

5 Five Reasons to Look Beyond 'Math-based' Next-Gen Antivirus

There is an abundance of noise around “Next-Generation Antivirus” point products that claim to be developed with ‘predictive mathematics’, ‘machine learning’, and ‘artificial intelligence’. Regardless of whether or not the underlying technology constitutes true A.I., the overall approach (from a security standpoint) is flawed. The industry’s most hyped math-based prevention product is one that will not come close to solving your overall endpoint protection challenges. Here are 5 reasons why.

1. Against today’s threats, prevention is only *part* of the battle.

If organizations only had to defend their user endpoints and servers against Portable Executable (PE) and DLL-based malware, then prevention-only products would solve a large part of the problem. Not the whole problem, though; these types of attacks represent only 50% to 60% of new malware observed each week, coupled with the fact that no single security technology is 100% effective. But what about other types of threats? A significant percentage of today’s advanced attacks use multiple vectors—several of which don’t even involve files. For example: memory-based malware, exploits, script-based attacks from the inside. A prevention solution built to uncover malware based on binary characteristics is completely ineffective against these other vectors of attack.

2. Some things can’t be predicted.

The premise of ‘math-based’ static prevention is that the true nature of a file (benign or malicious) can be predicted through statistical analysis of predefined malicious binary attributes. Basically, this is an application of the same kind of mathematics used across the financial world to predict stock market performance. How well does that actually work? It doesn’t work well enough to confidently anticipate all booms or crashes. The reason for this is simple: markets are driven by human behavior. So is the creation of malware. It is simply impossible to predict what new techniques and tactics attackers will develop to successfully compromise an endpoint system or breach an organization.

3. Attackers will still win when protection is a numbers game.

The thing with statistics is that perspective is critical—especially when it comes to cybersecurity. For example, claiming a 99.9% efficacy rate against malware is excellent if you've got a sample set of 100 different types of malware. But 99.9% efficacy for a sample size of 1,000,000 malware variants changes the whole perspective (1,000 variants go undetected, in this case). Consider that today, one new zero-day attack is discovered almost every week, and that there are nearly 1 million new malware variants released EACH week. Do you still feel comfortable about a 99.9% prevention rate, especially when that prevention is your only layer of protection? All it takes is a single attack for an organization to be left reeling from the ensuing financial and reputational damage.

4. YOU have to teach the A.I. (and that takes time).

The application of artificial intelligence (A.I.) and machine learning to endpoint protection marks a big leap forward in cybersecurity innovation. In the best case, the system 'learns' new criteria and adapts quickly with a short ramp-up that doesn't require much (if any) administrative intervention. However, the math-based next-gen AV product falls short. On initial deployment, there's substantial configuration overhead where security and IT teams need to spend time telling the system what's safe (versus what's not), as the product doesn't use definition files. It's up to the admin to investigate files based on MD5 hashes and threat intelligence reports, too. Depending on the environment and the number of IT resources dedicated to the security project, this process could be extremely time-consuming.

5. Cloud-based management is the only deployment option.

If your organization adheres to stringent data privacy policies that require it to own its own data, then the industry's most hyped math-based next-generation AV isn't an option for you. It is strictly cloud-based, with no option to deploy as an on-premise management server.

What Next?

Don't buy into the hype. Today's threat landscape is far too diverse and sophisticated to rely solely on preventing file-based malware—or on security solutions driven only by predictive analysis.

The best approach to Next-Generation Endpoint Protection addresses all phases of the threat lifecycle. It combines advanced prevention, behavior-based detection and automated response capabilities that can be executed autonomously—on the endpoint itself—for best-in-class protection across all major vectors of attack.

This is the essence of SentinelOne.

SentinelOne®

Next-Generation Endpoint Protection Platform

For more information about the SentinelOne Endpoint Protection Platform and the future of endpoint protection, please visit: www.sentinelone.com