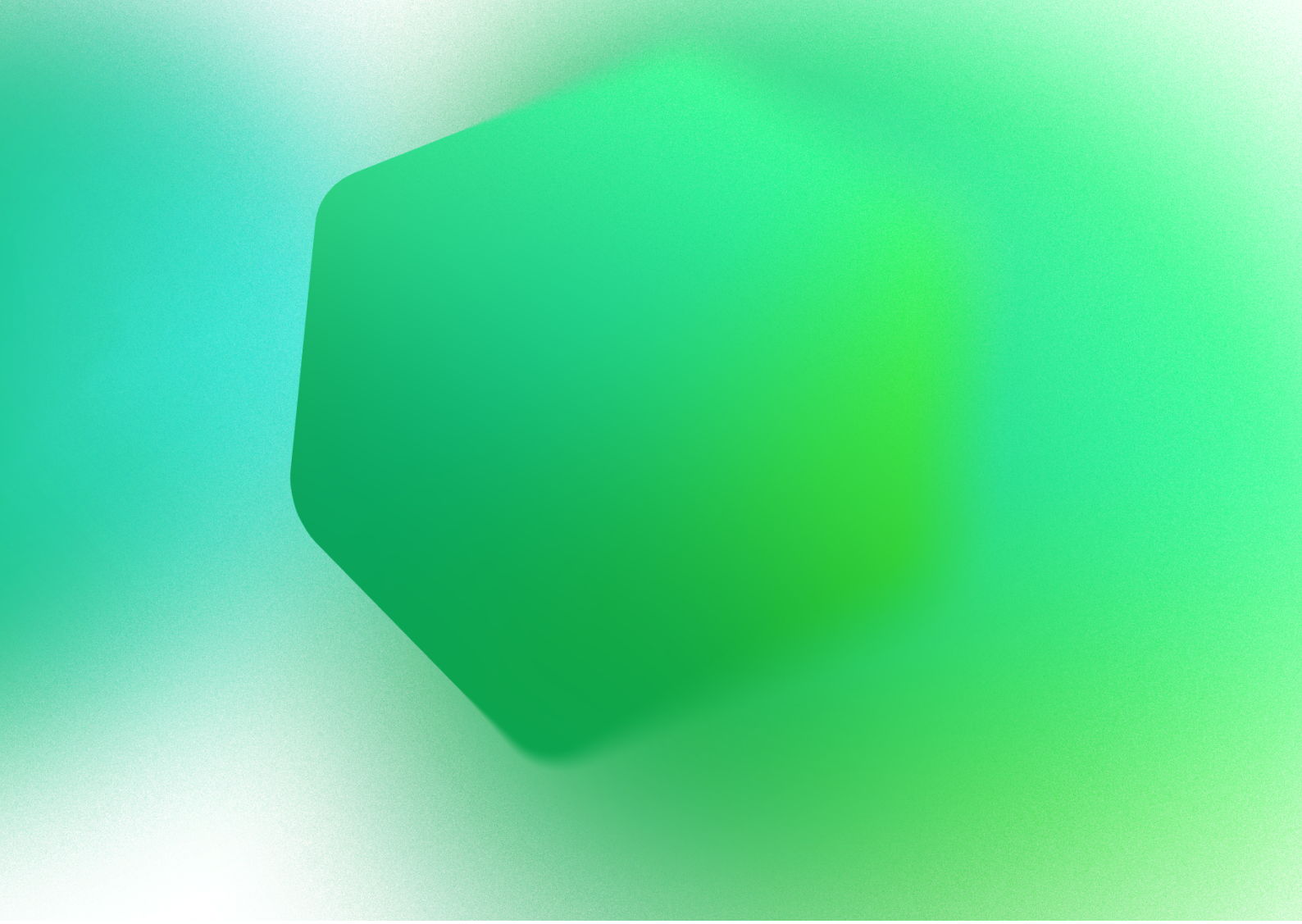


EDR – the case for automation and simplification

kaspersky

Learn more on kaspersky.com
#bringonthefuture

Introduction

Unless you've spent the last couple of years with your head stuck firmly in the sand (and we do appreciate the attractions of this posture) you'll have been bombarded with scaremongering about the escalating volume and complexity of cyberthreats.

It's all true. But it's nothing new. Cybercriminals develop attack mechanisms, vendors develop counter-measures, cybercriminals develop ways or getting around these, we counter these with further technologies and so on. That's just how it works.

At this point, you'll also have heard on all sides that Endpoint Detection and Response (EDR) capabilities are now a necessity rather than a luxury.

This is also true. But, as with all cybersecurity considerations, there's a balance to be found. How likely are you to be attacked by which forms of threat, and how much time, money and resources should you be allocating to addressing what? The answers will differ depending on the nature of your organization, its size and geographical spread, and the resources available to you.

So, is this a good time to invest in EDR if you haven't already done so? The last few weeks and months, with so many organizations reliant on employees working beyond the IT perimeter, and the scope of gateway level protection, has dramatically brought home to us the importance of continous, safe corporate information sharing and communications channels, and our reliance on effective endpoint security. Organizations of every size and type, regardless of their levels of cybersecurity expertise, need to be considering advanced detection, better visibility and an instant response to complex threats.

But you do need to know what you're getting for your money, and what you would do with it.

What is EDR?

Endpoint Detection and Response (EDR) is an element of endpoint protection which provides continuous monitoring for and response to advanced threats on endpoints, as opposed to antivirus (AV) and anti-malware elements which focus primarily on stopping threats in the pre-execution phase. While EDR extends the range of 'classical' EPP, it's not a replacement: to justify your investment in EDR, you need to be sure you already have a good foundation of protection capabilities. If you're looking to 'shore up' less than satisfactory endpoint protection performance by adding EDR, you'd be better advised to focus first on upgrading your core EPP.

All EDR products have the same objective - to more readily identify, investigate and respond to advanced and complex malware threats. The toolset used to achieve this will include most if not all of the following:

- A detection engine, using techniques such as machine learning-based structure analysis and emulative sandboxing to detect and prevent malware specimens.
- A real-time analytics engine, monitoring memory and searching for patterns in behavior, thus enabling detection of exploits and rapid diagnosis of most complex and previously unknown threats.
- Applied threat intelligence, which may come from a number of separate sources.
- Visibility throughout endpoints – this is critical to detecting malicious activities.
- Real-time event data monitoring and recording, and its collection for use in analytics.
- Forensic tools to investigate past breaches and to hunt out threats which might be lurking unidentified on an endpoint
- Incident response - the generation of automatic alerts and responses.
- Incident filtering to prevent 'false positives' - an overload of unnecessary alerts.

Not all EDR tools work in the same way. Some might perform more analysis on the agent, while others focus on the backend via a management console. The timing and scope of data collection may vary, as may the quality and sources of threat intelligence. And not every tool on offer may be relevant to your own cybersecurity operations. Threat hunting, for example, requires resources and specific expertise that the majority of IT Departments can't command.

So, rather than evaluating every EDR solution against every capability it boasts, it's important to identify and focus on what you actually need to do the job. There's no point in paying for functionality you won't use and which adds unnecessary complexity. Look for a product that you can rely on to perform effectively for you, without increasing your overheads or workload and which will integrate fully with the rest of your EPP estate.

The term Endpoint Threat Detection and Response (ETDR) was coined in 2013 by Gartner's Anton Chuvakin, and defined as "the tools primarily focused on detecting and investigating suspicious activities (and traces of) other problems on hosts/endpoints." The word 'Threat' was later dropped, and ETDR became EDR.

"A weak EPP[1] solution will destroy e value of an EDR tool"

IDC, Endpoint Security 2020: The Resurgence of EPP and the Manifest Destiny of EDR, Doc # US45794219, 2020

1 EPP – Endpoint Protection Platform

What threats does EDR combat, and how?

Indicators of Compromise (IoCs)
An IoC is a piece of forensic data that identifies potentially malicious activity on a system or network, and which can act as a breadcrumb leading to the detection of malicious activity early on in the attack sequence.

Cyberthreats in general are best addressed through a multi-layered approach, using a series of filters to address ever more evasive forms of threat.

As the threat enters the host, an endpoint protection engine will use an assortment of approaches, such as structural ML models, behavior analysis and other complex detection techniques, to identify and neutralise the vast majority of what remains.

Having filtered out most malware through these straightforward and highly automated processes, resources can be concentrated on the very small fraction that's left. These still-undetected threats include complex, evasive and advanced attacks, which can of course be the most deadly and destructive of all.

And this is where EDR comes in.

One of the main tasks of EDR is providing **visibility** - helping your team to see what's actually happening on your endpoints. Quick access to incident data, enriched information and scanning for Incidents of Compromise (IoCs) are all essential elements in monitoring security on endpoints.

Another key component of EDR activity is **investigation.** Even if EPP has reacted to - for example - a file drop, or to process injection into a legitimate process (a malwareless attack), this doesn't always mean the threat has been dealt with, especially in more complex attacks. Understanding the root cause of a threat means not allowing any leftover components to go unnoticed. For example, simply deleting a malicious file might still leave the hacker connected to the host via other means, and killing a single process may not prevent re-infection if the root cause hasn't been identified and dealt with.

Finally, many of today's threats develop very quickly, and the consequences of failing to detect a threat's components swiftly could be devastating (ransomware is just one example). So a **quick and preferably automated response** is crucial - not just detecting and understanding the threat, but also neutralizing it.

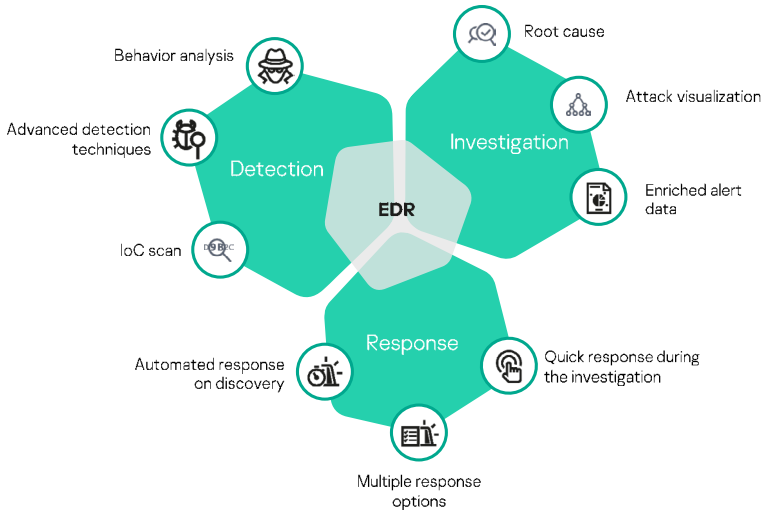


Figure 1. Main EDR capabilities

A note on resources

Global IT security skills shortages have now surpassed four million, according to (ISC)[2].

Cybersecurity workforce study, 2019, (ISC)[2]

Any EDR solution has to fit with the resources you can realistically allocate to its deployment and maintenance. Finding the budget for hardware and software is one thing: finding the right skilled staff is another.

IT security personnel recruitment is at crisis levels. At the time of writing, the number of unfilled positions globally stands at 4.07 million, up from 2.93 million this time last year. So if you don't currently have a full complement of security specialists, it's no good banking on being able to attract more. You're going to need to find another way.

How far can EDR be automated and simplified?

One of the most effective ways of delivering EDR with limited resources is through automating processes wherever this can be done safely, and simplifying those processes where automation is inappropriate or impractical. Automation saves time, resources and money - and, as machines are less error-prone than people, it will actually increase the effectiveness of your security. The simpler your EDR solution is to operate by your hard-pressed team, the more swiftly and accurately they'll be able to work. For those fortunate enough to have skilled IT security professionals on board, automation and simplification will free these specialists up from tedious manual tasks, so they can devote more of their expensive time on the really challenging and rewarding aspects of the job.

Which EDR processes can be automated effectively, and how can manual processes be simplified?

Pre-filtering

First and foremost, your Endpoint Protection solution needs to be fully effective in pre-filtering incidents before EDR comes into play. The earlier in the attack kill chain the vast majority of threats can be identified and countered automatically, the less the overall impact on resources. Most security incidents can be seen off right away by a good EPP solution, leaving your EDR solution and your security staff free to focus on the more advanced, and therefore the more dangerous, threats. We know we keep saying this, but – make sure your EPP solution is pulling its weight.

Simplifying incident analysis

Root cause analysis, or RCA, is simply the process of working out what's happened, in order to identify the culprit, ensure that the incident has been dealt with comprehensively, and ensure that it can't happen again.

Visibility into what's happening is also key. An automatically generated and clear visual representation of each stage of the progress of the incident (which itself may involve more elements - including components already buried inside your system - than EPP has detected at this point) can then provide all the data needed for investigation.

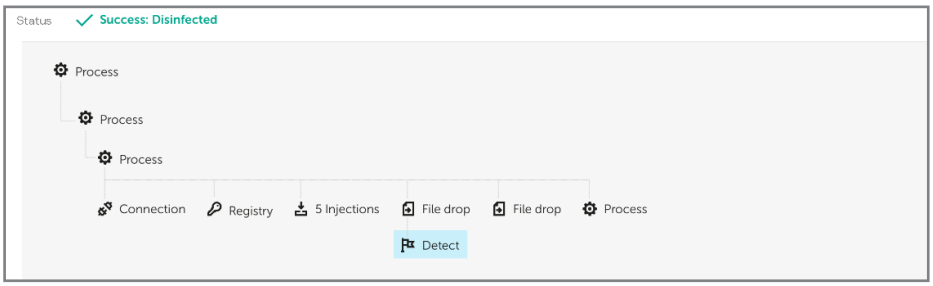


Figure 2. A way to visualize the path the threat has taken and what connections are present

The second step is the automated generation of a single alert card, bringing all the information needed into one place in order to simplify and speed up the investigation process. This information should include full details and context of the incident: when exactly and on which host it occurred, what user accounts have been used and various details on the file, process, registry key change or connection associated with it.

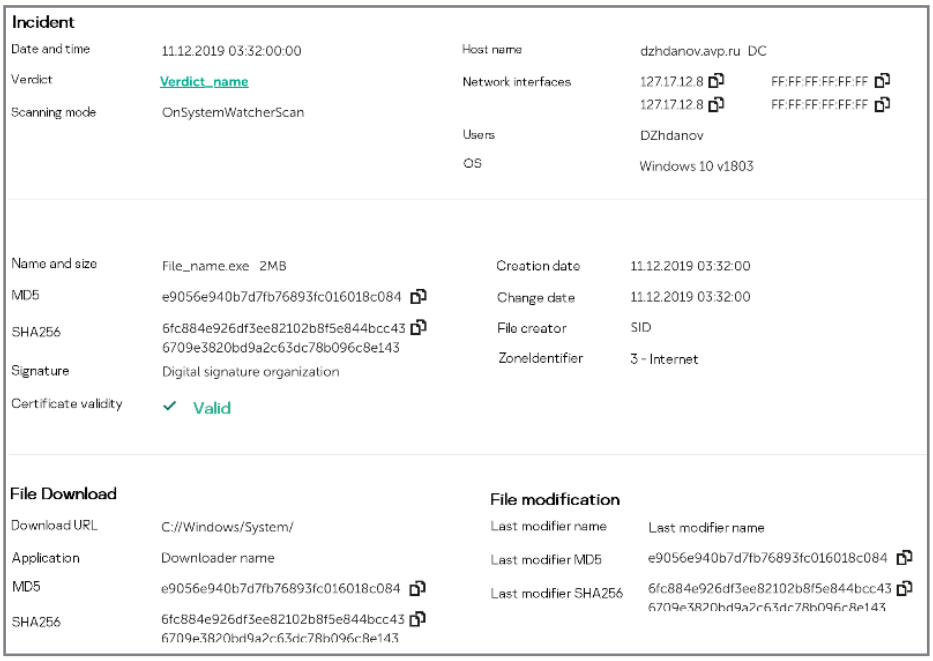


Figure 3. What an alert card with necessary information might look like

History & connections

Details & context

True scope revealed

Use case

Clicking on an alert, the security officer opens the alert card and sees all the necessary information, starting from file and host data and the detections made and response actions performed by different detection layers, to drill-down visualization of how different events on the host are connected. With this data, all in a single place, it's much easier to investigate the alert and understand if there are any threat components still active or dormant in the system, and if the threat's scope is larger than at first imagined. That way, the security officer can make sure that no remnants of the attack are still present in the system.

Straighforward IoC generation and automated scanning

Import or generate IoC

Set up scan on schedule

Find traces of a threat

Root Cause Analysis of an incident may well result in the generation of an Indicator of Compromise (IoC) based on activities associated with the detected threat. Scanning for IoCs is, as we have said, an important defensive mechanism within EDR, allowing you to understand what other hosts might have been compromised or where signs of a threat are present. Known IoCs (for example, provided to you by your regulatory authority or gathered from a specific newsletter or mailing list) can be imported into the solution as an automated process, and regular automated scanning for both newly generated and imported IoCs is essential to maintaining system health. Scanning for IoCs generated from an analyzed threat on a regular basis is valuable because it's very possible that the same threat will resurface in the future. And if you know that a specific attack is happening to organizations like yours and the IoCs are available, regular scans for these imported IoCs will help you find and respond to that threat in the shortest possible time.

Use case

Intelligence reaches you of an attack happening in your specific industry, and means you need to look for specific IoCs. Rather than do this manually, you simply import these IoCs and set up a scheduled scan.

Automated response

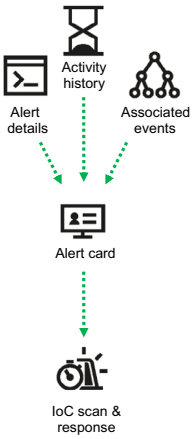
EDR solutions need to be able generate a swift, automated response, which can be handled effectively in one of two ways: through automation (when, for example, an IoC scan has been run and threats found, requiring an immediate response) or directly from the alert card if, for example, the security officer needs to isolate the host during analysis.

Response options may include preventing a file from executing (e.g. create a rule to block a file with a specific hash to be run on hosts), isolating the infected host, removing a file, and automatically scanning other hosts for signs of infection using EPP.

Use case

During an investigation, the security officer comes to the conclusion that a particular file or application (for example, a legitimate RAT (remote administration tool) of unclear origin) is a cyberattack component capable of many potentially malicious activities. Circumstances (the tool was detected on a machine where sensitive data is handled) dictate that the host should be immediately isolated as a precaution, until the incident is fully analyzed and the attack dealt with in full.

This done, the officer can initiate an IoC scan to find similar files across all endpoints, and set up an automated response (such as removing the file or, as a more drastic measure, isolating the host from the network pending further investigation) – ensuring an instant response to the threat on its discovery in the network.



Keeping it all together

Switching between multiple tools wastes valuable time as well as introducing opportunities for mistakes through compromised visibility. Your staff need to be able to conduct investigations and root cause analyses, respond to threats, and see everything that's going on clearly through a single console. If your core EPP solution uses the same console and agent – even better.

Use case

On discovering a suspicious or malicious activity, you don't have to go to several tools or the endpoint itself to analyze logs, associated events, EPP and EDR activity history, or to perform IoC scans or response actions with yet another tool. You can do all of this within a single console.

Results of effective EDR implementation incorporating automation

Process automation and simplification will save you time and resources – and it also makes for better security. You can expect:

- No lethal 'leftovers' from attacks – eliminating any ambiguity about whether a threat could still be present in your network.
- A faster Mean Time to Respond (MTTR) for incidents – a crucial metric for some attacks, ransomware being just one example
- Incidents that are dealt with promptly in every case – high levels of automation mean nothing gets sidelined or passed over because 'alert fatigue' has kicked in.
- More attention being given to those incidents actually requiring human intervention, aided by increased visibility and enriched incident data
- Not having to invest in additional training or dedicated highly skilled security specialists in order to manage your EDR solution on a day-to-day basis – these should be able to step in only as needed.
- A happier team who, freed from routine tasks and equipped with a simple EDR toolkit, work better and are less vulnerable to poaching.

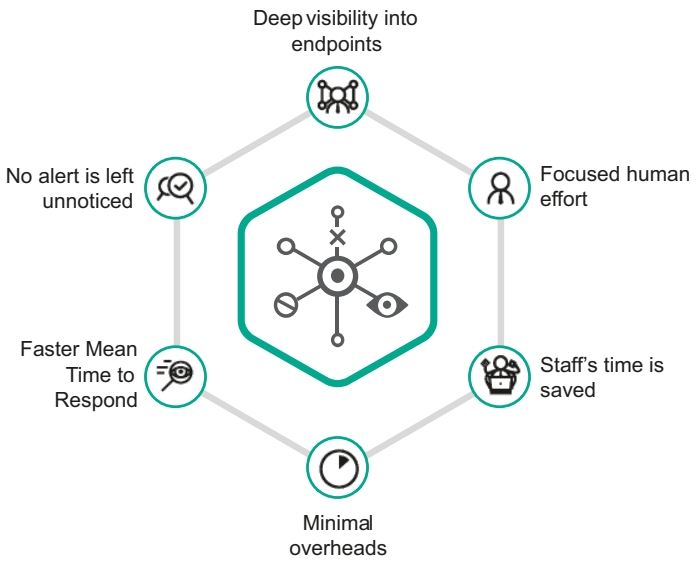


Figure 4. Main results of effective EDR implementation

Introducing Kaspersky Endpoint Detection and Response Optimum

Based on all of these concepts, we at Kaspersky have created our new EDR product – Kaspersky Endpoint Detection and Response (EDR) Optimum.

Kaspersky EDR Optimum helps you build true defense-in-depth against complex contemporary threats, without any additional overheads.

Combining an easy-to-use, highly automated detection and response toolkit with the unequalled endpoint protection and advanced detection capabilities of Kaspersky Endpoint Security for Business in a single unified offering provides highly effective and efficient security for your endpoints.

A streamlined workflow, no additional overheads and automation features all mean that incidents are dealt with swiftly and efficiently, while saving your cybersecurity staff time and hassle.

What's next?

No two organizations are the same, so we urge you to take a serious look at what EDR capabilities are actually required for your specific business.

Do you want better threat detection and response capabilities – while also minimizing hassle for your overworked staff with a simple and automated tool? In that case, **Kaspersky Endpoint Detection and Response Optimum** might be right up your alley.

Or do you need enhanced threat discovery, proactive threat hunting and centralized incident response capabilities, arming your team of experts to fight the most complex and dangerous targeted attacks? Then you might want to look into **Kaspersky Endpoint Detection and Response**, perhaps as a part of **Kaspersky Anti-Targeted Attack Platform**.

Or maybe you want to make sure your organization is protected 24/7, while keeping your staff and resources free for other tasks? **Kaspersky Managed Detection and Response** answers that need perfectly.

If you have any questions on how Kaspersky can help your business stay safe, please visit **https://kaspersky.com/enterprise-security/**.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com/

www.kaspersky.com

kaspersky BRING ON THE FUTURE