cybereason

When Next-Gen AV Meets EDR: Overpowering Advanced Threats

Overpowering today's attackers and responding to threats requires EDR plus NGAV. The bad guys treat all of an organization's machines as possible entry points. EDR plus NGAV takes this concept and uses it to the defender's advantage by using all of a company's endpoints for protection.

New threats curb antivirus' effectiveness

For several years, protecting endpoints meant using antivirus (AV) software. These programs, which are commonly referred to as AV, are designed to detect malicious programs, prevent them from executing and provide security analysts with a way to remove malware. Antivirus was designed as a mouse trap to identify malware based on signatures. Signatures are a unique string of bits, or the binary pattern of a specific malware. They're like a fingerprint that can be used to identify malware. Antivirus software contains a library of signatures and uses them to identify malicious code.

Every time new malware is discovered, antivirus vendors add its signature to a blacklist of applications. Blacklists are lists of application signatures that are denied system access and prevented from installing and running. Antivirus software works by looking for these signatures and blocking the program from executing.

Antivirus software and its signature-based detection approach worked well for detecting older malware that had already been identified and labelled by security researchers. As long as the malware was known, your vendor promptly added signatures to its software and you kept your antivirus updated, you were protected.

But attackers and their tactics have evolved. Malware is no longer the only weapon in their tool kit. The threats today's security teams face include advanced persistent threats and ransomware attacks. There are also targeted attacks, which use tailor-made, never-before-seen malware variants; fileless malware attacks, which do not use any malware; and zero-day exploits that leverage unknown vulnerabilities in software installed on the endpoint. Unfortunately for the defenders, all of these threats can bypass antivirus detection mechanisms.

Even the development of malware has evolved. Attackers run their own QA labs that test their newly developed malware against antivirus products, releasing the program only after it can evade antivirus software. Plus, attackers are developing new malware strains faster than vendors can add the signatures to their antivirus programs. Some malware is even designed to be polymorphic so they automatically generate a new hash as they spread, making detection by signature irrelevant.

What does this ultimately mean for antivirus software? As the threats grow more advanced, the less successful these products are at blocking them.

Why keep using AV?

So why do companies continue to use antivirus software if it's ineffective against today's attackers? The first reason is simply because antivirus software is required for legal and compliance reasons. The Payment Card Industry Data Security Standard (PCI DSS), for example, requires organizations to install and update antivirus software on all machines that store, process or transmit credit card information. And for companies in less regulated industries, foregoing antivirus programs makes them look irresponsible, opens them to lawsuits if a security incident causes damage and could jeopardize their ability to collect breach insurance. So whether your business is regulated or not, there's a need for antivirus software.

And while antivirus cannot catch advanced threats, it does provide some level of protection. There is still a lot of known malware out there so as long as the program can identify a malware signature and prevent it from executing, it's worth using. Even if antivirus blocks only half of the threats a SOC handles in a day, that still helps security teams by allowing them to focus on the other half of those threats.

Just don't expect antivirus to be an organization's only line of defense. Even antivirus vendors acknowledge that antivirus is now just one tool in a defender's arsenal and needs to be used with other products, like technology that monitors endpoints for odd behavior.

What's next for AV?

With antivirus software being unable to address enterprise security needs, vendors begun offering next-generation antivirus, anointing it as the successor to the legacy product. While the definition of antivirus is established, there's no accepted meaning of what constitutes next-generation antivirus (NGAV). At a minimum, next-generation products need to go beyond just performing signature-based detection and incorporate some type of advanced technology.

Also open to debate is whether next-generation antivirus can replace standard antivirus. If the next-generation product can perform signature-based detection in addition to using advanced technology then, in theory, the switch can be made. But if the next-generation product just offers detection through advanced technology and doesn't include traditional antivirus capabilities, then one can't replace the other. Companies still need protection from known, older malware threats.

Ideally, a next-generation product should be able to replace a legacy antivirus solution. Agent fatigue is huge challenge companies face. Many organizations refuse to add an additional endpoint agent to a machine unless it can replace an agent that's already being used. More agents running on machine means more agents to manage, giving more work to already busy IT and security professionals. Adding agents to machines also risks a computer's ability to function. Agents don't always work well with software that's already installed on a computer, causing machines to crash. And when workers can't use their computers because an agent crashed it, user productivity and business functions suffer. Enterprises prefer to have one agent that can perform traditional antivirus detection and offer next-generation capabilities.

Using a next-generation antivirus product also provides organizations with the opportunity to get a better return on their endpoint security budget. Purchasing a next-generation antivirus product that also handles legacy antivirus functions allows a company to spend the allocated antivirus budget on a better solution that can protect against advanced threats.

The limitations of NGAV

AV and NGAV share the same flaws

Even with advanced technology, next-generation antivirus products still look for certain file attributes that are associated with malicious activity. This is equivalent to scanning an endpoint for a list of specific attributes and labelling a program malicious if it contains them. In this way, next-generation antivirus and signature-based detection share the same fatal flaw. Both approaches entail looking for specific characteristics and don't account for human ingenuity. Opponents will adapt and eventually figure out how to get around next-generation antivirus. Neither the legacy product nor its successor offer true behavioral detection.

Looking at one machine at a time

Many NGAV products lack the ability to cross-correlate data from multiple endpoints and only know what's happening on one machine. Cross-correlating data from multiple endpoints can generate a full attack story, allowing defenders to understand the entire attack campaign and fully remediate the threat. Only looking at data from one machine gives an incomplete attack story, leading to partially remediating the threat and still leaving the company vulnerable to the attack.

So while greater endpoint visibility is provided with NGAV, companies still have no way of knowing if a strange process on one machine is connected to an odd process running on another computer and, if reviewed together, indicate malicious activity. This is a very siloed approach to security. And, unfortunately, attackers don't work alone in silos. They operate as teams and work together to use multiple entry points to get into an organization. NGAV needs to operate in a similar manner and leverage all of an organization's endpoints working together to protect the entire environment.

Focus only on prevention

NGAVs focus only on preventing attacks. For the attacks that NGAV can't prevent, these solutions offer little or no visibility into what actually happened. Companies gain very little insight into what tactics, techniques and procedures the attackers used to infiltration the environment. They don't help with investigation, forensics or any remediation activities.

Plus, prevention is only one part of the modern security equation. Companies need a way to detect attacks, stop adversaries that have already gotten past a company's defenses and remediate an incident. But NGAV lacks these functions. While prevention is great for helping a SOC figure out what security concerns are legitimate, additional capabilities are needed to handle what happens when prevention can't stop a motivated and sophisticated adversary.

EDR+NGAV=The holistic approach

Organizations need to detect advanced threats and stop known malware as well as detect and immediately respond to threats that get past their defenses. The best way to get this protection is by using a product that combines EDR with NGAV.

EDR technology takes a proactive approach to security. Unlike traditional security products that react after a threat is detected, EDR technology monitors endpoints in real time and hunts for threats that have already infiltrated a company's defenses. EDR also offers greater visibility into what's happening on endpoints, a superior level of attack context and mechanisms for immediately remediating an attack. Adding EDR to next-generation antivirus allows for behavioral-based threat detection, which is a superior way of detecting malicious operations. Unlike signatures or attributes, behaviors are much more difficult and costly for attackers to change.

An example: How combining the strengths of EDR and NGAV can handle modern threats

Let's assume that a legacy antivirus or even NGAV solution detects an unknown executable on a single machine. Based solely on the executable's properties, the antivirus software must determine if the executable is malicious and should be allowed to run. However, since neither solution has cross-correlation abilities, only data from a single endpoint is collected. These technologies ultimately fail to provide enough information to determine if the executable is malicious.

Here's how that same scenario would play out using a product with EDR plus NGAV that collects and cross-correlates data from all of a company's endpoints and offers greater visibility into what's occurring in the environment. Let's assume that the same unknown executable is detected on 100 machines. A solution with EDR plus NGAV product can determine that on five of those machines the executable generated a process that connects to a known malicious command and control server. Having more visibility into the environment allows the solution to put context around what's happening and determine, with a high degree of certainty, that the executable is malicious and blocks it.

An EDR platform's cross-correlation and behavioral analysis capabilities supercharge next-generation antivirus, making the technology especially helpful for detecting ransomware. Given how lucrative ransomware attacks are, adversaries are quickly creating new programs. Since these programs are new, the hashes are unknown to legacy antivirus programs while some next-generation antivirus products may be unable to detect ransomware attributes. But adding EDR capabilities to next-generation antivirus programs allows them to use behavioral detection to stop and block new ransomware families and variants by looking at how these programs act.

Antivirus isn't enough to face today's threats

Antivirus alone is no longer enough to protect a company. Overpowering today's attackers - whether they use advanced techniques like fileless malware or malware that's been around for awhile - and responding to threats requires EDR plus NGAV. The bad guys treat all of an organization's machines as possible entry points. EDR plus NGAV takes this concept and uses it to the defender's advantage by using all of a company's endpoints for protection.

About Cybereason

Cybereason is the leader in endpoint protection, offering endpoint detection and response, next-generation antivirus, and managed monitoring services. Founded by elite intelligence professionals born and bred in offense-first hunting, Cybereason gives enterprises the upper hand over cyber adversaries. The Cybereason platform is powered by a custom-built in-memory graph, the only truly automated hunting engine anywhere. It detects behavioral patterns across every endpoint and surfaces malicious operations in an exceptionally user-friendly interface. Cybereason is privately held and headquartered in Boston with offices in London, Tel Aviv, and Tokyo.

cybereason