AUTONOMOUS ENDPOINT PROTECTION

BUYERS GUIDE

SECRUTINY

TABLE OF CONTENTS

Introduction

Today's security landscape

In the past two decades of tech booms, busts, and bubbles, two things have not changed – malicious actors are still finding ways to breach security measures in place, and the endpoint remains the primary target. And now, with cloud and mobile computing, endpoint devices have become the new enterprise security perimeter, so there is even more pressure to lock them down

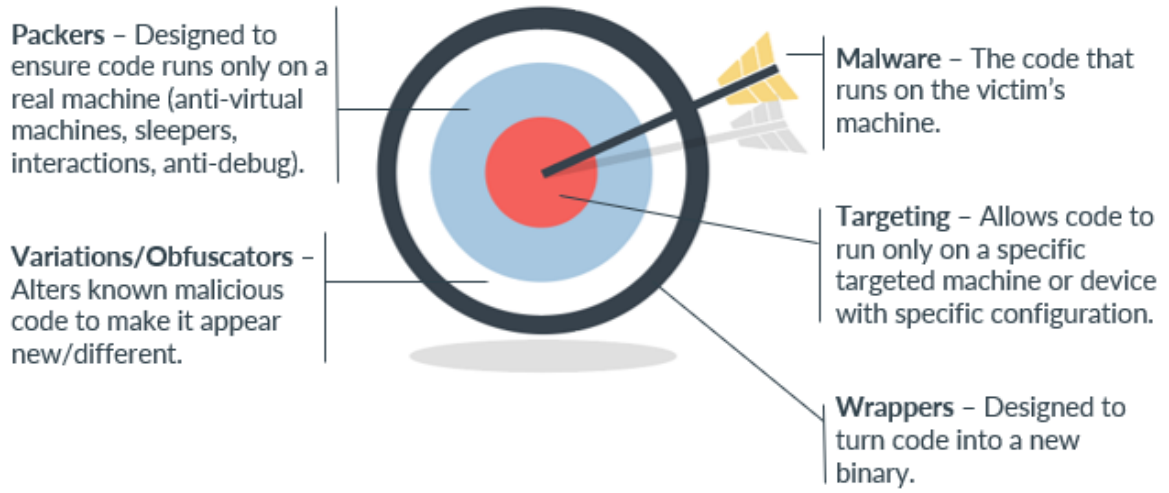
Companies are deploying piles of software on the endpoint to secure it – antivirus, anti-malware, desktop firewalls, intrusion detection, vulnerability management, web filtering, anti-spam, and the list goes on. Yet with all the solutions in place, high profile companies are still being breached. The recent attacks on large retail and hospitality organisations are prime examples, where malicious actors successfully used credit-card-stealing malware targeting payment servers to collect customer credit card information.

Why traditional security is not working

There is a fundamental problem with the security that leaves us basically in the same spot. It is looking for something known - a known hash, IP address, vulnerability, behaviour. Ultimately malicious actors can use enough masking techniques to bypass the security software, leaving the server or laptop once again the victim of an attack. It's very easy to alter this malicious code with downloaded or created tools to bypass security measures. Anyone who has basic coding skills can do it.

The diagram shows a few **attack masking techniques**, which are often used in conjunction with each other to take a known binary and cause it to appear completely new, unknown, and benign on the surface.

Along with masking techniques, malicious actors are using different vectors or paths to deliver the malicious code and carry out their attacks. Top attack vectors are listed to the right. Attacks can be single-vector or part of a multi-vector, more sophisticated attack.



Is Antivirus Dead?

Antivirus has been around now for 25 years yet has not innovated to protect against attacks that use unknown threat techniques. It continues to look for a known hash, and small changes to the hash can bypass the system.

Antivirus also overlooks the fact that attacks can be file-less, infecting the memory and writing directly to RAM rather than file systems. In addition, antivirus is known to not be user-friendly, hogging bandwidth with updates, and spiking CPU with resource-intensive scans. This not only leads to downtime but often causes users to get frustrated and take strides to disable the software or ignore security warnings.

Sandboxing as a Defence?

Approximately five years ago, network-based sandboxes began entering the scene. They 'emulate' the execution of unknown files inside a virtual machine residing on the network and monitor file behaviour throughout its execution inside the 'protected' environment. While these solutions have been able to increase detection rates of new threats, they are far from being 100% effective.

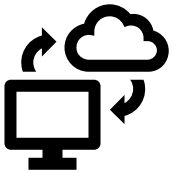
Attackers quickly realised while their current packing techniques could not be used to bypass the sandbox environment, they just needed to detect the environment. This could easily be done by noticing limited emulation time, lack of user interaction, and only a specific image of the OS.

Once the environment is identified, they ensure their malicious code will not run in the emulated environment, will be flagged as benign, and will continue its route to the end device and only run there (where the endpoint antivirus can do little to stop it).

Math-Based Next-Gen AV

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 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. With the new threat landscape, a new model that uses a different approach is needed.

Attack Vectors

Malware	Exploits	Live/Insider Threats
Executables	Documents	Scripts
Malware, Trojans, Worms, Backdoors, Payload-based.	Exploits rooted in Office documents, Adobe, Macros. Spearphishing emails.	PowerShell, WMI, PowerSpoilt, VBS.
		
Fileless	Browser	Credentials
Memory-only malware. No discbased indicators.	Drive by downloads, Flash, Java, Javascipt, vbs, iframe/html5.plug-ins.	Credentials scraping, Mimikatz,Tokens.

Four Reasons to Look Beyond Math-Based AV

1. File-based malware-only half the battle

PE and DLL-based attacks ONLY represent 50% to 60% of new malware observed each week. Prevention-only products will be completely ineffective towards threats that use multiple vectors, especially when they don't even use files, such as:

- Memory-based malware
- Exploits
- Script-based attacks from the inside

2. 99% is not enough

When 99% pertains only to file-based malware, that isn't enough. Even if 99% of file-based malware is blocked, what will you do with the 1%? If you are being threatened by 100 variants of malware, then 99.9% prevention sounds pretty good, but what if there are millions?

One new zero-day attack is discovered almost every week, and there are almost 1 million new malware variants released each week. Just one of these attacks could cause tremendous financial and reputational damage to an organisation.

3. Teaching the A.I. takes time

On initial deployment, there's substantial 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.

4. No on-prem management option

If your organisation 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.

A New Approach to Endpoint Security

Autonomous Endpoint Protection

In the past couple of years, a new type of technology emerged designed to detect and prevent threats at the endpoint using a unique behaviour-based approach. Instead of looking for something known or it's variant like signature-based detection, autonomous endpoint security is analysing file characteristics (to uncover known and unknown file-based malware) as well as the entire endpoint system behaviour to identify suspicious activity on execution.

Endpoint detection and response (EDR) monitors for activity and enables administrators to take actions on incidents to prevent them from spreading throughout the organisation. Autonomous Endpoint Protection (AEP) goes a step further and takes automated actions to prevent and remediate attacks.

Until recently, administrators have been hesitant to use the protection capabilities because of false positives associated with flagging unusual behaviour that isn't malicious.

Skype, for example, defies many rules of a 'normal' application, jumping ports and protocols, yet it's a legitimate application often used for business use. The AEP must have the ability to learn the local systems and environment, so it doesn't flag benign behaviour.

Autonomous Endpoint Protection as an Antivirus Replacement

If you're evaluating autonomous endpoint security solutions, you may be thinking it's yet another tool to install and potentially bloat your endpoint (as well as your budget.) And if you're in a regulated industry, you may be required to keep your Antivirus and install endpoint protection as an additional layer to protect against new and unknown attacks.

Many autonomous endpoint security vendors would not claim that they can be an Antivirus replacement. But if the autonomous vendor has been tested and certified as meeting Antivirus requirements, you can consider replacing your Antivirus with autonomous endpoint security.

To replace the protection capabilities of existing legacy, static-based endpoint protection technologies, AEP needs to be able to stand on its own to secure endpoints against both legacy and advanced threats throughout various stages of the threat lifecycle - pre-execution, on-execution and post-execution.

Your Autonomous Endpoint Protection (AEP) solution needs to address four core pillars that, when taken together, can detect and prevent the most advanced attack methods at every stage of their lifecycle:

Advanced Malware Detection

Your AEP must be able to detect and block unknown malware and targeted attacks - even those that do not exhibit any static indicators of compromise. This involves dynamic behaviour analysis - the real-time monitoring and analysis of application and process behaviour based on low-level instrumentation of OS activities and operations, including memory, disk, registry, network and more.

Since many attacks hook into system processes and benign applications to mask their activity, the ability to inspect execution and assemble its true execution context is key. This is most effective when performed on the device regardless of whether it is on or offline (i.e. to protect even against USB stick attacks.)

Mitigation

Detecting threats is necessary, but with detection only, many attacks go unresolved for days, weeks, or months. Automated and timely mitigation must be an integral part of AEP.

Mitigation options should be policy-based and flexible enough to cover a wide range of use cases. These include quarantining a file, killing a specific process, disconnecting the infected machine from the network, or even completely shutting it down. Quick mitigation during inception stages of the attack lifecycle will minimise damage and speed remediation.

Remediation

During execution, malware often creates, modifies, or deletes system file and registry settings and changes configuration settings. These changes, or remnants that are left behind, can cause system malfunction or instability. AEP must be able to restore an endpoint to its pre-malware, trusted state while logging what changed and what was successfully remediated.

Forensic

Since no security technology claims to be 100% effective, the ability to provide real-time endpoint forensics and visibility is a must. Clear and timely visibility into malicious activity throughout an organisation allows you to quickly assess the scope of an attack and take appropriate responses. This requires a clear, real-time audit trail of what happened on an endpoint during an attack and the ability to search for indicators of compromise.

Evaluating Autonomous Endpoint Protection Vendors

Now that you know what to look for in an autonomous endpoint protection solution, you'll need to start evaluating vendors on your shortlist. Request an evaluation from the vendor, and make sure it's full production software so that you can see how it will perform in your environment and against the security test you've outlined. For your evaluation, take the following considerations into account:

- Is the EPP and EDR solution combined in a single agent to be deployed via traditional software deployment tool and managed/operated via a single central management console?
- Does the software offer a multi-tenancy functionality for endpoints both on-premise and in the cloud?
- For endpoints (including mobile devices, if supported), which operating systems and major operating system versions are supported? For each of these, what are the performance requirements (CPU, memory, storage)?
- How, in technical methods, does the product detect and prevent attacks from each vector - including malware, exploits, and live/insider threats?
- How frequently are updates made available? Are updates pushed or pulled to the endpoint?
- Do the updates require any user intervention (i.e. reboot)?
- Can the product prevent threats if the endpoint is offline from the network?
- How scalable is the product? How many clients can be supported by each management console?
- Is the management server cloud-based or on-premise?
- What is done to prevent false positives and learn benign system behaviour?
- What is the current false positive rate?
- Do they integrate with SIEM systems for incident management?
- Are there prevention policies to protect against threats in real-time?
- What levels of contracted support does the endpoint protection vendor provide?
- Are software updates and upgrades part of the licensing fee?

Who Are Secrutiny?

We are Incident Response specialists who spend 95% of our time making sure our clients don't need to respond to incidents.

Secrutiny was founded by three people – all veterans who came to realise there is much confusion in the industry… tools were often overly complex, misconfigured and isolated, and adding further 'layers to the security onion' at significant cost was not the answer.

Through responding to 300+ incidents, we learnt the way to help organisations NOT to be breached is to support them in achieving better security and risk reduction with what they already have; adding capability, where necessary, based on evidence and risk appetite.

We're here to answer any questions you may have and always happy to share our experiences. Reach out to us and we'll respond as soon as we can.

www.secrutiny.com

enquiries@secrutiny.com

0203 8232 999