

How to choose an Endpoint Protection solution

Between EDR and HIPS: which approach is best to effectively block sophisticated cyberattacks?

WHITE PAPER



While the topic of cybersecurity continues to be in the spotlight, cybercriminals are trying to fly under the radar. This objective leads them to constantly evolve their attack techniques. And because they know how things work, they seek to develop malicious tools to fool the cybersecurity solutions present on employees' workstations.

Today, conventional antivirus applications and other detection systems, especially those based exclusively on signatures, seem to be overtaken by complex techniques, such as the hijacking of legitimate applications and privilege elevation, as well as by stealthy malware. Therefore, solutions that focus on the detection and prevention of known attacks are becoming insufficient to deal with this new generation of sophisticated and unknown cyberattacks.

It is essential for organisations to implement ***solutions that analyse in great detail the behaviour of running processes to identify potential threats present in the machine****. The chosen solution must therefore be able to detect and block them proactively, automatically and in real time for the smoothest possible business continuity.*

This white paper describes the various mechanisms that a protection system for workstations and servers must have to satisfactorily fulfil its threat detection and terminal protection role.

Aimed at Information System Security Managers, it will provide you with the necessary elements to better support you in your decision-making.

Contents

1

Cyberattacks: how do they work?

2

Behavioural Analysis Solutions

3

Endpoint Detection & Response

The security ideal?

4

The different HIPS protection techniques

4.1 The rule-based approach

4.2 The contextual approach

4.3 "Hardening" security solution self protection

5

Stormshield Endpoint Security Evolution

The workstation protection solution

01

Cyberattacks: how do they work?

According to the ANSSI (French national computer security agency) between 2019 and 2020, the number of victims of cyberattacks has increased fourfold. As a report by the French Senate indicates[2], cybercriminals have taken advantage of this, resulting in a 667% increase in phishing attacks recorded between 1 and 23 March 2020.

Furthermore, although user awareness has gradually improved, no system or infrastructure can be 100% secure. This is why cyberattackers are always finding new tricks to penetrate the information systems of companies of all sizes in an increasingly targeted manner.

91%

of targeted attacks are carried out using spear phishing

Their goal: To exfiltrate sensitive data (medical, banking, industrial, etc.), to encrypt it, to hold it for ransom or to publish it, or even to damage the productivity of the targeted company (stop production lines, block or impede online sales, etc.). To do this, cyberattackers seek to bypass the security systems in place in order to gain access by exploiting, for example vulnerabilities in the software or device installed.

To better understand how a cyberattack works, we will focus on the three most decisive phases that allow an attacker to achieve their final goal. The initial phase will be to compromise an exposed user machine or service, providing initial privilege-free access to the system. In phase two, the cyberattacker then seeks to penetrate the information system by obtaining access to a privileged account or by infecting other machines. In phase three, the attacker can proceed with triggering the malicious action: encryption, exfiltration, etc.

We will discuss these three phases in more detail.

[2] http://www.senat.fr/rap/r20-678/r20-678_mono.html

First, cybercriminals make inquiries to identify victims within the targeted company. The attacker seeks to implement attack vectors that may be human and/or technological.

At the human level, the attacker uses social engineering techniques (LinkedIn, Facebook, etc.) to collect information that will be used to divert the attention of the person chosen as the victim for the primary infection.

PHASE 1

DISCOVERY AND PRIMARY INFECTION



They attempt to trick the recipient into opening an attachment or clicking on a malicious web link. A technique known for its effectiveness: 91% of targeted attacks[2] are carried out using this spear phishing method.

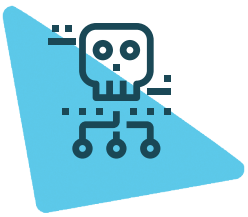
Distracting attention may, for example, consist in the cyberattacker impersonating a sender (financial institution, supplier, etc.) known to the targeted person.

On the technological level, the cybercriminal takes advantage of systems that are not properly protected such as RDP servers accessible from the Internet. They may also attempt to exploit weaknesses in vulnerable and non-updated applications. FOR example, the Canadian Cybersecurity Centre[3] issued an alert in March 2021 recommending several updates against the active exploitation of Microsoft Exchange-related vulnerabilities.

The goal: to execute malicious code to install a program in the targeted machine that allows the cyberattacker to infiltrate it.

[2] http://www.itpronews.fr/3648/2012/12/spear-phishing-plus-de-90-des-attaques-ciblees.html

[3] https://cyber.gc.ca/en/alerts/active-exploitation-microsoft-exchange-vulnerabilities



PHASE 2

LATERAL MOVEMENT AND EXPANSION

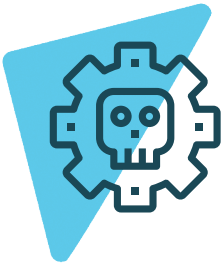
Once the primary infection phase is over, the attacker tries to scan the network to get to know it better. In this lateral movement phase, they want to penetrate the information system more deeply to identify the machines and user or administrator accounts that will be used to achieve their objectives.

Initially, they will therefore navigate and pivot through different systems and accounts. They can also remotely install their own tools in an attempt to exploit vulnerabilities in the system and retrieve login credentials.

The goal: to penetrate deeply into the infrastructure to find targeted machines where the attack will have the most impact.

They then seek to penetrate deeply into the system, which is the expansion phase. They often pose as an authorised user, which is very difficult to detect. To do this, they can perform a privilege elevation to impersonate a local administrator or take over a user account that has access to a particular software. They also combine several attack vectors in an attempt to compromise other vulnerable machines.

Common approaches are to exploit weaknesses, misconfigurations of the infrastructure or existing vulnerabilities. For example, poor segmentation within the company's network allowing access to machines of interest to them, for example, a server with sensitive data.



PHASE 3

IMPACT

This third phase is the culmination of the attack, where the cybercriminal performs actions in line with their intended objective. If the cyberattack is activated, it may allow **data to be exfiltrated/stolen, operational processes to be modified or a server vital** to the smooth running of the organisation to be **shut down**.

The attacker keeps their actions hidden to extend their presence in the network. This stealthy approach also serves to enable them to re-exploit the machine later or to launch an attack (more or less virulent) such as the one suffered by the French television station TV5 Monde[4] in 2015.

IT SHOULD BE noted that in some cases, attackers take care to delete the various backups and traces of malicious activity.

The aim: to undermine the infrastructure in order to block an element required for the company's production. Also, to exfiltrate data for resale and/or publication (such as health data on the dark web) or for encryption to obtain a ransom from the targeted structure.

[4] https://www.lemonde.fr/pixels/article/2017/06/10/le-piratage-de-tv5-monde-vu-de-l-interieur_5142046_4408996.html

02

Behavioural Analysis Solutions

In particular, cybercriminals use attack techniques to fly under the radar and avoid detection of their malicious code by the various security solutions. **The detection of suspicious behaviour and the preventive interception of potentially dangerous activities are therefore essential.**

As a result, the *Host Intrusion Prevention System* (HIPS) helps protect workstations and servers against malware by blocking suspicious activity that may affect infrastructure systems.

"Some intrusion prevention systems allow users to send logs of malicious activity and suspicious code fragments directly to the provider for analysis and possible identification. "

Stephen J. Bigelow

Senior Technology Editor

Source: Techtarget

Below, we will discuss the main aspects of different types of HIPS and the best approach for each organisation

HIPS **by signature**

These are based on the **knowledge of vulnerabilities in an application and known threats** and block their use. They work with a database that needs to be regularly updated.

They identify known attacks. However, they **cannot detect** unknown or 0-day attacks. They are **not well suited to situations where the workstation is disconnected** from its update server.

Few options present in the software.

Behavioural HIPS

Real-time blocking of **known and 0-Day attacks**: detection of suspicious activity in legitimate applications and processes without the use of signature databases or application anomalies.

Some HIPSs combine **behavioural and heuristic methods, memory protection or the hardening of the operating system** (OS) to provide better protection against threats.

Highly configurable based on lists of settings or rules and filters to suit different organisations.

*"A HIPS behavioural analysis solution recognises and blocks common and sophisticated **attack techniques,** such as the exploitation of application vulnerabilities to ensure **effective user workstation protection.** "*

Edouard Simpère
Stormshield Security Division Manager

Ubiquitous in the lexicon of the cybersecurity world in recent years, EDRs or Endpoint Detection & Response[5] applications are software that can detect and block known and unknown threats without waiting for patches or updates. They usually deploy agents on the various endpoints of a network, notably on workstations, mobile phones or the various servers of the infrastructure.

A general feature of EDRs is that they carry out **continuous monitoring of endpoints**. In addition, some solutions incorporate EPP components to provide real-time protection. This provides an effective first barrier of protection against most known and some unknown threats.

Endpoint Detection & Response: the security ideal?

As the ANSSI[6] underlines, these solutions, which manage large amounts of data, generally offer **detection** (suspicious behaviour of legitimate applications, *fileless*[7] attacks), **investigation** (complete visualisation of the detected attack) and **remedial** (remediation of files, etc.) capabilities.

As a result, EDRs now supplement traditional signature based solutions. They provide **global visibility** and generally detect abnormal behaviour in legitimate processes. Following this detection, the solution implements a response to interrupt the attack by stopping the malicious process. In a more or less automated way, it allows the administrator to be informed. Then either the administrator can apply a response, or the EDR is able to provide it automatically and in near real time (this will depend on the solution used). As a result, ransomware and polymorphic attacks can be detected and blocked using these tools.

On the administrative side, they can be integrated into the organisation's SIEM to provide the necessary logs to help SOC analysts optimise efficiency in the search for attacks.

[5] https://www.ssi.gouv.fr/uploads/2021/06/anssi-france_relance-edr.pdf

[6] https://www.ssi.gouv.fr/uploads/2021/06/anssi-france_relance-edr.pdf

[7] https://www.riskinsight-wavestone.com/2018/10/fileless-attack-le-retour-a-la-terre/

In addition, most EDR solutions on the market today opt for a *cloud-only* or *cloud-first*[8] approach to centralise data collection and analyse the precursor or compromise signals that indicate an attack. Indeed, the cloud lends itself to this collection and analysis of large amounts of data.

However, this approach is not always possible due to the sensitivity of the data being processed. For these use-cases **the on-premise mode can be an effective option** (defence, ministries, industry, etc.). In addition, it is important to distinguish between the level of protection established either by the server or by the client installed on the workstation.

We will look at the major differences between the two approaches:

Protection focused **on the server**

In this approach, the lightweight agent installed on the workstation **sends all information to the server**. It does not have extensive functionalities.

The server, whether on-premise or in the cloud, analyses the logs sent back by the agent in search of malicious behaviour, anomalies present on a particular workstation, etc.

The light agent needs **a permanent connection to feed back information**. There may be some latency in the response obtained.

Protection focused **on the agent**

The agent on the workstation is **autonomous in making decisions** and protecting the workstation without the need to access its server.

The server has less global visibility due to the **agent's extended capabilities** for managing the machine against malware.

The agent can **work independently blocking** malicious behaviour **in real time**.

Thus, to ensure the best protection at all times, **solutions that can detect malware without the need for a network connection should be given preference to ensure real-time, reliable protection of the workstation**.

[8] https://www.pcpresse.com/wp-content/uploads/2020/10/LINFO-CR01_MD.pdf

04 The different HIPS protection techniques

Cybercriminals are aware that their attacks must not attract attention in order to go unnoticed (phase 2: lateral movement and expansion). To do this, they constantly strive to develop new tactics and attack techniques to bypass traditional protections

We will discuss the main techniques used and how the attacker will employ them to try to thwart the various security protections.

255%

This figure corresponds to the increase in reports of ransomware in 2020, according to a study by ANSSI

In the table below, we have observed different attack techniques in the three phases of a cyberattack. As a reminder, in the third phase, the attacker has already taken control and starts the impact phase such as data exfiltration or theft. It should be noted that these extractions are often complicated to detect because attackers use tools and identifiers that are *a priori* legitimate.

Phase	Techniques	How does the attacker use it?	Impacts
Phase 1: discovery and primary infection	Buffer overflow. Example: - Stack Pivot	The attacker uses a buffer overflow by providing poorly formatted input data in order to make the targeted application write data to memory beyond the normal limit. This overwrites the correct data and allows the attacker to take control of the application's execution flow.	The code that the attacker has inserted into the targeted application allows them to gain remote access and/or download and execute other malicious files (payload).
Phase 1: discovery and primary infection	Packed Malware	This technique consists of preventing the analysis of the malicious file by security solutions by dynamically loading all functions.	Packers make it more difficult for security teams to identify malware and increase analysis time. In addition, the contents are hidden from signature-based solutions.
Phase 1: discovery and primary infection	Process Hollowing. Examples: - RunPE - Doppelgänging	The principle is to make the system execute malicious code by camouflaging it under the identity of a legitimate process. The RunPE technique exploits the weaknesses of the executable code loading system. The Doppelgänging technique uses the NTFS transaction mechanism.	Process hollowing allows the attacker to fly under the radar of security solutions that generally ignore the legitimate system processes that it is posing as. It being the process hollowing technique.
Phase 2: Lateral movement and expansion	Privilege elevation Examples: - DLL hijacking - Access token manipulation	The attacker tries to gain higher-level access to a workstation or system to achieve their goals. For the DLL hijacking technique, the attacker manipulates an application with elevated privileges by making it load a malicious DLL. For the access token manipulation, the attacker can steal or duplicate access tokens in order to modify the execution context of the targeted application, allowing them to gain additional permissions.	After obtaining advanced rights (administrator or system rights), the attacker becomes difficult to stop because they have a strong footprint in the target machine. These advanced rights facilitate the lateral movement of the attack. This may be possible in some cases without advanced rights.
Phase 2: Lateral movement and expansion	Pass the hash	The attacker steals a hash used to identify a more privileged account and can be potentially used to connect to other machines.	This technique allows the attacker to authenticate themself on other computers using this stolen identity. The aim is to infect new machines.
Phase 2: Lateral movement and expansion	Discovery of the network from the command line	The attacker uses commands (such as netdiscover) to detect workstations on the same network.	The attacker can gain a complete overview of the different networks in place.
Phase 3: impact	Data encryption	The attacker encrypts data stored on machines (workstations and servers) to make it inaccessible to the victim. They generally uses legitimate cryptographic techniques related to Windows APIs.	This technique is used in ransomware attacks in which the cybercriminal demands a ransom for data recovery.

4.1
The rule-based approach: an effective method

There are a number of solutions that use rules to perform detection on workstations. However, in some cases it is not possible for administrators to access them. It is true that the implementation of these rules is rather simple but they cannot be adapted to different business uses with particular security frameworks.

In other solutions, however, it is possible to find a certain level of configuration that can be adjusted to better suit the organisation where the solution is deployed.Thus, in addition to the rules provided by the security provider, the user can also include rules according to the position, the business, etc.

Some HIPS systems will combine several protection techniques together in the form of parameters or rules that form what is referred to as the "solution security policy". This allows the administrator to adapt it according to the business process to be protected. For some solutions, the various settings or rules can be customised, which offers better adaptation and protection for the organisation.

Did you know?

The behavioural rules applied on the agent side offer immediate protection of the workstation to limit the impact of an attack.

The granularity of the protection solutions used

Some solutions offer lists of predefined rules that can be extended by the administrator to counter malware.

As we have seen from the various examples provided previously, HIPS solutions that provide **configurable and very fine-grained rule sets to control any action performed on workstations**, such as the monitoring of running processes, files and registry keys, privilege elevation etc., should be given preference.

This granularity allows the organisation's administrators a high degree of customisation and, more generally, the possibility of implementing a security policy that is as close as possible to the needs and requirements of the organisation.

As a general rule, a workstation or server should be considered according to its context (e.g. outside or inside the company network) and its level of exposure to threats.

4.2 The contextual approach: better understanding the environment

Each organisation is unique and has different needs. The protection solution must be able to adapt to the different use cases. As a result, the workstation and server protection chosen must **be adapted to the context of use of each individual and take into account different mobility scenarios**. For example, to control which Wi-Fi networks are allowed, and to disable them when a LAN connection is active. Or to block any connection other than the VPN when it is active to prevent rebound attacks.

Thus, the implementation and use of a workstation protection solution must have a security policy that is capable of being dynamic. That is, it must **know where the workstation in question is located and adapt its security to the particular environment**.

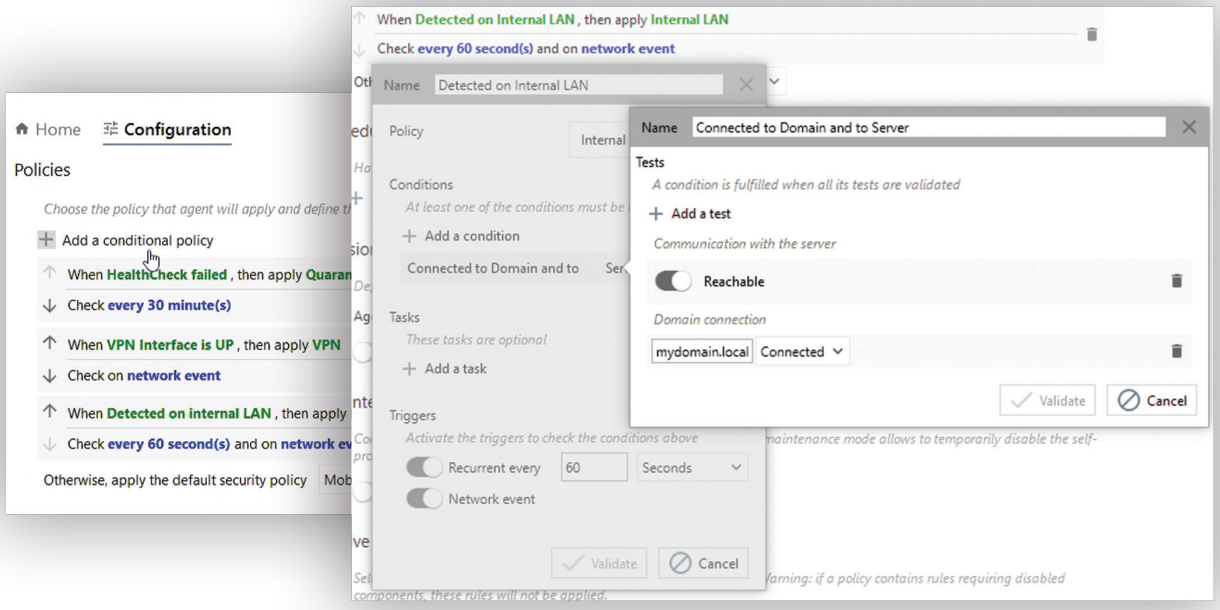


Figure 1

Endpoint security solution with different security policies

4.3
"Hardening" security solution self protection

Security solutions are a target for attack by cybercriminals. They seek to disable protection or take advantage of the privileged rights of these solutions by misusing them. Moreover, as the ANSSI[9] points out, the software (and hardware) of an infrastructure must be checked and its configuration hardened before it is used.

The attack surface must also be taken into account. Experts agree that each new component (hardware and software) added to the infrastructure increases the risk that there will be a bug or vulnerability related to that component, allowing it to be exploited by a cyberattacker.

In order to limit the attack surface and reinforce the protection of workstations, some protection solutions integrate the *Security by design approach*[10] into their development. That is, solutions in which security and the associated risks are integrated and studied from the product design stage onwards.

[9] https://www.ssi.gouv.fr/uploads/2020/08/anssi-guide-recommandations_architectures_systemes_information_sensibles_ou_diffusion_restreinte-v1.1.pdf

[10] https://www.securecontrolsframework.com/security-privacy-design-principles

[11] https://www.zdnet.fr/actualites/une-faille-0day-de-l-antivirus-trend-micro-utilisee-dans-le-piratage-de-mitsubishi-electric-39898077.htm

Cyberattack at Mitsubishi Electric[11]

The Japanese carmaker has acknowledged that it suffered a cyberattack in June 2019. According to an investigation carried out over several months, attackers gained access to the company's internal network and stole 200 MB of sensitive files related to thousands of their employees and also of confidential technical information

How did this happen?

A Chinese-based cybercriminal group allegedly exploited a 0-Day vulnerability in the organisation's antivirus software to install malicious files. According to the manufacturer of the hacked software, the criminals exploited a directory traversal vulnerability to extract files from an arbitrary zip file to a specific folder on the antivirus server. This apparently allowed *Remote Code Execution*.

To do this, the general architecture of this type of solution must be developed according to defensive software programming rules around a secure micro-services architecture. This is precisely where the principle of least privilege applies.

This enables the solution to be split into **several independent services** guaranteeing maximum security, each with a specific role and limited privileges. Thus, for example, the module that manages the connection to the configuration server must not be that in charge of interpreting this data. Or the service managing logs is exclusively in charge of this task and cannot access the security cybercriminal policy in place.



Figure 2
Security solution divided into several independent services

To achieve a high level of robustness, the processes for building security software must also define strict coding rules and provide for the use of various compilation and execution options. These options enable the limitation of the risk of exploitation in the event of a bug and also the limitation of the number of errors by increasing checks before and during execution.

In summary, **hardened or robust solutions based on these principles provide better protection against cyberattacks**.

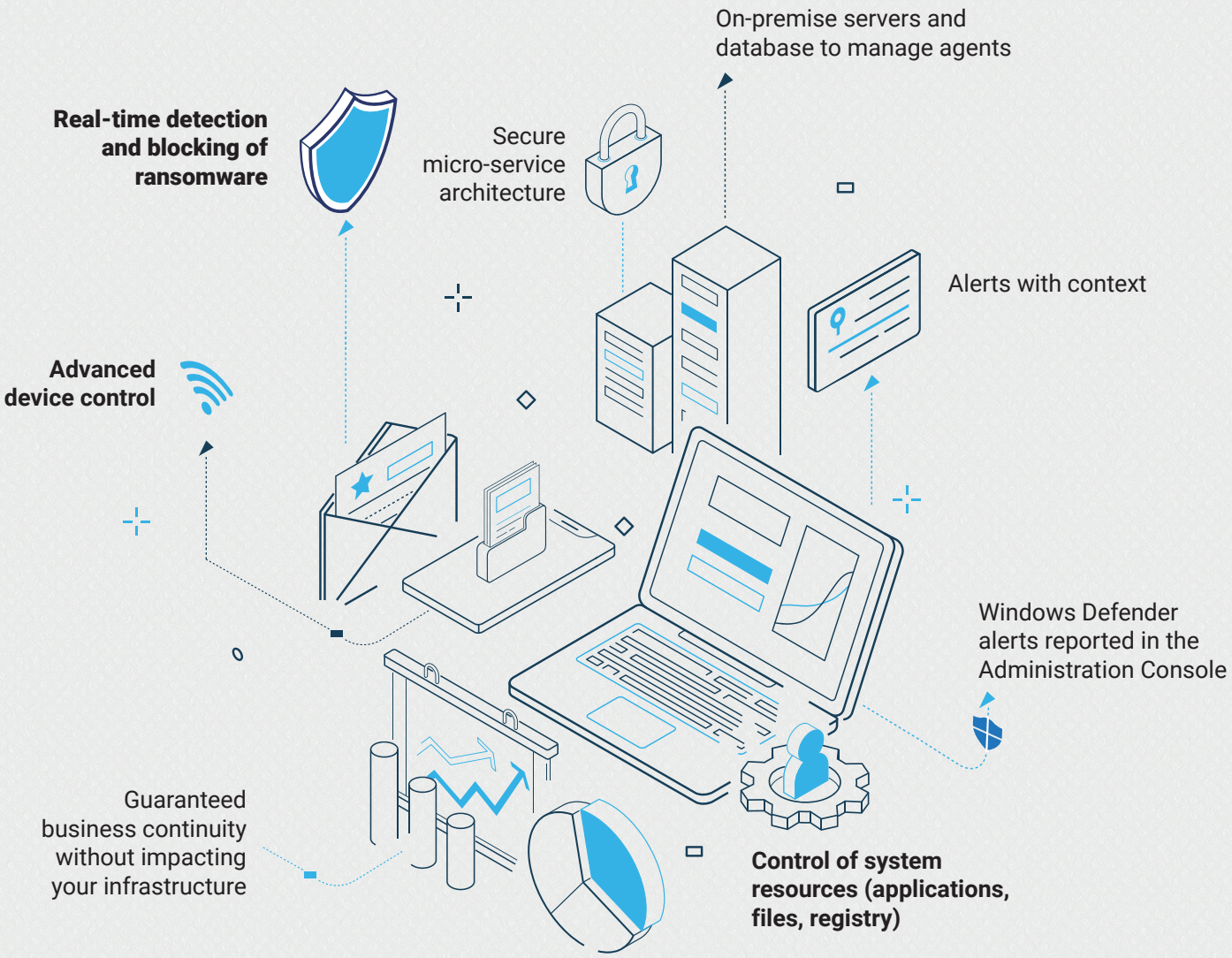
Stormshield Endpoint Security Evolution: the workstation protection solution

Stormshield Endpoint Security Evolution **protects sensitive environments** by blocking attacks at the earliest stage, before they impact your environment

Advanced behavioural analysis capable of blocking unknown threats, 0-Day attacks and fileless attacks.

Stand-alone solution that requires no network connection to operate and maintain endpoint security.

Advanced device control. Extensive range of controls to manage WiFi networks, USB devices, disk volume access and network connections.



91%

of targeted attacks are carried out using spear phishing

40%

of primary infections use the process hollowing technique

255%

Increase in ransomware reports in 2020 (according to a study by ANSSI)

SOME EXAMPLES OF ATTACKS

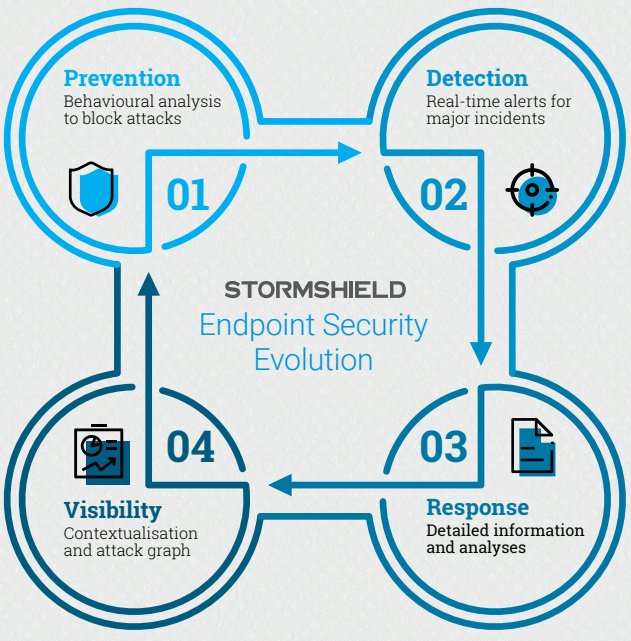
- COMPUTER WORM
- E-MAIL MALWARE
- INFECTED DEVICES
- PASSWORD STEALING
- SYSTEM SCANNING
- FILELESS ATTACK
- PHISHING
- HACKER
- TROJAN
- DATA LOSS
- SOFTWARE VULNERABILITIES
- ...

SOME ESSENTIAL ADVICE

Beware of suspicious emails with attachments or links to questionable sites.

Carry out **regular backups.**

Update your applications, plugins and operating systems.



THE **EUROPEAN CHOICE** IN **CYBERSECURITY**

www.stormshield.com

All distribution, reproduction or representation, even in part, of this white paper, for any purposes other than private use, regardless of the medium, is prohibited, and may engage the civil and criminal liability of any person failing to comply with this prohibition.

Copyright © 2022 Stormshield