ESET white papers

ENJOY SAFER TECHNOLOGY™

THE DEFINITIVE ENDPOINT PROTECTION: CONSIDERATIONS AND EVALUATION

Author:
Andhika Wirawan ESET APAC Enterprise Lead

CONTENTS

Author:
Andhika Wirawan, ESET APAC Enterprise Lead

OBJECTIVES

This paper aims to determine what should be the best industry standard for endpoint protection by evaluating the varying level of technology employed by security solutions that are commonly found in the market. We will assess each technology based on its effectiveness and efficiency against trending threats while also taking an organisation's security posture and susceptibility to cyberattacks into consideration.

MULTI-FACETED ASSAULTS: CYBERATTACKS THAT GRAB HEADLINES

Today's increasing maliciousness and frequencies of cyberattacks can have far-reaching impacts that leave businesses with costly damages ranging from business disruptions to the loss of credibility. The extent of such profound cybersecurity incidents is exemplified when over 10 APT groups based in different parts of the world took advantage of four Microsoft Exchange zero-day vulnerabilities discovered in January 2021 to launch cyberattacks against thousands of email servers worldwide[1].

Rapid digitalisation, further accelerated by the recent pandemic, has increased the creation of new software codes exponentially, exposing new vulnerabilities and escalating the instances of zero-day threats. As organisations consider how to best protect themselves, it is vital to know the common types of threats, the variety of endpoint security protection available, and ways to evaluate their effectiveness and efficiency.

KNOW YOUR STUFF: COMMON THREATS

Before analysing the available defensive technologies to adopt, it is important to understand the adversaries to face: What are they, how they enter the environment (attack vector), and who's behind it, in order to understand what will work and what won't. Here are some of the terms that we will use throughout this paper:

- Malware is a generic reference to any type of malicious software designed to exploit programmable devices, services or networks. Examples include Botnet, Ransomware, Rootkit, Spyware, Trojan and Worm.
- Zero-day attack refers to the exploitation of security flaws in software that is yet to be fixed. These vulnerabilities open up attack surfaces that 'attract' cybercriminals to carry out zero-day attacks which are often characterised by never-before-seen signatures and heuristics. 60 per cent of today's breaches involve vulnerabilities for which a patch is available but not applied[2]. Another study by Cybersecurity Ventures predicted that by 2021, there will be a new zero-day exploit daily, up from one weekly in 2015[3].
- Advanced Persistent Threat (APT) refers to a new breed of highly motivated cyber-warfare adversary that is orchestrated and sponsored by nation state, terrorist, or well-funded cybercrime syndicate. Their attacks are sophisticatedly planned to undermine a specific target (files, individuals, or organisation), and often employ fileless technique, which leverages applications that already exist in the organisation's network. The low footprint of fileless attacks had been studied to be ten times more likely to succeed than file-based ones, which makes it a favourite amongst APT groups.

Ransomware

As one of the most common and feared malware, ransomware encrypts a victim's files to demand a ransom before restoring access to the files. Victims are given specific instructions to pay a fee, often in Bitcoin, for the decryption key. On average, ransomware attacks have cost organisations US$ 646,000[4].

Three common attack vectors:

- Remote Desktop Protocol (RDP) takes the top position as the most common vector of attack for ransomware. A large part of the reason is that RDP ports are often poorly secured and thus easy to penetrate. Since RDP access is dependent on password-based credential, threat actors can easily buy compromised passwords from the dark web, which can come as cheap as $20 each[5].
- Phishing emails, which seek to trick users into taking a compromising action, come second as the most popular ransomware attack vectors. These emails look deceivingly legitimate and contains a link that will request the recipient to enter their credential. This will allow threat actors to steal access to a system in the environment. Many organisations have tried to mitigate the impact of phishing with technology, but the most effective way is still to educate employees through a security awareness programme.
- Unpatched software and system may allow attackers to access the network without having to have any access credentials, and that's why it is the most common ransomware delivery method. When this vulnerability is exploited by threat actors, a zero-day threat is born. It will continue to be a cause of concern until the patch is applied, or the organisation has a solution to detect new behaviour in real time.

Endpoints continue to be the primary landing point for infiltration by threat actors. Not only do they contain the primary objective of data and organisation processes, but their capabilities also allow threat actors to pivot to other objectives to target other endpoints or purpose-built devices. It is this argument that necessitates organisations to make endpoint security their first consideration, prior to increasing their security posture in other areas.

Let us take a look at the various core techniques that had been employed in a typical endpoint protection product, as we attempt to evaluate their effectiveness and efficiency.

FIVE LEVELS OF ENDPOINT SECURITY PROTECTION

Level 1: Black and Whitelisting (Automated)

Black and whitelisting is one of the most basic methods of endpoint security protection. It decides whether to block or allow execution by looking at a range of parameters — from file size, directory paths to cryptographic hash value — to identify 'known' bad (blacklist) or good (whitelist) codes. Backed by security intelligence, this method relies on analysis results from past encounters with the suspected file (sample).

This method is inefficient because: Vital responsibility lies with software vendors and IT administrators to maintain the blacklists and whitelists accurately and update them in a timely manner. With new malware burgeoning every month (8.99million in Oct 2020 alone; adding up to a total of 1,149.83m as of 20 January, 2021[6], security vendors who rely solely on this are constantly playing catch-up. IT administrators find it tedious to maintain whitelisting requests as they are often inundated with operational issues, ensuring network performance, monitoring IT assets, and more. This method also fails to address parameters in the middle ground, such as suspicious or unsure codes.

Level 2: Signature-based Endpoint Security (Automated)

This method identifies known threats by their signatures: A set of unique data or bits of code that differentiate it from others. It employs algorithms to quickly scan and examine if an object matches those of known malicious codes. When a known signature is identified, remediating actions can be taken to prevent the threat from wreaking havoc. Due to its sheer speed, this technique is used by top endpoint protection vendors only as the first pass scan to increase scanning speed. It is also used predominantly by firewalls, email and network gateways to protect against known or older threats that remain active.

Relying on this method alone is ineffective because it is reactive and relies on a database of known signatures. According to a Cisco's study, 95% of malware files analysed were often less than 24 hours old[7]. Today's newest malware strikes fast with sophisticated capabilities to alter its signature to avoid detection — including code permutation, register renaming, expanding/shrinking code, insertion of garbage code while preserving the object's functionality and behaviour, and more. The sheer rate of mutation renders this method ineffective as unknown signatures consistently draw a blank, while businesses cannot afford to wait for new 'signatures' or rules to be developed.

Level 3: Heuristic-based Endpoint Security (Automated)

Heuristic-based endpoint security goes a level up by investigating a malware's behaviour for suspicious "intended actions" prior to execution, then comparing it against a list of known malicious behaviour, before classification.

It continues to rely on a database of 'known' malware behaviour for analysis. By examining the file and looking out for suspicious behaviour — such as an attempt to disable security controls, installing malicious codes, registering for auto-start, and more — a sample is classified as 'malicious' or 'good'. This determines if any remediating actions need to be taken. While this method does not require an exact match to available signatures, which makes it capable to detect malware variants, it may not be able to address new behaviour that is seen in zero-day attacks. Therefore, in the face of the rising trend in zero-day attacks, relying on this method alone is starting to become ineffective.

Level 4: Sandboxing Endpoint Security (Automated)

This method employs Artificial Intelligence(AI)/Machine Learning(ML) to automate the detection of never-before-seen threats in a sandbox. The suspect file is isolated in a secure, virtualised sandbox environment, equipped with a full-running operating system. As the file safely detonates in the sandbox's isolated environment, its behaviour is first examined by AI/ML deep learning neural network via both static and dynamic analysis. This enables the suspect object's behaviour to be observed and classified accordingly.

Utilisation of AI/ML in Cybersecurity

The use of AI/ML automates and speeds up malware classification through the deep learning of millions of malware samples and analysis of firewall data, to predict and score malicious attempts to intrude an IT network. It enhances the accuracy of analysis by increasing the instances of true positives and reducing false positives.

The effectiveness of ML's contribution to cybersecurity investigation is determined by the quantity of labelled data, the cleanliness of the data and its verifiability. It all culminates in the most important factor — the volume of training set designed by domain experts and data scientists to establish the algorithms used to determine how contextual decisions are made. These subsequently empower the ML to ask the right questions when investigating a malware's behaviour.

Relying on this method alone is ineffective when the organisation is an attractive target and needs to deal with APTs which are often funded by nation states that are highly motivated on taking down high-value targets. Not long ago, Dutch Bangla Bank Limited (DBBL) reportedly lost as much as US$3 million after being targeted by cybercriminals[8]. This was not the first time cybercriminals had targeted large banks in Bangladesh as prior to this, hackers had stolen US$81 million from Bangladesh Bank's account with the Federal Reserve Bank of New York in what remains as one of the largest cyberattacks. Depending on its implementation, this method can be vulnerable to sandbox evasion tactics especially if it is built on top of a non-proprietary sandboxing technology.

Level 5: Endpoint Detection and Response

Unlike the other levels of endpoint protection, endpoint detection and response (EDR) security solution provides continuous comprehensive monitoring of real-time endpoint activity, complete with in-depth analysis of suspicious processes to enable an immediate response to incidents and breaches.

How it works:

- It starts with the collection of various events that are happening in the endpoints being managed.
- Data correlation, filtering, rules and ML/AI are then applied to highlight anomalies. This will then trigger an alarm to the operators. These alarms, often called incidents, need to be investigated or analysed by the Incident Response team.
- Each incident may have different scoring and priority, and depending on the context and seriousness of the incident, they are handled by different experts.
- Once it is confirmed that the incident is malicious, a response action is then taken. This can be in the form of isolating the infected machine to prevent lateral movement, process killing, downloading the malware for further forensic investigation, quarantining and/or deleting the file.

This method is highly effective for most businesses. Although it offers the best protection against attacks on endpoints by threat actors who are experts in adversary techniques, it is also one of the more costly options, and might be inefficient. Risk-averse or prominent organisations will need to incur high upfront capital expenditure to set up their own in-house expertise, Security Operations Center (SOC) or to outsource to a Managed Security Services Provider.

To avoid being at the 'losing end', businesses that do not have the resources for such investments — whether to create or hire a specialised team, can consider deploying an endpoint protection solution with sandboxing technology as the next best option to EDR.

Viewpoint:
A robust, sandboxing solution can help businesses strengthen their defence against the most malicious attacks by automating the process of identifying suspicious file, observing its behaviour, making a conclusion, and removing it from the endpoint. Leveraging on the report from AI/ML, it also helps IT teams better understand today's threat vectors and their behaviour – all in an isolated, secure sandbox. Sandboxing protection helps businesses keep a close eye on critical threats to ensure that no stone is left unturned when defending against today's destructive attacks.

EVOLUTION: SANDBOXING SOLUTIONS

Sandboxing has been largely acknowledged as an effective way to guard against and strengthen one's defence against zero-day attacks. Of the two types of sandboxing, namely On-premise and Cloud-based, the latter has seen increasing adoption due to these factors:

- On-premise Sandboxing: Requires high initial capital investment and ongoing capital expenditure to continually upgrade/maintain the servers. Scalability is constrained by available hardware resources (servers, user's devices), resulting in the use of a smaller number of ML modules for analysis. The performance of the ML analysis may also be affected by a lag in accessing the source of definitions/modules by a few minutes, opening up windows of opportunity for cyberattacks.
- Cloud-based Sandboxing: Flexibility to scale up/down dynamically to avoid unforeseen expenses and business interruption, enabling a more cost-effective OPEX model for future growth. The dynamic scalability to a bigger pool of resources means larger ML models can be employed to conduct more complex analysis. The constant cloud-based updates of ML models provides further protection from definition/module degradation to ensure the effectiveness of endpoint protection.

USE CASES: CLOUD SANDBOXING

Zero-day attacks

- Challenge: Lucrative ransomware business model motivates threat actors to keep creating new techniques to exploit any software vulnerabilities that they found.
- Solution: Cloud-based sandboxing automatically protects against new threats by leveraging multi-layered observations and ML which is constantly upgraded via the deep learning of millions of samples — without waiting for new detection or signature updates.

Virtual patching

- Challenges:
  - Need to patch enterprise assets against vulnerabilities presented by unpatched endpoints.
  - Cannot rely on vendor patching as most vendors no longer issue patches for older systems.
  - IT administrators often find the patching process tedious, with insufficient resources to ensure timely patching while preventing business disruption.

- Solution: Virtual patching via cloud sandboxing helps separate running programs to mitigate system failures or software vulnerabilities from spreading — without harming the host machine or the operating system. This lowers costs while eliminating revenue/productivity losses from any potential disruption. The built-in security policies and rules proactively prevent the exploitation of a known vulnerability to ensure that attacks are not missed. It also guards against the erroneous blocking of legitimate files.

CHECKLIST: 7 FACTORS WHEN CONSIDERING YOUR CLOUD-BASED SANDBOXING SOLUTION

1. Automated protection: The solution must be capable to work without the need for manual intervention in order to be effective. It should already be capable of filtering out the "known good" and the "known bad", and automatically submit suspicious files for further analysis as well as to perform automated remediation based on the policy assigned.
2. Rate of sandbox analysis: The solution must not hinder the organisation productivity. A speedy analysis is important, preferably in a couple of minutes for a completely new sample, and in seconds for a known sample.
3. Proactive protection: This prevents the execution of a file until the result of sample detonation proves that it is benign. This technique will stop the occurrence of patient zero in the organisation.
4. Capability to analyse fileless attack: Knowing the high success rate of fileless attack, the solution must be able to accept the request to analyse scripts, archives, documents, aside from executables.
5. Utilisation of proprietary AI/ML: Leverage proprietary AI/ML to guard against sandbox evasion techniques. Effective ML is characterised by a high quantity of labelled data that is clean and verifiable, backed by a large, well-designed training set with expertly designed algorithms.
6. Dashboard for situational awareness: User-friendly portal displaying statistics such as the statuses of files being analysed, including easy-to-understand reports explaining the reasons behind classifying suspect files as malicious, suspicious or benign.
7. Support for roaming devices: Threat actors rarely gives up when they failed to penetrate a single endpoint, and will keep trying with others. This is why, when the analysis result of a sample had been completed and it is malicious, the endpoint protection solution should also distribute the detection to other endpoints in the organisation, no matter where the device is.

To better mitigate the impact of endpoint cyberattacks,
contact *ESET* today

Footnotes:

[1] https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

[2] https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

[3] https://www.blackstratus.com/ultimate-guide-zero-day-attacks/

[4] https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

[5] https://securityboulevard.com/2020/01/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate/ & https://www bankinfosecurity com/ransomware-gangs-not-so-secret-attack-vector-rdp-exploits-a-13342

[6] https://www.av-test.org/en/statistics/malware/

[7] https://www.infosecurity-magazine.com/opinions/malware-detection-signatures/

[8] https://www.zdnet.com/article/silence-hackers-hit-banks-in-bangladesh-india-sri-lanka-and-kyrgyzstan/

ABOUT ESET

For more than 30 years, *ESET®* has been developing industry-leading IT security software and services for businesses and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defences in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centres worldwide, working in support of our shared future. For more information, visit www.eset.com or follow us on *LinkedIn*, *Facebook* and *Twitter*.

ENJOY SAFER TECHNOLOGY™