STORMSHIELD

VISION: MULTILAYER COLLABORATIVE SECURITY

COORDINATING PROTECTION SYSTEMS
IN ORDER TO RAISE THE OVERALL LEVEL OF SECURITY
AND COUNTER THE MOST SOPHISTICATED ATTACKS

White Paper

NETWORK SECURITY I ENDPOINT SECURITY I DATA SECURITY

Difficult to detect, **the latest advanced attacks require multilayered protection**. Corporate security solutions therefore must be carefully integrated and coordinated.

Attacks launched on networks keep getting more elaborate and harder to detect. Highly discreet, these threats combine several attack vectors to achieve their goals.

Once a victim has been identified, such attacks often start off by using the first intrusion vector which appears harmless. At this stage, victims do not realize they have fallen prey to an attack that the protection systems in place have completely failed to notice. The attack will then spread to the targeted network through several distinct and successive techniques in order to attain the objective that has been defined (server corruption, data exfiltration, etc). The time between the start of the attack and when the objective is achieved is one of the characteristics of **APTs (Advanced Persistent Threats).**

COORDINATED PROTECTION

These advanced attacks have been designed to bypass conventional protection systems, and the combination of several security solutions in the form of silos is not even effective enough. However, these attacks leave trails that act as weak signals, such as access to an uncategorized website, for example.

By associating these weak signals with each other and correlating them to a vulnerability map, a threat can then be identified, thereby revealing its true critical nature. Multilevel attacks **can therefore be countered by associating several layers of protection and making them interact with each other.**

In practice, this can be done in two distinct ways. The first consists of correlating events through SIEM solutions. Security events and incidents are collected then analyzed in order to identify abnormal behavior. However, events can only be correlated once an attack has taken place. The administrator can only take reactive action on the security policy.

In the second way – with an approach based on the integration of security engines and actual interaction between the various defense solutions – the different protection methods collaborate to exchange data and analyze behavior according to other events detected. **Correlation takes place in real time and the various weak signals are taken into account globally.** In this way, the level of protection is strengthened and the security policy can be adapted dynamically. Abnormal behavior can then be blocked more quickly, and even proactively.

This approach is the basis of Stormshield's vision for countering new threats.

CONTENT

Understanding advanced attacks

When they are careful prepared, advanced attacks exploit vulnerabilities in order to weave their way into the internal network, locate new targets then **disable crucial services or steal sensitive data**.

AN ENVIRONMENT OPEN TO VULNERABLE PLATFORMS

Within three decades, the digital landscape has undergone full transformation: IT has become a commodity, while PCs, smartphones and touchscreen tablets themselves have changed the habits of private and professional users. The web and social networks have also revolutionized the way we communicate and work. Creating and sharing information has never been easier – everyone can share content and interact with his environment.

This open and constantly connected environment is a golden opportunity for abuse. Since user awareness has increased over the years, hackers need to find more elaborate techniques to achieve their goals. They now exploit vulnerabilities on legitimate websites or in e-mail attachments to infect the workstations of users who open them. Malicious code that hackers use often exploits zero-day vulnerabilities, particularly those in applications that are most frequently used for reading documents or web content.

Every day, new websites are taken hostage with the aim of injecting and hosting malicious code. Such code hijacks the numerous vulnerabilities found on web browsers and their associated components, like Flash or Java, to compromise the workstations of internet users.

Improved attack techniques also respond to the evolution of protection methods. The current principle consists of either using totally unknown malicious code or combining several techniques that display a sufficiently low level of gravity to sneak through filters that have been set up.

A WELL-ORGANIZED THREAT

Cybercrime has become an underground economy of its own with its organizations, dedicated sources of financing and currencies. The objectives of cybercrime are varied:

- Cyberwarfare, political destabilization, cyberespionage on behalf of state organizations,
- Political or ideological activism (Anonymous or Lultsec),

- Financial gain (ransom, blackmail, data theft or resale, hacking or attack "services"),

Cybercrime is often very well prepared so that attacks can be launched efficiently and on target. To successfully pull off a malicious campaign, the objective and target are jointly and carefully selected.

Table 1 illustrates how APTs indiscriminately strike government ministries, newspapers, IT companies, energy and leisure industries.

Attack	Year	Vector	Objectives	Target(s)	Sources suspected
Stuxnet	2008	USB key and worm attacking a Siemens industrial control system	Industrial sabotage by compromising centrifuges	Nuclear industry in Iran	USA and Israel
Operation Aurora	2009	Zero-day vulnerabilities and backdoor	Theft of source code from innovative MNCs	Source code repositories of Adobe, Google, Juniper, Rackspace, etc.	China
Bercy (French ministry of the economy, finance and industry)	2010	PDF attachment with Trojan horse	Gathering of information on G20	150 systems infected	Asia
RSA	2011	Htran malware	Theft of information regarding SecurID tokens	Network of the security branch of the EMC group	China
New York Times	2013	'Spear-phishing' attack: e-mails with malicious links	Theft of passwords and journalists' files	The daily's offices	China
Sony Pictures	2014	Probable spear-phishing with Trojan horse and ransomware	Destruction of files, theft of private data and unreleased films	Production servers of studios	North Korea

Table 1
Several high-profile APT attacks since 2008

NO ONE IS SPARED

Cybercrime in all its forms takes advantage of the interconnection of the information systems of companies of all sizes, grouped together in IT ecosystems. As a result, no supplier, commercial or technological partner is spared.

To escape the notice of a targeted corporation, a hacker relies on the IT networks woven between small and medium businesses working together in complete trust. By simply compromising a host on a partner's or subcontractor's network, the entire ecosystem will be jeopardized.

Given the diversity of the reasons behind cybercrime, most of the smallest structures are also concerned. Indeed, the financial data of clients of an accounting firm, information on patients of a medical center or the manufacturing secrets of a research unit are all examples of data to be protected. Moreover, a security incident on the information system of a small structure can quickly lead to the shutdown of its activity, since it has become heavily reliant on the use of computers tools.

AN ONLINE INFORMATION GOLDMINE

The explosion of social networks has made it so much easier to collect information on the victim and increase the chances of a successful hack. Once a targeted corporation has been chosen and the objectives defined, the hacker will first start identifying the victim of the primary attack, in general an employee of the corporation who is active on social networks. The aim of this tactic is to devise a way to deceive the targeted employee.

This phase of the social engineering plan makes it possible to distinguish the attack vector, such as an e-mail with targeted content or a USB key left intentionally at a place the victim frequents.

THE THREE PHASES OF AN APT

The most elaborate threats are conveyed by an APT (Advanced Persistent Threat). Highly targeted, the APT combines several attack vectors and is executed in three phases in order to go unnoticed.

An APT is prepared by choosing the targeted corporation and its victim. A social engineering exploit determines the ideal vector for the primary attack in order to increase its chances of success. Then, the attack will take off with a primary infection that takes advantage of the vulnerabilities on applications on the victim's workstation. The attack vector – an e-mail or a USB key – will contain either a specially forged

attached document or a link to a malicious website.

Once the victim's workstation is infected, the expansion phase will aim to reach the host or even the targeted data. The first viral load may be modified in order to set up a command and control channel and seek to compromise other machines connected to the network. Lastly, the advanced persistent attack will enter its third phase to implement the action defined. At this stage, the attack will become active and disable a server or even extricate confidential data. If a disabled server quickly reveals that an attack has taken place, the data leak may be gradual – the attack would then persist and remain undetectable.

Take for example an employee in charge of shipping orders. Social engineering would make it possible to identify this victim's workstation and the name of a regular logistics carrier. To make the employee believe that he is reading an official message, a malicious e-mail will spoof the carrier's identity and include a plausible attachment, such as an order form:

PHASE 1 :
THE PRIMARY INFECTION

Malicious code relies on vulnerabilities found on common applications such as web browsers and office tools (Office, PDF). Flaws on web browsers and their software components create a very particular target as one out of every three web attacks exploits vulnerabilities on Java plugins in this way.

Another way in which malicious code can be transported is by documents attached to e-mails. The victim will open an attached document or will visit a corrupted website, installing the malicious code without realizing it. Since this installation process takes place without incident, the victim would not suspect anything.

Going back to our example, the employee in charge of shipping orders would assume he is opening an ordinary order form. Once this document is opened, a system flaw will be exploited to discreetly install malicious code.

PHASE 2 :
EXPANSION

The primary infection creates the entry point for the advanced persistent attack, which will then attempt to spread through the targeted corporation. The APT combines several vectors in order to find various anchoring points and attain the objective set. In general, these anchoring points are initiated by setting up a command and control channel between the attacker and the compromised hosts. This channel will allow the hacker to remotely modify the behavior of the malicious load. In this way, the infected host will set up a legitimate connection to an unknown command and control server.

The expansion phase takes place on two simultaneous focus points:

- The malicious load is transformed through the command and control channel. It can upgrade the malware in order to add features so that it can penetrate the targeted corporation more efficiently. It may also attempt to increase privileges or execute arbitrary code in order to set up network connections on other hosts or even replay an authentication phase.
- The number of infected hosts goes up: the malicious code or the unknown command and control channel acts as a relay to search for new vulnerable hosts. This phase combines various attack vectors and seeks to compromise hosts that may potentially be less protected.

The purpose of spreading the attack is to reach the set target in advance, a financial transaction server or a database. Once this target has been located, the APT enters its final phase. This is when the attack becomes truly active, and only in certain cases, detectable.

PHASE 3 : COMPROMISING OR LEAKING DATA

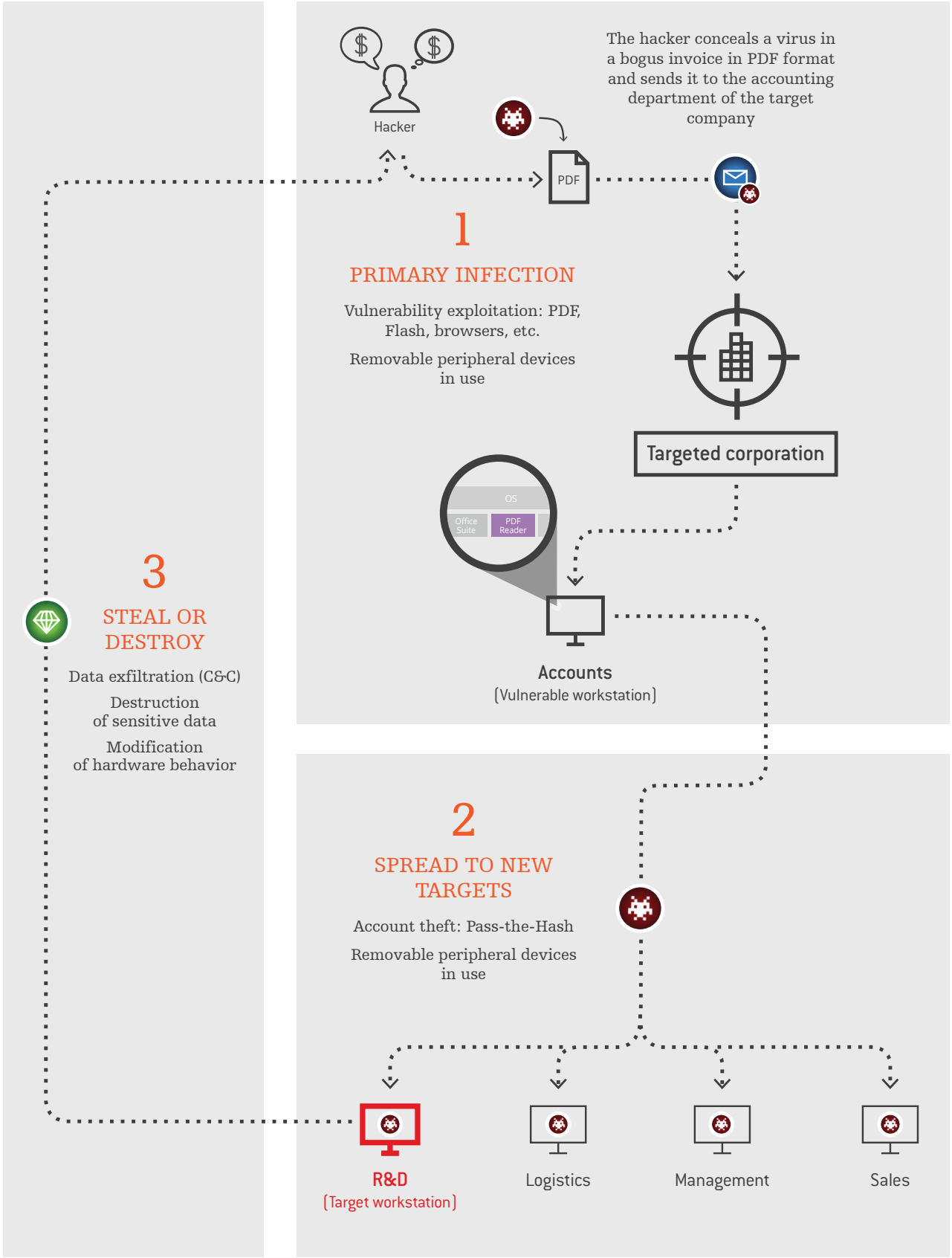
This phase of the advanced persistent attack strikes the chosen platform with a specific objective. This may be a PC in the Human Resource Department that produces pay slips, a workstation in the supply chain department, or an e-commerce or financial transaction server. The attacker has prepared his attack, for example, to hold up an online service in order to demand a ransom before he allows it to run again, or to extract confidential data for the purpose of reselling it. To illustrate this point, in June 2014 Domino's Pizza was asked to pay up 30 000 € after the theft of 600 000 clients' personal information.

In the case of a compromised server, the implementation of an attack indicates the presence of malicious code within the targeted corporation. Even so, it will not be eradicated instantaneously after this discovery. The server may be reinstated until the attacker decides once more to exploit the harmful code, demand a new ransom or destroy files remotely.

In the case of a sufficiently discreet data leak, the APT attack may not necessarily be detected. The attack can then continue to retrieve confidential information for many months or years.

Illustration of a sophisticated attack

How Advanced Attacks work



Choose multilayer protection

The protection solutions set up on a corporate network have to **exchange information on behavior observed between themselves and on a global scale**, in order to be ready when the next attack strikes.

LIMITS TO SILO PROTECTION SYSTEMS

When pitted against increasingly sophisticated threats, conventional protection mechanisms (antivirus, IPS, HIPS, URL filtering, etc) do indeed diminish the surface of an attack but also show their limits. The combination of several attack vectors and the APT's unit loads increase the risks. Since the primary infection of the APT does not directly activate malicious code, it uses a system or application vulnerability to locate and then control the targeted computer remotely.

The malicious load that exploits an office application's vulnerability often has no impact on the operation of a workstation. It will, for example, initiate an http connection to a command and control server to activate new malicious code. As it is not detected as a genuine threat, conventional protection solutions will not block it. Given the fact that such loads are often specially forged, signature-based systems would not know it.

The threat gets real only when the primary infection is associated with the expansion. In a real zero-day threat, the risk increases the more the attack spreads. The advanced attack will however leave trails (connection to a website that does not fall under any category on the web filter solution, alert upon the detection of interactive connections or even suspicious internal connections) which are considered weak signals.

The real threat appears more obvious when various events, seemingly harmless when considered on their own, are correlated. As a result, full understanding of the context in which these weak signals come into play is paramount in identifying or blocking advanced persistent attacks.

CORRELATION OF EVENTS

A global vision of security events that occur on the corporate network provides the context in which the advanced persistent attack takes place. Several types of suspicious behavior and weak signals appear from a central point, facilitating the detection of a multivector threat. Analyzing many security events would allow identifying each of these threats singularly and suspecting overall abnormal behavior. On the other hand, the detection of the APT requires an additional analysis.

The application of event correlation facilitates the analysis, as it could highlight a sudden spike in the number of connections from a certain host and over a defined time slot, connections to unusual services or resources, etc.

In this way, associating individual events provides a contextual view that may reveal an advanced persistent attack. Despite the advantage that this approach has of not disrupting production, it only detects the attack after it has occurred. It also requires permanent monitoring in order to analyze alerts and apply the remediation measures that must be implemented in the event of a disaster.

MULTILAYER APPROACH

The analysis of correlated events only allows countering advanced attacks reactively. A proactive approach therefore needs to be set up in order to raise the level of protection and prevent operations teams from being overloaded. The principle of this approach is the collaboration of various protection methods over 3 distinct layers:

- **Layer 1 – Collaborative protection:** the protection engines belonging to a system (multifunction firewall or workstation protection) exchange information on weak signals observed in order to detect and block malicious behavior,
- **Layer 2 – Contextual protection:** the various security solutions of the information system work with each other to exchange their weak signals, identify new illegitimate behavior and offer a coordinated response,
- **Layer 3 – Global protection:** all the protection solutions deployed in multiple organizations report information that would allow obtaining a global vision of threats and observing new anomalies. Making use of such data would then enable the implementation of countermeasures or new protection methods that will be made available to security solutions.

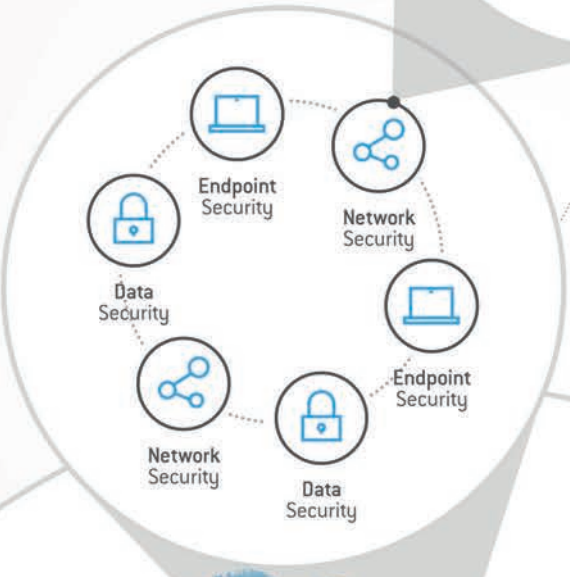
Multi-Layer Collaborative Security

by Stormshield

STORMSHIELD

1 Collaborative protection

Protection engines belonging to a system (multifunction firewall or workstation protection) **exchange information on weak signals observed**



2 Contextual protection

The various security solutions of the information system **work with each other** to exchange their weak signals

3 Global protection

Making use of such data would then enable **the implementation of countermeasures or new protection methods** that will be made available to security solutions

COLLABORATIVE PROTECTION

The first layer of this new approach consists of integrating the protection engines of a security solution so that they work together. For example, multifunction protection solutions and new-generation firewalls offer several security components. In general, these products provide traffic filtering functions as well as intrusion prevention, antivirus, antispam, URL filtering, data leak prevention and even vulnerability detection.

Each of these functions only takes into account the context it is supposed to act on. The network traffic control and filter function is able to block access from a malicious host. Intrusion prevention can raise an alert if a session appears suspicious or a new command and control channel appears. The antispam module reports information on the main recipients of unsolicited mail linked to social networks, and vulnerability detection can map the risk level of connected hosts in the company.

Even though each component runs independently, reproducing the limits of silo protection, they could make their different engines work together in order to increase the level of security. When processing traffic or data, each module would take into account the operations carried out or the information provided by the other modules. When it assesses behavior, the security module would act according to the context in which a probable attack would take place.

Take the example of a vulnerable host used for visiting an uncategorized website. It does not pose any particular risk and the website only presents a moderate risk. However, if the URL filtering module knows that this site is being visited from a vulnerable host on which interactive connections have been detected, it may block access to this website.

Each security module would contribute in this way to the overall protection at the level of the new-generation firewall. Instead of simply allowing an event deemed low-risk to pass through, a particular module may record a weak signal and define the associated risk level.

When another module then analyzes an event in relation to the first, it would be able to raise the risk level or block access. The various risk levels would have their own weight that would then add up as the protection modules coordinate to detect attacks. Each module would correlate the event it is processing with the risk levels defined by the other modules in order to consider the threat from a global point of view.

The protection system may then set off an action according to the result of the global analysis. It would block traffic or quarantine a suspicious host or place it in a

remediation zone. The threat would then be blocked or mitigated, thereby increasing the level of protection.

CONTEXTUAL PROTECTION

The second layer of this new approach is more global, considering that a corporation has protection systems deployed in several locations within its infrastructure. A new-generation firewall protects network access as well as traffic passing through the corporate network. A system deployed on workstations intercepts the most sophisticated zero-day threats and examines the other attack vectors (USB key, negligence or internal abuse).

Following the same principle of correlating weak signals on a collaborative solution, the collaboration between the various security solutions would make it possible to further increase the level of protection. Not only will events relating to network traffic or workstation protection be taken into account, but all security information available within the corporation – protection then becomes context-based.

Going back to our example of the vulnerable host, the vulnerability detection mechanism is enhanced and offers more accurate contextual information. Indeed, an analysis of vulnerabilities would reveal a potential risk relating to the presence of a weakness in an application, whether it is exploited or not. If, after such behavior has been detected on the new-generation firewall, the workstation protection solution detects illegal memory access or prohibited use of a USB key, such relevant information would correct the exact measurement of the risk level.

Security systems have a lot to gain by working together and exchanging information in order to increase the level of protection. The new-generation firewall could then restrict network access to a quarantine zone for a host whose memory has been accessed illegally. It could also ask the protection system on a workstation to modify the security policy in order to isolate the host or restrict its access to only the decontamination server. Likewise, the workstation protection system could share with the firewall information on illegal content in order to counter the lateralization of an attack or protect hosts that do not have advanced protection systems.

GLOBAL PROTECTION

Since cybercrime operates on a worldwide scale, a global response would be most appropriate. From protection solutions deployed around the world, security

information can be collected and correlated on a global scale. This approach makes it possible to follow the latest attack techniques appearing all around the globe and provide an active or proactive response.

This approach has already been implemented by antivirus software vendors for many years. Once gathered data has been analyzed, it reports on the latest attack behavior as well as the latest vectors used. It is therefore possible to improve protection mechanisms and provide responses to the zero-day exploits used. The worldwide data collection allows providing a global response to the threat.

Apart from the latest exploits used, the analysis of consolidated data also makes it possible to understand how vectors and viral loads are coordinated. In this way, new attack techniques can be anticipated. By including international organizations such as CERT, SOCs or MSSPs, the data collection zone can be further widened. It will involve protection solutions of various origins and several operations centers that monitor security in order to offer an even wider response. In addition to the quantitative aspect mentioned earlier, these organizations are also capable of providing a qualitative approach to new types of behavior.

The collaborative exchange of data with the security ecosystem on online threats also helps in the preparation of effective countermeasures. There are three possible types of responses:

- Signature definition offers the capability to respond to an attack that has been discovered. In general, the signature can identify the viral load that was exploited.
- The behavioral response provides protection based on the legitimate use of a resource (network, memory or data registry). It anticipates the exploitation of a zero-day vulnerability.
- The context-based response takes into account all protection modules. It can modify the weight of the various weak signals according to data that has been collected recently.

These countermeasures may be deployed in the form of new signatures, software upgrades or configuration recommendations, and using them would strengthen information security on a global scale.

Stormshield's approach

As a response to the compromise of critical services and the leak of corporate data deemed sensitive, **Stormshield provides monitoring of threats on a global scale and a comprehensive system of coordinated protection**.

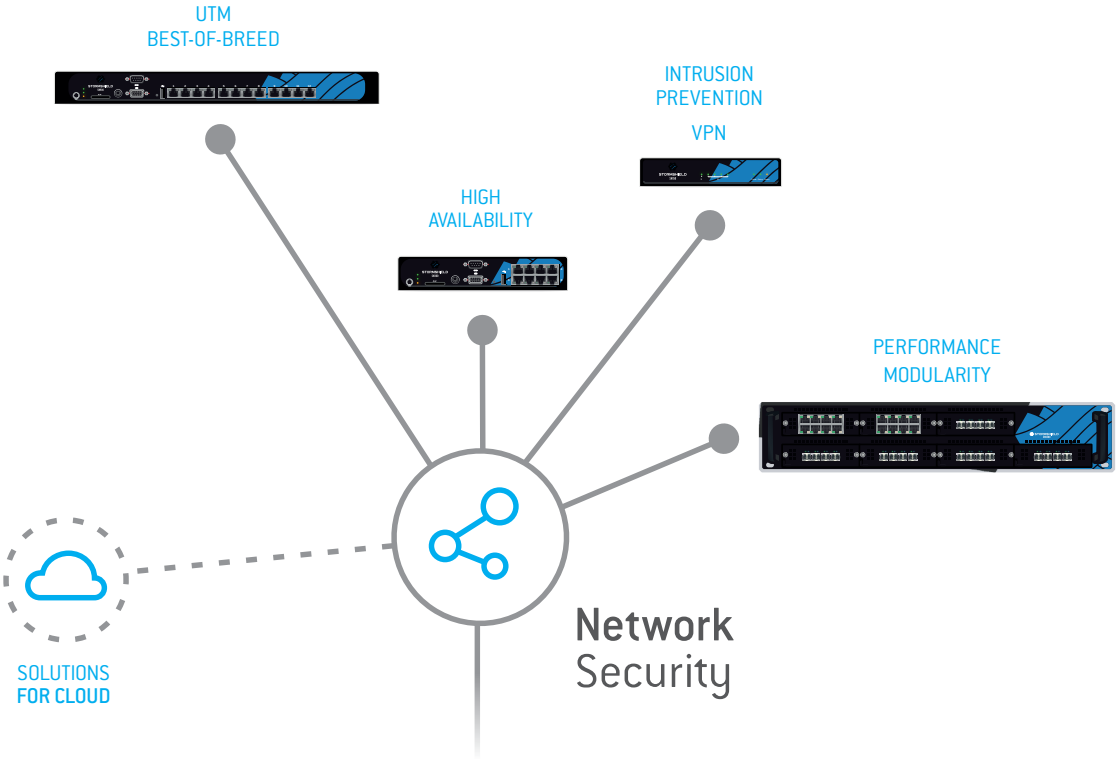
This new **Multilayer Collaborative Security approach** is the basis of Stormshield's vision to improve security. It serves as the main theme for the development of its multifunction solutions and its multiproduct portfolio.

The **Stormshield Network Security** product range groups a set of multifunction network protection solutions that integrate, among other components, a vulnerability management module. **Stormshield Endpoint Security** products provide effective workstation protection that responds to the most sophisticated attacks. **Stormshield Data Security** offers protection for the most sensitive information, guaranteeing an effective barrier against data leaks.

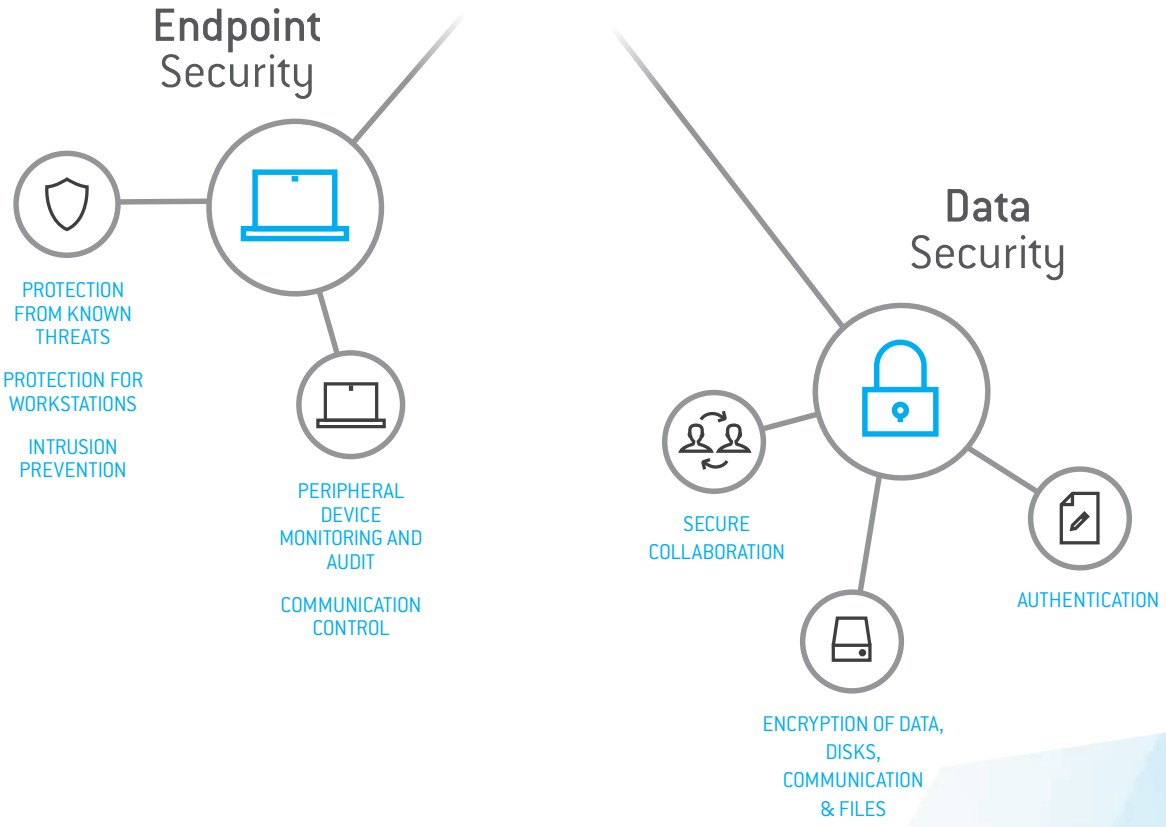
By involving the cooperation of its security modules and products, Stormshield is able to provide a response on the first two layers of the collaborative approach. The way information is reported on products deployed ensures that a global vision of the threat is given on the scale of all these clients*.

This synergy benefits Stormshield's vision, which consists of responding to mutivector threats through effective and multilayered protection, internal collaboration, context-based protection and a global analysis of threats.

* may be disabled



MULTI-LAYER COLLABORATIVE SECURITY



STORMSHIELD

Phone

+33 9 69 32 96 29

WWW.STORMSHIELD.EU

Arkoon Network Security

1 place Verrazzano - CS 30603 69258 - Lyon Cedex 09 - FRANCE

Netasq

Parc Scientifique Haute Borne - Parc Horizon, Bat 6, Avenue de l'Horizon 59650 Villeneuve d'Ascq - FRANCE