STORMSHIELD

OPINION ARTICLE

ENDPOINT PROTECTION SOLUTIONS AND ANTIVIRUS: WHAT'S THE DIFFERENCE?

Julien Paffumi
Product Portfolio Manager,
Stormshield

It is nearly a decade after the death of traditional antivirus software was announced, yet it remains very popular with the general public. Although a still commonly-used term in the computer world, antivirus is no longer the flavour of the month. Here's why.

The use of traditional antivirus software now seems to be obsolete, with the terms "Next Generation Antivirus" (NGAV), "Endpoint Protection Platform" (EPP) and "Endpoint Detection and Response" (EDR) having taken their place. What are the differences between all these detection technologies? Do we still need antivirus software today? We answer these questions in this paper.

DO ANTIVIRUSES STILL OFFER RELIABLE PROTECTION?

Antivirus software is a computer program that is designed to be installed on individual devices such as computers, tablets and phones with the aim of detecting and removing malicious software. Developed for the first time by IBM in 1987 in response to the "Brain" computer virus, **the term "antivirus" has been popularised over the years with a great deal of publicity, becoming the only defence against computer viruses in the collective imagination.**

Such antivirus programs operate on the principle of searching for signatures. "*Like a vaccine, the antivirus has a signature database that enables it to recognise a computer virus. It is therefore essential for the signature of this specific virus to have been generated beforehand,*" says **Stéphane Prévost,** Product Marketing Manager at Stormshield. This method of operation generates a variety of problems and limitations. The first of these is that you already need to be familiar with the virus before you can identify its signature (and be able to fight it). The second – and no lesser – issue is the advent of polymorphism, a technique for generating malicious files whose digital signature is unique to each file but whose method of infection and payload remain common. This limitation is all the more significant given that 450,000 new malware programs are created every day, or nearly 4 million each month, according to the AV-TEST Institute. As a direct consequence of this explosion, it is technically impossible for antivirus software to have prior knowledge of all signatures... Worse still for antivirus software, cybercriminals' modus operandi have continued to evolve in recent years, to the point of concealing themselves in blind spots in detection algorithms, such as "fileless malware". And the result? Detection mechanisms based on searching for digital fingerprints in a file let the vast majority of malware through, and need to be supplemented by other protection techniques.

Evolving and increasingly sophisticated cyberattacks are even turning antivirus software itself into a target. For example, at the "Black Hat Europe" conference in December 2022, a security researcher revealed a previously-unseen vulnerability that affects several antivirus programs. This flaw allows antivirus software to be taken over and legitimate files to be deleted. So what can we do when our main protection tool no longer fulfils its role?

THE ADVENT OF BEHAVIOURAL DETECTION IN DESKTOP PROTECTION

In response to this new situation, **cybersecurity vendors had to come up with a new approach, moving from fingerprinting to heuristic analysis based on user behaviour.** Called *Next-Gen Antivirus* or NGAV, these new types of antivirus formed the basis of what became known as the *Endpoint Protection Platform* (EPP). EPP solutions offered an initial response to polymorphism and fileless attacks by integrating new features such as memory monitoring, behavioural analysis and verification of indicators of compromise (IoCs). Despite this technological advance, insidious cyberattacks continued to slip through the cracks. It therefore became imperative to detect them, even after they had happened, and to respond to them.

This was the observation that prompted the appearance of *Endpoint Threat Detection & Response* (ETDR) solutions in 2013 in Gartner's analyses, based on the themes of incident response and investigation. From 2015 onwards, the acronym ETDR was replaced by EDR for *Endpoint Detection & Response*. The particularity of this new approach lies in the ability to detect and respond to unknown threats in real time in semi-autonomous fashion, as Stormshield Product Manager **Noël Chazotte** points out: "*If it detects a threat, an antivirus will block the program upstream, sometimes quarantining it. EDR, on the other hand, kicks in once the security incident is detected or has already occurred on the machine, and tries to determine what has happened at machine level to help operational teams prevent the infection from spreading*."

How does EDR technology detect sophisticated attacks? "*EDR identifies abnormal behaviour using indicators of compromise (IoC),*" explains Stéphane. *These are not always exceptional events; they can be commonplace actions, such as opening a connection to an external server*." Hence the importance of precisely defining the operating framework of the solution during the learning phase to prevent "false positives". But EDR and EPP solutions remain complementary, as Stéphane points out: "*You can make an analogy with the physical security of a company. The EDR solution is like the surveillance cameras: they allow you to see, for example, whether an intruder is entering your industrial site. But to deny them entry, you need an on-site security guard: this is the EPP.*"

So where does the antivirus fit in to all this? In 2023, according to the security.org website, three out of four Americans believe that they need an antivirus to be able to use their personal computer with peace of mind. Given the technological advances mentioned above, the question arises at professional level: **why do we still need antivirus software today?** And the answer is: simply because it provides a first layer of security. Although this solution will not be effective against all cyberattacks, it does provide an initial level of protection against the least sophisticated attacks – with the guarantee of avoiding the problem of false positives and consuming very few resources on the workstation. But an initial layer of security implies the existence of others. "*We are seeing several protection solutions installed on the same machine,*" explains Noël. "*However, combining them is not always a successful strategy, as some of them can lead to conflicts, leaving another door open to cybercriminals*."

NDR, XDR, MDR: A TREND TOWARDS SPECIALISATION IN DETECTION & RESPONSE

Despite the promise of hands-free operation from such solutions, the management of these tools must be supervised by experts, as shown by the development of managed EDR or mini-SOC offers. **In addition to improved detection, it is essential for endpoint protection tools to include incident detection and response capabilities**. And given the proliferation of incident collection points, an SOC analyst must have access to all network and infrastructure equipment.

For example, Network Detection and Response (NDR) solutions analyse TCP/IP packets passing through the network to detect suspicious activity. The XDR (eXtended Detection and Response) system aims to combine all internal and external IT assets (network, directories, cloud resources, firewalls, etc.) to provide an overall view of events in the information system. According to Noël, "*an XDR platform is a set of collection points and, above all, a correlation platform to help mitigate risk, and provide a degree of response and remediation*."

Other acronyms have emerged in recent years, such as MDR. In practice, "Managed Detection and Response" (MDR) is simply a marketing mode of an XDR in which an external team handles alerts. Whatever the tool and technology, it must be borne in mind that the analyst's role remains central and that no single technology provides sufficient security for a sensitive asset.

According to a study by the Survey Risk Alliance, only 12% of cybersecurity professionals report having adopted an XDR solution in their organisation by 2022. The remaining 77% say they plan to adopt one within the next 24 months. The demand for security experts specialising in incident detection and response is therefore expected to continue to grow in the coming years. Because despite technological progress, human intervention remains essential for analysing and understanding incidents. Such profiles are highly sought after in response to constantly-evolving operating methods, and their services will no doubt be more easily accessible to companies via managed BDU or mini-SOC offers.

STORMSHIELD

Stormshield, a wholly-owned subsidiary of Airbus CyberSecurity, offers innovative, end-to-end security solutions for the protection of IT networks (Stormshield Network Security), workstations (Stormshield Endpoint Security) and data (Stormshield Data Security).

www.stormshield.com

Version 1.1 - Copyright Stormshield 2023