CONTEXT/BEHAVIOR-AWARE ENDPOINT PROTECTION AND RESPONSE TO MEET DIGITAL AND HYBRID WORKFORCE REQUIREMENTS

Author:

Romain Fouchereau

January 2022

An IDC Technology Spotlight sponsored by Stormshield

IDC #EUR148675622

Context/Behavior-Aware Endpoint Protection and Response to Meet Digital and Hybrid Workforce Requirements

Introduction

Endpoint security has evolved considerably over the years, but it remains a predominantly on-premises or on-device matter as most solutions require an agent deployed on the endpoints themselves to deliver the necessary functionality. A lot of those solutions do, however, use a cloud backend for analytics and to drive responses such as blocking connections or isolating endpoints.

IDC defines modern endpoint security as products that protect personal computing devices (PCDs, such as workstations and laptops) from cyberattacks through the detection of malicious code and behaviors present or operating within the PCD and then facilitate a counteracting response (e.g., block, remove, or isolate). Modern endpoint security products contain two detection and response mechanisms that are differentiated by response time and human involvement.

Endpoint protection platforms (EPPs) reach detection verdicts and initiate responses in real time and autonomously (i.e., provide removal and cleaning features without human involvement). Endpoint detection and response (EDR) is a second stage of detection and response for cyberattacks that have evaded EPP detection.

AT A GLANCE

Deploying behavioral analysis-based endpoint protection, a solution that is not cloud based and does not rely on a signature for zero-day attack protection, will not only ensure optimal protection, but will also have direct benefits for end users, security teams, and the business.

WHAT'S IMPORTANT

Benefits of behavioral analysis endpoint protection:

- » Behavioral analysis leveraging techniques used by hackers
- » Context sensitive and risk aware, it adjusts the security level to the environment
- » Dynamic security policies fit new hybrid work model requirements
- » Self-protection to stop changes in applications that try to disable the endpoint protection
- » Incident analysis with contextual data and response information for further analysis

With EDR, the time to reach detection verdicts and initiate responses can span minutes to days. How fast the cyberattack unfolds, its sequence of steps, and its sophistication and uniqueness are factors that affect the elapsed time in detection and response. Automation and predefined workflows help reduce the elapsed time, and human involvement from security analysts is typically kept at a minimum to confirm detection and/or authorize response.

Modern detection has moved on from relying solely on signature-based detection and is now powered by multiple engines that also examine system, memory, application, behaviors, network communications, and context.

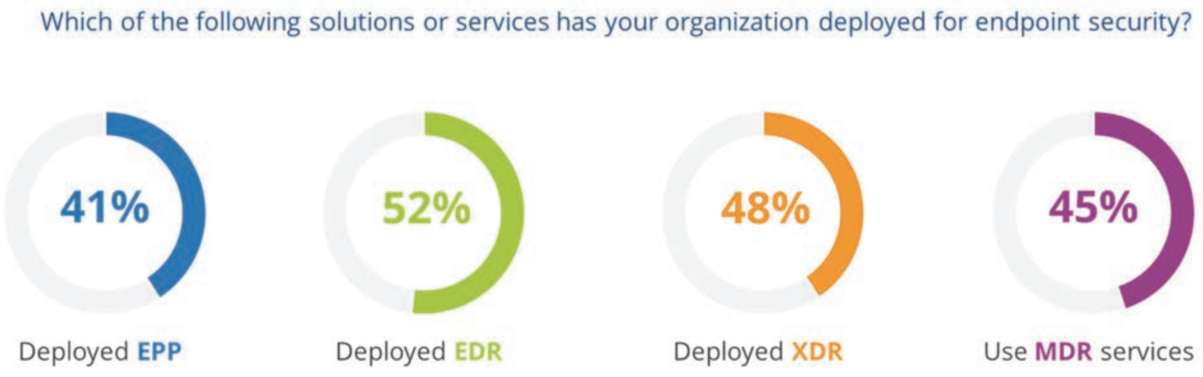
For European organizations deploying modern endpoints the main adoption drivers include the need for:

- More rapid and proactive detection of threats to mitigate potential damage to infrastructure and limit or prevent interruption of operational capabilities
- More sophisticated and contextually aware approaches to detect advanced or stealthy/evasive threats
- Improved response capabilities to accelerate and even automate containment and remediation to mitigate risk

According to IDC's 2021 European Security Survey, which asked security professionals across 12 European countries about their general approach to security and their security priorities and strategy, 41% of European organizations have deployed EPP and 52% have deployed EDR; 48% have deployed extended detection and response (XDR) services and 45% are using managed detection and response (MDR).

FIGURE 1

Endpoint Security Solution Deployment Types



Source: IDC 2021 European Security Survey (n = 140)

Technology Benefits and Trends

The way employees work has changed dramatically in recent years, with remote-working and working-from-anywhere models becoming the norm. As a result, endpoint protection needs to evolve to address new risks and threats in untrusted environments. Organizations can choose to deploy behavioral analysis-based endpoint protection, a solution that goes further than traditional EPP, because unlike most other endpoint solutions, it is not cloud based and does not rely on a signature for zero-day attack protection. Adopting this type of technology for endpoint security will also have some direct benefits for end users, security teams, and the business.

Benefits for Users

Being able to dynamically adapt to the environment — whether in the corporate office, at home, or on the go — means that the endpoint can take immediate action when necessary and adjust the level of protection in the event of a change in the surrounding context. This means that end users can work from anywhere with the same protection; unlike cloud-based endpoint solutions, the lack of connection does not impact the level of protection, which means they can work offline with no added risk. It also means that malicious behavior from USB plugged-in devices, for example, can be monitored without relying on connecting to a remote server as with traditional endpoint protection.

Benefits for Security Teams

Threat detection is a crucial component of an organization's overall security strategy because without effective detection, threats could become potential breaches even before remediation can be enforced. For the security teams, the endpoint solution will detect vulnerability exploitation and malware behavior to block known and unknown attacks. Behavioral protections and information gathering will help to block attacks and provide critical information to understand and analyze them.

In terms of monitoring, when an attack is detected, information provided by the security solution will help IT security teams assess the situation and immediately take the necessary steps. The information can then be fed back into a SIEM to gain better visibility and reactivity, so automated responses can be activated to deal with identified threats.

For incident analysis, leveraging context-based approach events and telemetry will help reduce time spent on logs and facilitate understanding of the exact situation for the analyst team.

Another benefit revolves around threat hunting, to detect possible threats that have eluded other security systems and might still exist within the organization. Leveraging insights on alerts (including what caused them) will enable analysts to determine if further action is required. For each event related to the attack, detailed technical information can be retrieved to investigate further and take the appropriate actions if needed.

Benefits for Business

Modern endpoint security products are a component of many interconnected and complementary security technologies and operations that function together to increase the security posture of endpoints and the resilience of business functions. This holistic view of endpoint security means that organizations benefit from the integration of products within the existing IT security environment to move into XDR capabilities, with software solutions that include endpoint telemetry but also complementary telemetry from network, cloud, mobile, and IoT, for example.

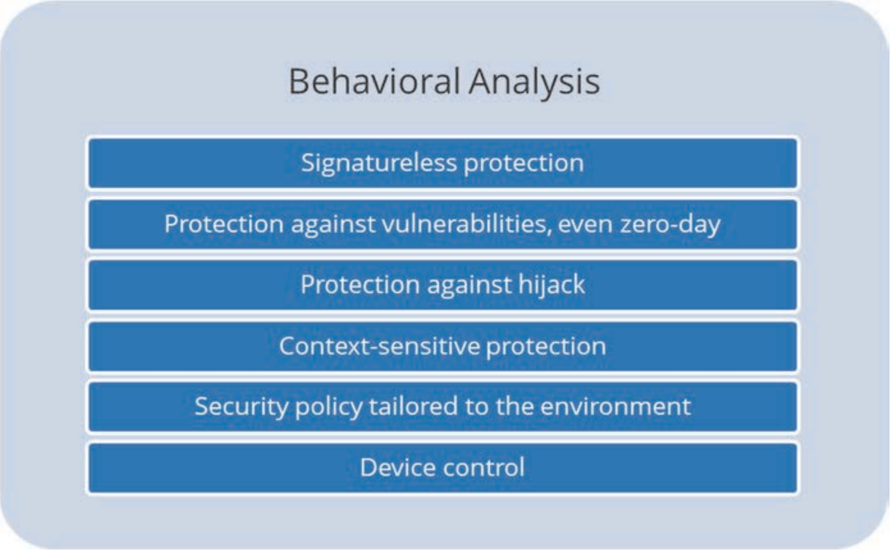
The integration of EPP and EDR enables additional security and IT hygiene functionality to create a unified risk reduction and breach avoidance platform. Accelerating and improving detection and response capabilities is not just about security, but also about building the resilience of business processes and ensuring service availability. The context-based approach will also help in zero-trust architecture — the control of communications between the endpoint and apps or data depending on the context — and this creates a more secure environment that protects against unauthorized access to sensitive data and digital assets. The shift to zero-trust models is in response to the continuous increase in users, devices, and network and cloud applications accessing the corporate network. It reduces business and organizational risk and securely enables new IT initiatives for digital transformation (DX) programs.

Stormshield Endpoint Security Evolution

The SES Evolution endpoint solution prevents sophisticated cyberattacks by increasing the security level to ensure optimal protection. It suits companies that want to keep control of the overall solution. It is also a good solution for customers looking for the same level of protection whether connected or not provided by autonomous agent. Based on behavioral analysis technology, the agent recognizes attack techniques such as the exploitation of application vulnerabilities or ransomware distinctive actions.

FIGURE 2

Behavioral Analysis Technologies



Behavioral Analysis

Signatureless protection

Protection against vulnerabilities, even zero-day

Protection against hijack

Context-sensitive protection

Security policy tailored to the environment

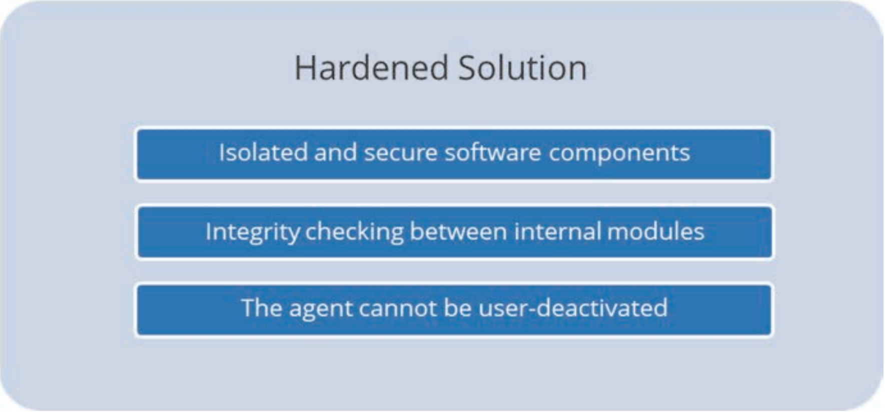
Device control

Source: IDC, 2022

Besides behavioral analysis, SES Evolution is also built to be resilient. This hardened solution has been developed by using defensive programming techniques. Its architecture is designed to prevent it from being compromised and limits the attack surface to its minimum level.

FIGURE 3

Hardened Solution Defense



Hardened Solution

Isolated and secure software components

Integrity checking between internal modules

The agent cannot be user-deactivated

Source: IDC, 2022

By pairing this technology with EDR features, SES Evolution can proactively block sophisticated attacks, with the response information available for later analysis.

How Is SES Evolution Different?

The Stormshield solution relies on behavioral analysis with a context-based approach that aims to intercept the techniques that hackers utilize for their cyberattacks. SES Evolution is conceived with a three-protection layer approach to ensure that attacks are blocked and the response information is available to the security teams for further analysis, endpoint security, core protection, and detection and response:

1. Endpoint Security

- Behavioral analysis drawing on techniques used by hackers for advanced attacks (APT) and ransomware: this includes protection against many attack techniques such as buffer overflow, process hollowing, token stealing, and heap spraying, but also more specific detection of ransomware malicious actions
- Adaptive policy according to context and device control rules
- Predefined security policy templates available
- Network firewalling (including WiFi connection)
- Peripheral device management

2. Core Protection

- Self-protection function that includes defensive programming rules to stop changes in applications that try to disable the endpoint protection

3. Detection and Response

- Block the attack thanks to the security mechanisms
- Incident analysis with contextual data
- Incident analysis for first insights on cause of alert
- Attack chart to visualize the attack (process tree)
- Further analysis to take appropriate actions

Benefits

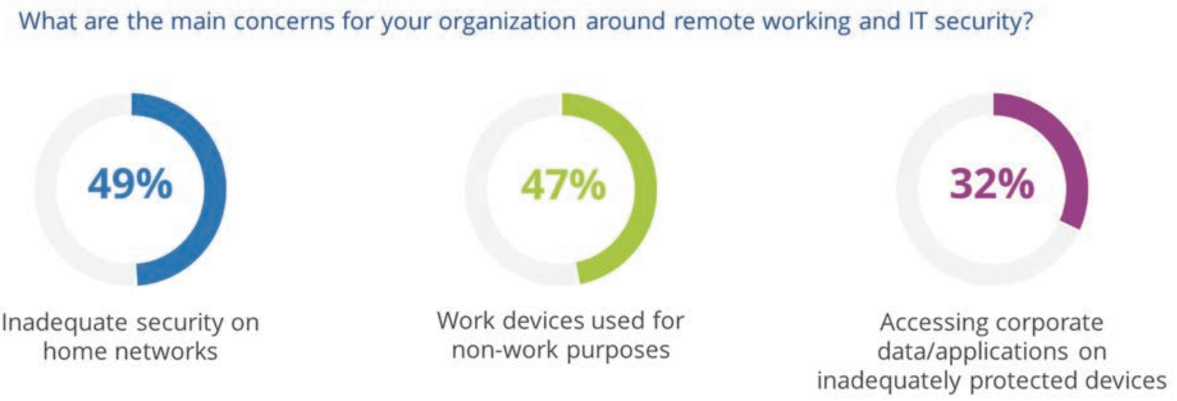
SES Evolution is a standalone protection system that does not need an internet connection to update itself, with its security mechanisms blocking zero-day threats (known and unknown threats) without requiring software updates or adaptations. Because it is context sensitive, it is risk aware, which means it continuously and dynamically adjusts the security level to the workstation's environment. In terms of granularity, SES offers customers the flexibility to choose either to use one plug-and-play security policy from the different templates or to customize to their own more specific needs, tailored to the company's exact requirements. The new remote worker and hybrid work models create a challenge for organizations, IT, and security departments. Employees may be alternating between the office and home with a single device, meaning that endpoint protection configurations must be suitable to the environment from which they access their corporate applications.

SES Evolution's context-aware capabilities mean that it adapts to the level of risk created by the surrounding environment and this varies depending on whether an employee is working from home, travelling, or working in a public space or on the company premises in the corporate network.

This dynamic security policy ensures an optimal level of protection depending on location, a strong concern for European organizations (as highlighted in IDC's 2021 European Security Survey). When asked about the main concerns for their organization around remote working and IT security, 49% cited inadequate security on home networks, 47% had concerns about work devices used by other family members for non-work purposes, and 32% worried about employees accessing corporate data/applications on inadequately protected devices.

FIGURE 4

IT Security Concerns Around Remote Working



Source: IDC 2021 European Security Survey (n = 140)

Other benefits linked to hybrid work model environments include the ability to manage peripherals such as the use of USB sticks to specify what is authorized and what is prohibited and the ability to control connections to any public or unsecure WiFi networks. Authentication and access controls for partners and contractors is the top challenge that organizations face in terms of identity and access, according to the 2021 IDC European Security survey. This is an issue that SES evolution can address by only granting access for non-corporate devices, such as contractors, only if the workstation requesting access is connected to the company VPN. SES can also further increase host security with embedded network protection against FTP bounce attacks when connected to the corporate VPN.

Challenges

Despite the advantages of leveraging endpoint solutions such as SES Evolution, the current focus for many companies is cost optimization and business resilience to withstand a possible recession. However, organizations must also focus on strategic planning as they look to position themselves to compete in the next normal as economic activity accelerates into recovery.

IDC's European Security Survey 2021 found that 24% of organizations saw their 2021 security budgets either frozen or reduced due to COVID-19 and that the number 1 driver for vendor selection was cost effectiveness (cited by 23%). Also, the number 1 attribute that organizations look for in an endpoint security solution is low cost per device — with 51% of respondents selecting this as either very important or important.

Endpoint security solutions will remain a core element of every organization's security infrastructure. However, price pressure, the competitive nature of the market, and the need to secure a diversity of endpoints (different operating systems, use of mobile, Internet of Things, etc.) are also important.

Conclusion

European organizations have long had core endpoint security components deployed as their first line of defense from threats and attacks. However, the evolution of the threat landscape has increased the appetite for more advanced tools that can enable earlier and more preemptive detection of threats and the overall demand for improved detection and response capabilities.

Building more resilience with the pairing of EPP and EDR techniques will help protect against sophisticated cyberattacks by increasing the security level while ensuring optimal protection, as this will prevent the environment from being compromised, limit the attack surface, ensure attacks are being blocked, and make the response information available for analysis by the security teams.

The addition of context-sensitive protection and behavioral analysis capabilities will support endpoint detection and response to help block and mitigate potential damage to their infrastructure. It will also improve operational capabilities in case an attack does manage to penetrate the organization.

Accelerating and improving detection and response capabilities is not just about security, but also about building the resilience of business processes while ensuring service availability. This is why IDC believes organizations will also need to determine for which infrastructure and processes they need to safeguard critical business operations, and that covers everything from desktops and notebooks to servers, applications, and access.

MESSAGE FROM THE SPONSOR

For over 20 years, Stormshield has offered innovative end-to-end security solutions to protect networks (Stormshield Network Security), workstations (Stormshield Endpoint Security), and data (Stormshield Data Security). All around the world, companies, governmental institutions, and defense organizations need to guarantee cybersecurity for their critical infrastructure, their sensitive data, and their operational environments. Certified and qualified at the highest European levels, Stormshield's technological solutions meet the challenges faced by IT and OT to protect their activities. Our mission is to provide cyber-serenity for our clients so they can concentrate on their core activities, something which is vital to the satisfactory operation of our institutions, our economy, and the services provided to our populations. When you choose Stormshield, you are choosing a trusted European cybersecurity provider.

About the Analyst

Romain Fouchereau, Research Manager, European Security, IDC

Romain Fouchereau focuses on network security and the security technologies linked to the extended enterprise such as IoT, edge, and IT/OT convergence. He closely monitors the development, evolution, and penetration of these technologies and the approaches vendors are taking to stimulate adoption at both the channel and end-user levels.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.uk.idc.com

Global Headquarters

140 Kendrick Street,
Building B
Needham,
MA 02494
+1.508.872.8200
www.idc.com

Copyright and Restrictions

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the Custom Solutions information line at 508-988-7610 or permissions@idc.com. Translation and/or localization of this document require an additional license from IDC. For more information on IDC visit www.idc.com. For more information on IDC Custom Solutions, visit http://www.idc.com/prodserv/custom_solutions/index.jsp.