The State of Endpoint Security: Past, Present and Future

WHITE PAPER

NYOTRON
SECURING THE WORLD

Is Malware Winning?

It does not look like things are getting better in the world of cybersecurity… powerful ransomware, breaches affecting 100+ million people, state-sponsored attacks and unprecedented vulnerabilities. Just think back to 2017 that saw WannaCry ransomware, NotPetya wiper malware, and the Equifax breach, to name just a few incidents. Shipping giant Maersk estimates that the "NotPetya cyber attack cost it $250m-$300m in lost business."[1] Already this year, Meltdown and Spectre vulnerabilities have affected computing environments at a scale not seen before. According to a SANS survey, 53% of organizations have experienced an endpoint compromise within the last two years.[2]

Why are we in this situation? Besides being such a lucrative business for organized crime (with very little downside), as well as government-level sponsorship, malware's asymmetric advantage over defenders is attributable to the following factors:

1. Sheer Volume

AV-Test.org registered 118 million new malware samples in 2017.[3] Even at a 99.9% detection rate, there would be 118,000 undetected threats, and this is just for known file-based malware. It is relatively easy to create new malware and even more straightforward to modify or obfuscate existing malicious code in order to avoid antivirus detection. Malware writers employ a number of off-the-shelf tools for obfuscation, including:

- Crypters (e.g., Cryptex, Debug Crypter)
- Packers/compressors (e.g., UPX)
- Protectors (e.g., WProtect)
- Frameworks (e.g., Veil-Evasion, Shelter)

[1] Milne, Richard. (2017, November 7), Maersk cuts profit guidance in wake of cyber attack. Financial Times. Retrieved from https://www.ft.com/content/711be9fa-c396-11e7-a1d2-6786f39ef675

[2] Next-Gen Endpoint Risks and Protections: A SANS Survey. SANS Institute. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/next-gen-endpoint-risks-protections-survey-37652

[3] AV-Test.org. Retrieved from https://www.av-test.org/en/statistics/malware/#tab-6907-4

To demonstrate how pervasive new malware is, Palo Alto Networks reports that VirusTotal had never seen 45% of malware detected by WildFire.[4] Moreover, Lastline states that 65% of samples it saw were not submitted to VirusTotal and were submitted only once to Lastline.[5]

According to the Ponemon Institute, 77% of attacks that successfully compromised organizations in 2017 utilized fileless techniques that it expects to grow 20% year-over-year.[6] With fileless malware, there is nothing to obfuscate or scan. Attackers can easily create it by leveraging legitimate administrative tools, such as PowerShell, WMI, WScript, CScript, etc.

2. Existing Approaches

The majority of endpoint security products approach the malware challenge by attempting to "enumerate badness" (i.e., applying the Negative Security model). This requires managing a list of bad applications, behaviors, signatures, indicators of compromise (IOCs), etc. and letting through anything that's not in the very long list. Way back in 2005, Marcus Ranum called enumerating badness one of the "Six Dumbest Ideas in Computer Security."[7] Why so? One reason is that by "1992 the amount of Badness in the Internet began to vastly outweigh the amount of Goodness."

Building and maintaining an infinite list of badness is, by definition, impossible. Human ingenuity is limitless and bad guys will always find a never-before seen or used way of getting in. No wonder that 69% of organizations surveyed by the Ponemon Institute do not believe that their antivirus can stop the threats they are currently seeing.[8]

Some of you may have watched a television show called Mr. Robot. In episode 9 of the second season, Angela uses a USB stick called a Rubber Ducky.[9] Even today, a $45 Rubber Ducky[10] can bypass the majority of Antivirus (AV) and Next-Generation Antivirus (NGAV) products. This highlights just how difficult it is to focus on badness. It is too hard for products based on the Negative Security model to define the infinite "badness" of Rubber Ducky for a variety of reasons.

[4] Palo Alto Networks. https://www.paloaltonetworks.com/campaigns/brighttalk.html?commid=306617
[5] Lastline. Q4 2017 Malscape Monitor Report.
[6] Ponemon Institute. The 2017 State of Endpoint Security Risk Report.
[7] Ranum, Marcus. The Six Dumbest Ideas in Computer Security. Retrieved from http://www.ranum.com/security/computer_security/editorials/dumb/
[8] Ponemon Institute. The 2017 State of Endpoint Security Risk Report.
[9] http://www.usanetwork.com/mrrobot
[10] USB Rubber Ducky. Hak5 Gear. https://hakshop.com/products/usb-rubber-ducky-deluxe

The Evolution of Endpoint Security

1. Traditional Antivirus—Let's Add More Gates

Let's look at an example of a "traditional" AV product such as Symantec Endpoint Protection (SEP). It started out as an AV-only engine. Today, it contains about eight different technologies that work as gates: AB, Host Firewall, Application and Device Control, Heuristics/Behavior Monitoring, Host Intrusion Prevention, Memory Exploit Mitigation, Reputation Analysis, and Emulation/Sandboxing. These "gates" have significantly increased SEP's efficacy vs. just an AV engine.

What are the issues with adding more technologies? Obviously, the more technologies you add, the more heavyweight your agent becomes, and the more your users complain about the performance impact on their systems. This "agent bloat" has become a persistent problem as endpoint security products with legacy architectures have stuffed more countermeasures into their agents.

Even more importantly, if attackers manage to bypass all of these gates (and they will), they have a free pass to the system since traditional AV is transient security as opposed to persistent security that never stops looking for threats.

2. Endpoint Detection and Response—Let's Go Huntin'!

The "we are all doomed" attitude from a few years ago resulted in the rise of Endpoint Detection and Response (EDR) products. Actually, there are very valid reasons that support this approach:

- Average number of days to detect a breach: 206
- Average number of days to contain a breach: 55

Therefore, since all is lost, EDR suggests that we need to track every single event on all of our endpoints and continuously hunt for threats that have slipped through our defenses. With the goal of reducing the scary 206 days, EDR strives to provide security practitioners with better visibility into malicious attacks that have evaded endpoint-blocking measures and spread through the network.

> "Only a third of organizations believe they have adequate resources to manage security effectively." [11]
>
> – Ponemon Institute

An obvious concern with this approach is that you are already infected and the malware has likely done damage. Probably the most important downside is that you will need more security staff to perform threat hunting. Does anybody have underutilized security staff on their team? Is anyone having trouble hiring security talent or coming up with extra budget? By the way, Cybersecurity Ventures estimates that there will be 3.5 million unfilled cybersecurity positions by 2021.[12]

3. Next-Generation Antivirus—Machines Will Save Us All

Now, NGAV has become security's shiny new object. Security tools powered by machine learning, deep learning and artificial intelligence are supposed to save us. Since approximately 2014, early adopters and parts of the early majority have already been using these technologies. As we have seen from the news, even though these tools have improved detection efficacy, improvement in the overall security posture has been marginal. The reality is that most advanced attacks are still getting by NGAV.

> "The machine learning model is an imperfect summarization of tens of millions of malicious and benign software on which the model was trained…all machine learning models have blind spots (false negatives) and they can mistakenly call things bad (false positives)." [13]
>
> – Hyrum Anderson, Endgame (NGAV vendor)

[11] Ponemon Institute. The 2017 State of Endpoint Security Risk Report.

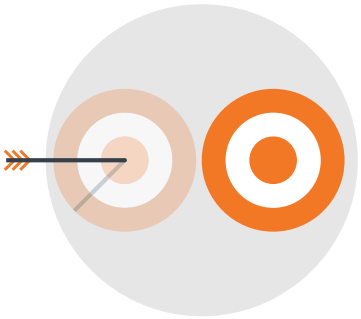
[12] Morgan, Steve. 2017 Cybercrime Report. Cybersecurity Ventures. Retrieved from https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

[13] Ragan, Steve. (2017, August 16). Here's why the scanners on VirusTotal flagged Hello World as harmful. CSO. Retrieved from https://www.csoonline.com/article/3216765/security/heres-why-the-scanners-on-virustotal-flagged-hello-world-as-harmful.html

Here are just some of the reasons for NGAV skepticism:

Vendors train AI-powered security tools on known malware samples. Hence, they are not fully effective against truly new unknown malware. Just look at the NSS Labs Advanced Endpoint Protection results.[14] The full test reports per vendor show efficacy against "unknown threats" as low as 54%. And, this is just for vendors who made their reports public.

Since AI tools focus on static file analysis, they are not necessarily effective against fileless attacks that are responsible for a significant percentage of modern-day attacks.



AI tools tend to produce significant false positives. Some public tests demonstrate that these can be over 20%.[15]

Do not forget that the bad guys are now using AI to beat AI-powered tools. After all, they have access to the same tools and technologies as the good guys.

Overall, we have reached a point called *AI Fatigue*.

[14] Advanced Endpoint Protection (AEP) Security Value Map. NSS Labs. Retrieved from https://www.nsslabs.com/security-value-maps/advanced-endpoint-protection-aep/

[15] AntiVirus Comparative. AV-Comparatives.org. Retrieved from http://www.av-comparatives.org/wp-content/uploads/2016/11/avc_mrg_biz_2016_10_symantec_en.pdf

The Year (Decade?) of Positive Security

Back in 1987, Fred Cohen's study of computer viruses revealed that there is no algorithm that can perfectly detect all possible viruses. The industry is searching for a better approach.

The concept of the Positive Security model is in sync with one of the major themes of RSA Conference 2018—Zero Trust (or Default Deny). Positive Security blocks everything that isn't "good" (e.g., unknown files or behaviors) by default. As the Positive Security model seems to be experiencing a resurgence in popularity, here are highlights of approaches:

Application Whitelisting/Application Control - vendors such as Carbon Black (Cb Protection), McAfee (McAfee Application Control) and Microsoft (Windows Defender Application Control). Whitelisting technologies are extremely burdensome due to the overhead from a high level of false positives and ongoing management. Additionally, they do not protect against vulnerabilities in whitelisted applications and are ineffective against fileless attacks.

Application Isolation (aka secure containerization or containment) - vendors such as Bromium, Sophos (Invincea), Symantec (SEP Hardening) and Microsoft (Windows Defender Application & Device Guard). Whether this approach is Positive or Negative depends on the specific configuration. If only high-risk applications—web-browser, email client and a few other applications—are isolated while allowing everything else, this is not Positive Security.

OS Hardening/Lockdown - primary example is Symantec (Data Center Security). This tends to be a complex and expensive product focused primarily on server protection. Its classification as a Positive Security approach is questionable.

OS-Centric Positive Security - Nyotron pioneered this technique. It's a well-designed approach to the Positive Security model that focuses on the damage stage (i.e., intentions or outcomes of an attack) and on OS system calls rather than on applications, user behavior or reputation. This reduces management overhead and does not have the micro-virtualization performance penalty of the Application Isolation approach.

Negative and Positive Security—Better Together

Endpoint protection solutions that include static file analysis (whether based on AV definitions or Machine Learning models) and that are based on the Negative Security model are, and will continue to be, at least in the mid-term, an important layer in an organization's defense-in-depth strategy. In some industries, compliance requirements drive their use as well. Therefore, the prudent course of action is to consider pairing traditional AV (or NGAV) with a Positive Security model-based solution.

With endpoint security products continuing to be at the tip of the spear of cyber defenses for years to come, the question is how to ensure the best possible security posture. No matter which way an endpoint security buyer turns, there is no one magic bullet. It is likely that a layered approach with multiple different technologies working together is required.

NYOTRON
SECURING THE WORLD

2880 Lakeside Drive Suite 237
Santa Clara, CA 95054
+1 (408) 780-0750
www.nyotron.com