kaspersky BRING ON THE FUTURE

Kaspersky Endpoint Detection and Response Optimum

Take your endpoint defenses to the next level and tackle evasive threats head-on – with no hassle.

It's time to step up a level. You're ready not just to protect your organization with mainstream anti-malware technologies, but to identify, analyze and effectively neutralize those threats deliberately designed to evade traditional protection, and to bury themselves deep in your systems, ready to do their worst.

Legitimate system tools are used in about **30% of successful attacks** to launch scripts and programs, download payloads, scan networks or get remote access to the infected host.
Incident response analyst report, Kaspersky, 2020

The challenges

Worse disruption

Malware, ransomware, financial spyware and other threats are becoming smarter at evading detection, and attacks are becoming cheaper to mount. So the risk of a serious attack is greater than ever, as are the levels of damage and disruption involved.

Complex infrastructures

Today, the vast majority of IT managers and security professionals have to protect a whole range of different endpoints – laptops, servers, virtual and cloud environments and remote workstations – while coping with barely manageable levels of IT complexity

Finding a balance

Cybersecurity is for the most part about finding the optimal balance between your available resources and the highest level of protection that's realistically achievable. And your IT specialist's time is one of the scarcest resources of all.

The answer

Kaspersky Endpoint Detection and Response (EDR) Optimum helps you identify, analyze and neutralize evasive threats by providing easy-to-use advanced detection, simplified investigation and automated response.

Even in successful attacks, financial losses were **32% lower** if a breach was responded to rapidly.
Incident response analyst report, Kaspersky, 2020

Fully armed and prepared

Based on advanced detection mechanisms, including machine learning and enhanced behavior analysis, Kaspersky EDR Optimum gives you deep visibility into threats, straightforward analysis and investigation tools and automated response. You'll be able to see the threat, understand it, reveal its full scope and instantly respond, preventing business disruption.

A single solution

Kaspersky EDR Optimum brings advanced detection, analysis and response capabilities to the Kaspersky security ecosystem, enhancing defenses across a whole spectrum of endpoints, including laptops, servers, cloud workloads and virtual environments. Centralized deployment and unified management of Kaspersky EDR Optimum are available from the cloud or on-premise.

Simple and efficient

Kaspersky EDR Optimum is built for smaller cybersecurity teams with limited resources who are looking to upgrade their incident response capabilities. Performance is optimized for maximum efficiency and minimum human input, making the most of your security specialists' time with automation and centralization of all administration and streamlining workflows.

Key benefits

- Protect yourself against more frequent and more disruptive evasive threats
- Defend every endpoint: laptops, servers, cloud workloads
- See the full scope of any threat over the whole network
- Understand the root cause of the threat and how it actually occurred
- Avoid further damage with rapid automated response
- Save time and resources with a simple and automated tool

Crucial EDR use cases

Advanced detection

Advanced detection is necessary to discover evasive threats:

- Behavior Threat detection and Exploit prevention powered by machine learning (ML)
- Heuristics, smart records, ML-based technologies
- Built-in Emulator for pre-execution detection of malicious behavior
- Sandbox for enhanced behavior analysis (available with Kaspersky Sandbox)
- Global threat intelligence data collected and analyzed in-lab by AI-based systems and experts

Answer vital questions

Evasive threats often hide in plain sight and should be investigated to be fully eradicated. EDR helps by finding answers to these questions:

- Am I under attack right now?
- Has this industry-wide attack reached my infrastructure?
- Where did this threat come from?
- What has it managed to do on my hosts?
- Are there any hidden layers to this threat?
- Are other endpoints affected?

Respond rapidly

Respond to threats with a single click or with an automated response as soon as they're discovered:

- Prevent the malicious file from running and spreading throughout the network during or after your investigation
- Automatically quarantine files associated with evasive threats on all endpoints
- Automatically isolate infected hosts on finding an Indicator of Compromise (IoC) associated with a fast- spreading threat

Now you can do so much more

Now you can understand the full scope of any threat attacking you and how it's developed on your endpoints, taking advantage of advanced machine learning-based detection and visibility into detects. And you can ensure that each threat has been fully dealt with — nothing's still burrowing away somewhere inside your system, working out how much harm it can do.

Defend hybrid infrastructures

Hybrid infrastructures bring unique security challenges as well as significant benefits. Now you can enhance your data and infrastructure protection for virtual and physical servers, VDI deployments and public cloud workloads with essential EDR functionality.

Avoid alert fatigue and make full use of your resources with centralized management across all your hybrid endpoints and workloads and streamlined EDR workflow from the cloud or on-premise.

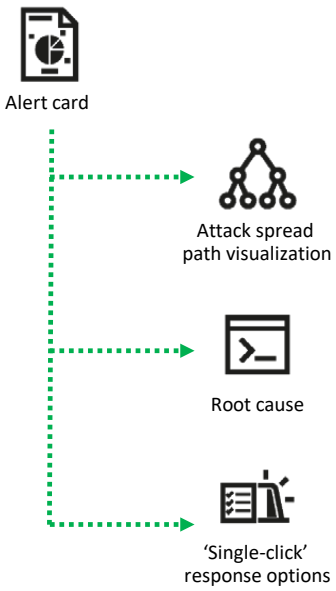
Multiple-level endpoint protection

EDR technologies don't exist in a vacuum – they can only function effectively from a solid base of strong endpoint protection. Multiple-level endpoint protection ensures that you're not distracted by handling commodity threats and incidents which should already have been dealt with by automated anti-malware software. That's why Kaspersky EDR Optimum operates in conjunction with one of our our most tested, most awarded[1] endpoint protection platforms: Kaspersky Endpoint Security for Business and Kaspersky Hybrid Cloud Security.

Analyze threats

In a single incident card, enriched data on the detect and a drill-down attack spread-path are gathered to perform quick analysis and make informed decisions for a 'single-click' or automated response.

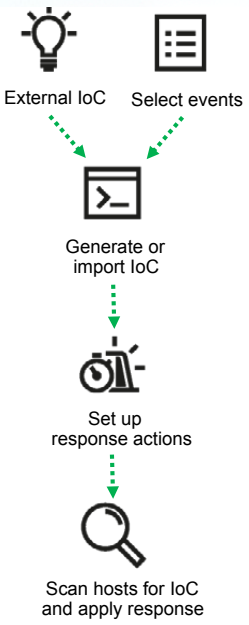
IoCs can be imported from trusted sources or generated based on the investigation in order to discover evasive threats lurking on endpoints across your infrastructure.



Automate your response

Instantly respond to threats during the investigation with 'single-click' options available in the incident card or set up automated responses upon discovery based on IoC scans. Response actions include:

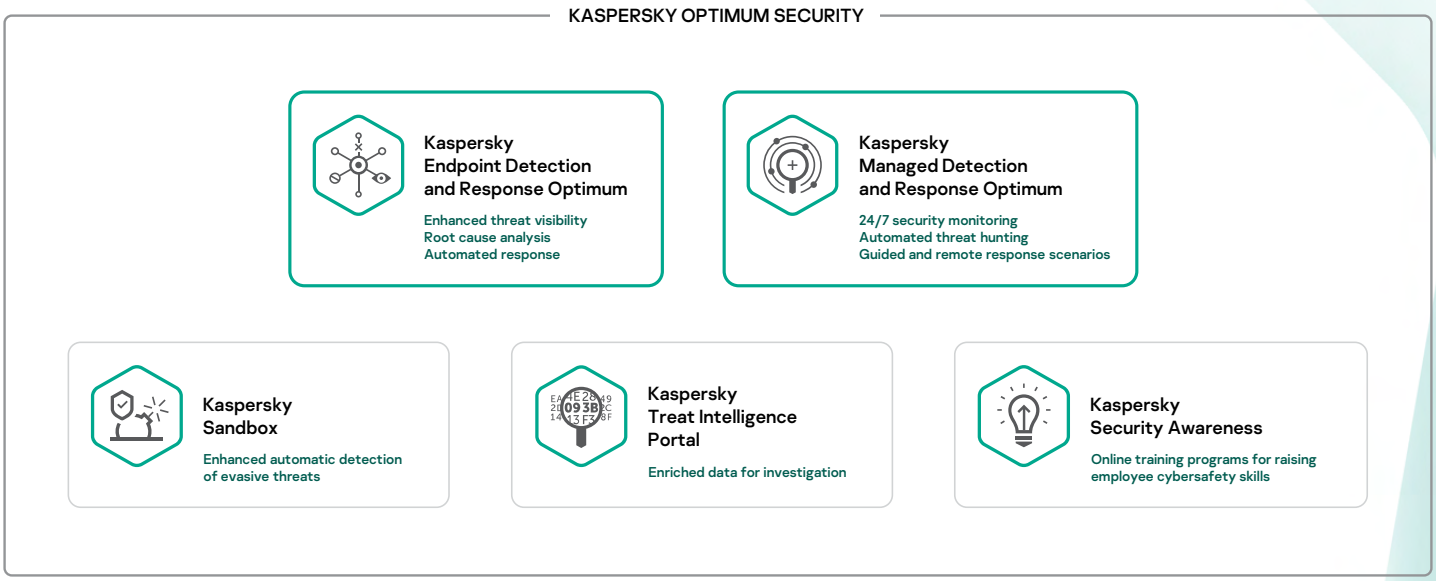
- Isolate host
- Quarantine file
- Prevent execution
- Launch critical areas scan



[1] https://www.kaspersky.co.uk/top3

Your Kaspersky Optimum Security platform

EDR is part of an ecosystem spanning multiple technologies, tools and services: Kaspersky EDR Optimum is they key component of Kaspersky Optimum Security, a wider solution strengthening multiple aspects of your defenses against evasive threats, while being easy on your resources:



A stage-by-stage approach

Kaspersky Optimum Security builds on Kaspersky Security Foundations. If and when you're ready to do so, you can choose to grow smoothly into the application of powerful tools that protect against the most advanced threats, with Kaspersky Expert Security.

Kaspersky Security Foundations

Automatically block the vast majority of threats.

- Multi-vector automated prevention of incidents caused by commodity threats – the vast majority of all cyberattacks
- The foundation stage for organizations of any size and complexity in building an integrated defense strategy
- Reliable endpoint protection for those with small IT teams and emerging security expertise

Kaspersky Optimum Security

Build up your defenses against evasive threats. Ideal for businesses with:

- Have a small IT security team with basic cybersecurity expertise
- An IT environment growing in size and complexity, increasing the attack surface
- A a lack of cybersecurity resources – in contrast to a need for enhanced protection
- A growing need to develop an incident response capability

Kaspersky Expert Security

Readiness for complex and APT-like attacks. For businesses with:

- Complex and distributed IT environments
- A mature IT security team, or an established Security Operations Center (SOC)
- A low appetite for risk due to higher costs of security incidents and data breaches
- And where regulatory compliance is a concern

To find out more about how Kaspersky Endpoint Detection and Response Optimum addresses cyberthreats while going easy on your security team and resources, visit http://www.kaspersky.com/enterprise-security/edr-security-software-solution.

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

www.kaspersky.com