kaspersky BRING ON THE FUTURE

Kaspersky Endpoint Detection and Response Optimum

Build true defense-in-depth with instant automated response and simple root cause analysis

The problem

91% of all organizations were affected by cyberattacks over the course of 2019, with **1 in 10** facing a targeted attack[1].

Complex threats bring disruption

The days of simplistic malware are long gone and threats have become much more complicated, bringing more disruption and greater losses to businesses, while staying undetected for longer

You are being attacked

These complex threats have become much cheaper and more frequent, so organizations who believed they were under the radar, now have to cover their backs.

Efficiency is imperative

Adding fuel to the fire is the lack of resources that organizations are now facing, Including two of the most valuable – time and skilled personnel.

How we help

«A weak EPP solution will destroy the value of an EDR tool»[2]

«People and time thus become the new ROI metric for EDR tool»[2]

Kaspersky Endpoint Detection and Response (EDR) Optimum helps you stay safe in the face of complex and advanced threats by providing advanced detection, simplified investigation and automated response.

Beyond essential capabilities

Provides deep visibility, simple investigation tools and automated response options in order to not just detect the threat, but to reveal its full scope and origins and instantly respond, preventing business disruption.

True defense-in-depth

Brings an easy-to-use, highly automated detection and response toolkit together with the unequalled endpoint protection capabilities and advanced detection of Kaspersky Endpoint Security for Business, forming a single unified solution.

Intelligent tool assures efficiency

Frees up your time and optimizes manpower resources and IT overheads by providing simple centralized controls and a high level of automation. A streamlined workflow from a single console available both on-premises and in cloud[3].

Key benefits

- Protect yourself against more frequent and more disruptive advanced and complex threats
- Save time and resources with a simple and automated tool
- See the full scope of complex threats over the whole network
- Understand the root cause of the threat and how it actually occured
- Avoid further damage with rapid automated response

Crucial EDR use cases

Answer important questions

- What's the context of the alert?
- What actions have been performed on the alert already?
- Is the detected threat still active?
- Are other hosts under attack?
- What path did the attack take?
- What's the true root cause of the threat?

Learn the full scope of the threat

Once you learn you're at risk of a global threat - e.g. regulatory authority asks you to run a scan for a specific indicator of compromise (IoC) - you can:

- Import IoCs from trusted sources and run periodic scans for signs of an attack
- Investigate an alert thoroughly, generate IoCs based on discovered threats and run scans throughout the entire network to find out if other hosts have been affected

Respond instantly to prolific threats

- Automatically quarantine files associated with complex threats on all endpoints
- Automatically isolate infected hosts on finding an IoC associated with a fast- spreading threat
- Prevent the malicious file from running and spreading throughout the network during your investigation

[1] The Kaspersky Global IT Risk Report, Kaspersky, 2019

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

[3] There are some restrictions to the range of features and functionality that can be managed via the cloud console. For full information, please visit https://kas.pr/epp-management-options

Now you can:

See the full scope of the threat

See security alerts on your endpoints and analyze them further to understand the full breadth and depth of the threat. This helps ensure the incidents are fully dealt with and no remainder of the threat is left on the endpoint.

Simplify your workflow

Streamlined workflow from a single console available both on-prem and in cloud is coupled with simple EDR scenarios and controls, including drill-down visualization, IoC scanning and response options that don't require too much cybersecurity expertise or time.

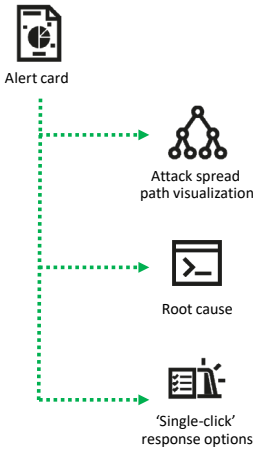
Give your defenses a boost

The further addition of Kaspersky Sandbox creates a complete Integrated Endpoint Security solution delivering simple, effective and highly automated multi-layered defenses against commodity, complex and evasive threats.

Analyze enriched alert data

Kaspersky EDR Optimum enriches incidents with necessary information and helps you understand connections between different events through attack spread path visualization.

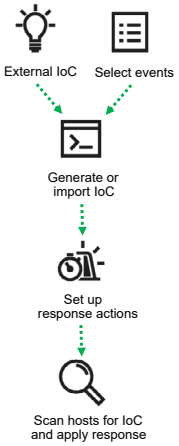
Visibility is provided across all hosts on the network by scanning for imported or generated Indicators of Compromise (IoCs).



Respond automatically

Set up automated responses for threats discovered across all endpoints based on IoC scans, or instantly respond to incidents upon discovery with 'single-click' options.

Response options include: isolate host, quarantine file, launch scan of the host and prevent file from executing.



Further EDR Options

Kaspersky Endpoint Detection and Response Optimum is one of number of EDR options we offer, each tailored to specific customer needs. You may also wish to consider:

Kaspersky Endpoint Detection and Response

Industry and customer acclaimed expert EDR solution perfect for IT organizations with mature IT security teams, which helps to get to the bottom of the most sophisticated advanced and targeted attacks. Provides enhanced threat discovery, powerful investigation, proactive threat hunting and centralized incident response.
https://www.kaspersky.com/enterprise-security/endpoint-detection-response-edr

Kaspersky Managed Detection and Response

A fully managed and individually tailored round-the-clock detection, prioritization, investigation and response - backed by over 20 years of consistently outstanding threat research - allows you to gain all the major benefits from having your own security operations center without having to actually establish one.
https://www.kaspersky.com/enterprise-security/managed-detection-and-response

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
IT Security for Enterprise: kaspersky.com/enterprise
Threat Intelligence Portal: opentip.kaspersky.com

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. This is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tomorrow.

Proven.
Transparent.
Independent.