# Solving the AV Problem

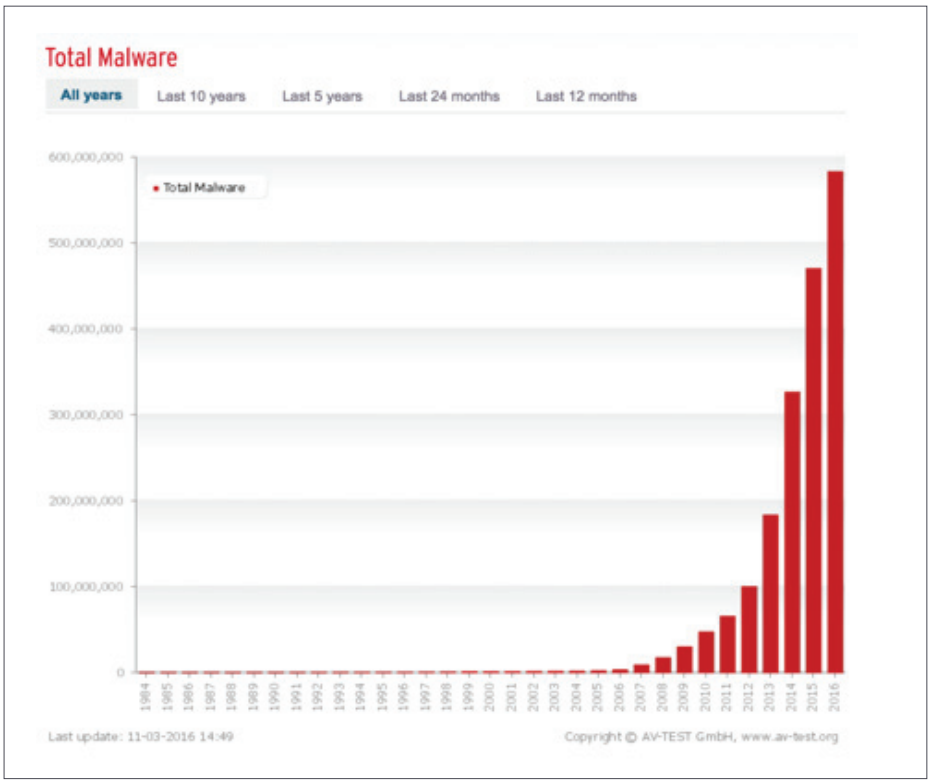
## Whitepaper

SentinelOne

# Cloud Infrastructure is on the Rise, and Security is Lagging Behind

The concept of antivirus, as it has been known since the first heuristic AV products were released in 1987, entered obsolescence sometime early this decade. Industry leaders first began noticing the decline around 2012. This was the first time that the volume of new malware samples began to outstrip the ability to write new signatures. Both the volume and sophistication of malware increased exponentially until 2014, when an executive at a prominent endpoint protection firm famously declared that antivirus was “dead.” [1]

At the time, contemporaries scoffed at the remark. After all, signature based endpoint protection products are still on the market, but a look at the trendline in malware samples from 2016 shows that things have gotten dramatically worse.




The chart above was last updated in November of 2016, so it does not show all the data from that year. Nonetheless, it already registers nearly six hundred million unique malware samples—an increase of 300 million since the year antivirus "died."

This increase in malware samples totally outstrips the industry’s ability to write individual signatures. What’s more, advanced techniques from nation-state actors have begun to filter into the mainstream of the hacking community, and malware authors have begun to spin off their own unique solutions to get around endpoint protection.

Volume and sophistication of malware have decisively smothered traditional endpoint protection methods. In response, several new and established companies have spun off new methodologies, such as endpoint protection and response (EDR), next-gen antivirus (NGAV), and next-gen endpoint protection (NGEP). However, not all of these approaches can fully encompass what's necessary to defend the enterprise during this dangerous time. Any product that attempts to protect the endpoint in this era of vulnerability can't just target present threats—it must also be future-proof.

# Malware: Present and Future

A common truism in the information security industry is that most hackers are "script kiddies." That is to say, most common hackers are just following directions that other, more advanced users have set out for them. This may be true, but now even the script kiddies have become powerful, armed with novel tools and techniques. More sophisticated hackers have become even more powerful in turn, and are now employing code inherited from nation-state intelligence agencies.

**Some of these techniques are simply amplifications of existing methods. For example:**

- **Packers** compress code, obfuscating malware data so it can't be read by security researchers or endpoint protection programs. Many packers are often commercially available. One such packer, known as Themida, was recently used in malware that was able to take over ATMs and turn them into skimmers. [2]
- **Wrappers** are used to extract malicious compressed code. Most of the time, wrapper programs try to pass themselves off as something benign. In one recent example, malware authors actually used out-of-date malware as wrappers in order to infect a hospital. Newer operating systems dismiss the out-of-date malware as irrelevant—leaving it free to seek out and infect vital systems that were still running Windows XP. [3]
- **Variations** allow malware authors to sneak generic malware onto endpoints and servers. Many low-grade EPP products will fail to recognize the more well-known forms of malware if even a slight change is made in their file structures. Criminals often employ what's known as a "crypting" service to professionally alter malware in ways that make it invisible even to the most advanced EPP products. [4]

All of these techniques have been seen and done before, but new advancements in criminal technology have made them ever deadlier. It's best to think of malware authors as a sort of render farm, cranking out iterations of malicious code at rates far faster than enterprises can match.

The firm AV-TEST, which is responsible for the chart in the introduction, registers almost 600,000 new malware samples per day [5]. Each sample represents a unique piece of code, which requires a signature to match. A large AV firm might employ 350 engineers to write these signatures—but they could work until the heat death of the universe and still not catch up with the volume. Worse still, these variants don't even last. Most malware blinks in and out of existence—shows up, infects, and disappears before a sample can be written.

## How Are Security Firms Responding to the Flood?

There are a number of methodologies that the security industry has adopted to get at the heart of the problem. Each technique understands that the idea of finding malware based on its signature is, at best, ancillary to the process of detection, mitigation, and response. Each technique attempts to find a workaround—but not every approach is sufficient. In order to succeed, novel anti-malware techniques can't just protect against present threats.

# Endpoint Detection and Response (EDR)

EDR has become a $490 million industry over the last few years [6]. Instead of looking for malware signatures, EDR focuses on indicators of compromise (IOCs). This includes a behavioral detection component—ideally, an EDR platform will automatically detect a behavior violation, quarantine the infected endpoint, investigate, or flag for investigation, and then roll back any malicious changes. Not every EDR platform is actually able to do these things however, and therein lies the problem.

Every EDR product on the market currently needs a human operator in the loop. These can't be low-skill personnel either, so it will be difficult for organizations to promote EDR supervisors from within their existing SOC. This is a problem, as many information security jobs are hard to fill as is [7]. More problematic is the fact that EDR solutions will need more and more human intervention as time goes by, because they don't currently protect against more advanced forms of malware, not to mention other types of cyberattacks, such as exploits or script-based attacks.

As an example, 38% of all attacks now employ Powershell [8], but not all EDR products are able to detect powershell-based attacks. EDR products also cannot detect file-less malware, a threat category that has been steadily rising in prominence. Lastly, EDR products attempt to quarantine malware by trapping it inside VMs—but there is already plenty of malware that can escape sandboxes [9].

In short, key features of EDR are already running behind the present-day reality of malware.

# Next Generation Antivirus (NGAV)

NGAV provides a different method to the same approach: shutting down the inherent weaknesses in signature-based detection. With NGAV, this capability is provided by limited machine learning capabilities. In short, they use a machine-learning algorithm to analyze compressed files. If the algorithm suggests that a file will unfold itself into malicious software, then the NGAV program will take steps to automatically mitigate and remediate.

Again, this runs into the same stop as EDR—the rise of file-less malware. If there are no files to unpack or analyze, this allows attackers to do a seamless end-run around these next-gen capabilities. Additionally, the algorithm itself requires constant fine-tuning, which requires manpower.

In the end, both NGAV and EDR run into the same problems. They require too much manpower in an age of limited resources, and they're present-proof—but not future-proof. The next generations of malware are already outrunning the next generation of antivirus. A different approach is needed.

# Next-Generation Endpoint Protection by SentinelOne

Any real solution to the challenges posed by the increasing volume and sophistication of malware must incorporate best-of-breed practices from every aspect of endpoint protection. This solution needs to cover malware of every variety and description, including file-less malware. Lastly, it needs to combine the tenets of defense-in-depth in a single product—incorporating mechanisms that deal with malware before it executes, while it's executing, and after it has executed.

- **Pre-Execution**, SentinelOne incorporates cloud intelligence to block known bad programs. Machine learning algorithms can extrapolate binaries to identify malicious files.
- **On-Execution**, the product identifies malicious behavior from any malware that gets past the automated blacklisting phase. Even file-less malware must undertake certain actions in order to compromise and exfiltrate data. This stage is where it stops.
- **Post-Execution**, threats are automatically mitigated. The machine-learning algorithm automatically programs itself to recognize and terminate any previously-unknown malware. Administrators are provided with a comprehensive view of the malware's attack path, and can use the SentinelOne application to manually or automatically roll back any changes.

With SentinelOne, administrators have access to a single product that provides deep expertise in multiple areas. A single product, it is both a jack of all trades and a master of all trades. SentinelOne protects Windows, MacOS, and Linux systems alike, and, as protection can be carried out by an autonomous agent independent of internet connectivity, it can even protect air-gapped systems.

Administrators who choose SentinelOne will have access to a versatile multi-platform product which encompasses multiple layers of defense. Built to stop cutting-edge malware, SentinelOne will remain a relevant security tool—no matter what the future may hold.

## Citations


1. http://www.wsj.com/news/article_email/SB10001424052702303417104579542140235850578-lMyQjAxMTA0MDAwNTEwNDUyWj
2. https://securelist.com/blog/research/74772/atm-infector/
3. http://www.darkreading.com/vulnerabilities---threats/attackers-wrapping-new-tools-in-old-malware-to-target-medical-devices/d/d-id/1326075
4. http://www.theregister.co.uk/2015/11/24/refudme_anti_antivirus/
5. https://www.av-test.org/en/statistics/malware/
6. https://www.gartner.com/doc/3179118/market-guide-endpoint-detection-response
7. https://techcrunch.com/2016/03/07/combating-the-cybersecurity-job-crunch/
8. https://www.scmagazineuk.com/microsoft-powershell-used-to-launch-38-of-cyber-attacks-in-2015/article/532081/
9. https://nakedsecurity.sophos.com/2015/05/14/the-venom-virtual-machine-escape-bug-what-you-need-to-know/