies have many methods to discover malware. One involves executing files in sandbox environments and digging through it for malicious behavior. Another involves scanning the code for common signs of malicious intent.

But cybercriminals have found ways around this. In the same way security professionals protect their assets, hackers can also protect malicious payloads within malware.

Newer malware can even detect a sandbox environment and remain benign, waiting to attack in a live setting. After this, it becomes nearly impossible for the AV to detect the malware after it's buried in its new sandbox environment.

Another method criminals use to attack AV involves "packers". This cybercrime gameplan uses encryption or compression to prevent someone from seeing within the file. Ever feed a pill to a dog by wrapping it in a piece of cheese? Same concept. The malicious code may also be wrapped, but within benign code to hide the injurious contents.

Cybercriminals wear many hats, so spotting their hidden attacks is getting increasingly difficult. Sometimes, AV protection can do more harm than good. For example, AV programs use heuristic scans within a sandbox environment, but this can actually help the malware evade detection before it goes live on a machine.

EDR:
The next level of endpoint security

The idea of cybercriminals creeping past your AV and into your systems can make anyone paranoid. We get it. Luckily, EDR is the multifaceted solution that gives you the usual AV benefits but offers many more for advanced security.

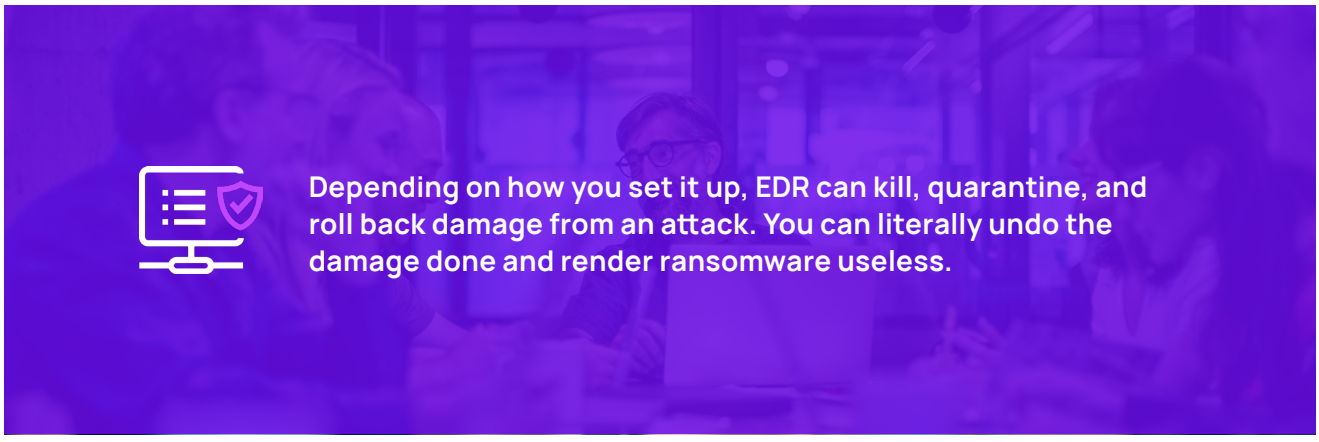
EDR doesn't just deliver greater security but peace of mind. Like AV, MSPs manage EDR without requiring any input from the end user. Cyberthreats spawn daily, so managing several endpoints with traditional tools like AV can be a headache and a security risk.

EDR is your software security multitool. It not only focuses on endpoint protection but can spot more threats than just malware. Comprising monitoring software and endpoint agents, integrated machine learning and advanced artificial intelligence (AI), EDR is built to stop the attack before it ever happens. Remember the fileless attacks? AV won't spot them, but EDR has them under a magnifying glass.

Suspicious activity? EDR can catch that too. Let's say multiple files are modified on an endpoint at the same time. EDR solutions can flag that behavior, alert the administrator, and allow them to stop it. EDR can even detect emerging threats that haven't been discovered yet, while signature-reliant AV is helpless in these situations.

Many AV users find themselves wasting time and resources dealing with slow uploads to the cloud in order to detect threats. EDR can get you that time back by processing locally on the endpoint, which allows you to rapidly detect threats and automate recovery.

But what about the damage that has already been done? You'll need to know how and why the endpoint was compromised. EDR shines here as well with active root cause analysis. EDR simplifies your problems via a "visual storyline", sort of like a picture book, where you can see what process spawned the attack, how it replicated and spread, and even how the threat is constructed. Now you can use that valuable information to improve your customers' security moving forward.



AV to EDR wrapped up

AV has long been the standard and is certainly better than nothing. But EDR is the future of software security and fast becoming the new standard for these reasons:

- **Proactive detection:** EDR combines the brainpower of AI and machine learning to detect potential threats and close the usual AV coverage gaps.
- **Wider protection:** EDR isn't one dimensional. It not only detects viruses and malware but also protects customers against malicious traffic and fileless attacks.
- **Rapid threat investigation:** EDR helps you step back and analyze the entire threat activity chain from root cause to lateral movement. This gives you greater attack insight and adapts security processes and controls to prevent the issue from recurring.
- **Fast remediation:** EDR turns back time on ransomware attacks by rolling back an endpoint to a known safe state straight from the EDR solution.
- **Resource lite:** EDR saves you time and reduces the recurring scans and updates. Users can feel protected from anywhere while working offline.

So, you may wonder, why employ AV at all if cybercriminals have figured out how to beat it?

AV still protects end users against known cyberthreats, so your customers will still need help managing that basic protection. But the main reason AV is still widespread is because it costs less per seat than EDR. And while the cost is attractive, the drain on your resources and potential downside of AV protection flaws could negatively affect your business in the long term. You can be sure breaches like ransomware attacks won't be overlooked by your current or prospective customers. In the end, the expense of EDR is frequently the more cost friendly option.