kaspersky BRING ON THE FUTURE

Kaspersky EDR Optimum

Reducing the risk of your organization falling victim to targeted and advanced threats has become a necessity rather than a luxury. We're out to make this process simple and cost-effective, while keeping everybody safe.

Kaspersky Endpoint Detection and Response (EDR) Optimum is a centralized automated tool that addresses advanced and targeted attacks in ways that make it easy on both your staff and your IT resources.

Highlights

- Reduces your risk of falling victim to an advanced or targeted attack
- Provides deep visibility into your endpoints
- Detects complex threats
- Gives your IT security team tools and information for root cause analysis
- Allows the creation and import of IoCs and scanning hosts for them
- Provides varied automated and 'single click' response options
- Undemanding and time efficient
- Highly automated, but allows for human input and expertise

Issues that organizations are now facing

Advanced threats have become commonplace

Targeted and advanced attacks have become much cheaper and easier to undertake, which means it's no longer just nation states and huge enterprises who are in danger. Organizations who believed they were under the radar in terms of these attacks, now have to cover their backs and search out adequate protection - **91%**[1] of organizations have been affected by cyberattacks over the course of a single year, with **1 in 10**[1] facing a targeted attack.

The average cost of an attack is rising year on year

Targeted and advanced attacks cost real money. Currently, the average cost of a data breach stands at approximately **$1.41M**[2], and that of an endpoint malware infection in an enterprise organization is around **$2.73M**[2]. These costs include investigation, remediation, compensation payments, PR campaigns and all the other things needed to mitigate the consequences of an attack.

Employing appropriate tools and expertise in order to prevent these threats costs a fraction of this.

Organizations have limited resources

The number of trained information security professionals you can hire and the amount of time they can devote to a specific task is not limitless. This isn't a new problem, but it's not going away on its own. Automating security tasks is one of the most effective ways to address this issue. Currently, **2 out of 3**[3] organizations are suffering from a lack of information security personnel; and it's projected that by 2021 **3.5 million**[4] cybersecurity jobs will be left unfilled.

Then there are the IT resources required to run security solutions. Corporate IT budgets are often spread thin enough as it is. The answer has to lie in lightweight solutions, or those with minimal IT overheads.

How we help

Kaspersky EDR Optimum was developed to address the need for high-quality security against complex modern-day threats, in the face of limited resources. It's designed to be robust in detecting threats, proactive in responding to them, and practical in terms of day-to-day operations.

1 – The Kaspersky Lab Global IT Risk Report, Kaspersky, 2019

2 – IT security economics in 2019, Kaspersky, 2019

3 – Cybersecurity workforce study, (ISC)^2, 2019

4 – Official Annual Cybersecurity Jobs Report, Cybersecurity Venture, 2019

Robust

The first step in protecting yourself against an attack is being aware of the threat, so robust detection and investigation are the cornerstone of any EDR solution."

Kaspersky EDR Optimum employs a varied set of techniques, capable of detecting any trace of an attack, including but not limited to:

- Malwareless attacks
- Lateral movement
- Suspicious behavior
- and others

Proactive

Detecting a threat is not enough - you have to be able to deal with it in a timely manner, both on the infected host and on other hosts in the network. Kaspersky EDR Optimum provides various ways you can respond to arising threats:

- Isolate host
- Launch scan of the host
- Remove (quarantine) file
- Kill process
- Prevent process from executing

Practical

How much time and effort your security team spends on analyzing and responding to threats is just as important as detection rates and response techniques. With Kaspersky EDR Optimum you don't need exceptional expertise, a large team or the whole day to stay protected. It provides detailed data, it's highly automated and it's easy on your IT resources. All this gives you strong:

Visibility

- Full information on incidents
- Kill-chain visualization
- Incident history and root cause analysis

Automation

- Single-click response options
- Automated creation of IoCs from an incident (or import)
- Search hosts for IoCs and automatically respond to threats

Performance

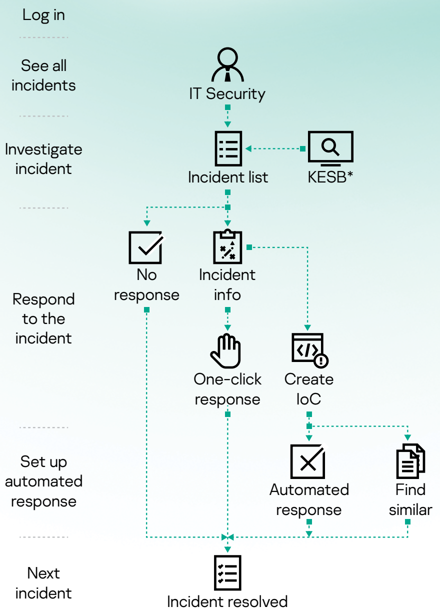
- No additional overheads
- Integrated with Kaspersky Endpoint Security
- Controlled from the Kaspersky Security Center console

Use cases

Here are just a few simple cases where Kaspersky EDR Optimum can be used to detect, investigate and respond to various threats.

Detect	Investigate	Respond
Malicious file detected and shown in the events list	Kill chain visualization shows this file was dropped by an unsigned process	Prevent process from executing with a single click, quarantine the dropped file
Process injection detected	Full information on the incident shows host info, file creation and modification date, author and signature, etc. Based on this information and the kill chain, the file is considered suspicious	Isolate this host and search for similar incidents on other hosts in the network
Suspicious connection detected	Incident data reveals the address the connection was established with. Kill chain visualization associates this connection to a registry key change, both of which were initiated by the same process	Isolate this host. Create IoC for periodic search on other hosts and set up automated response: quarantine file and launch scan on host

How it works



*Kaspersky Endpoint Security for Business

Kaspersky EDR Optimum adds enhanced visibility, root cause analysis capacity and automated response to existing strong EPP (Kaspersky Endpoint Security for Business), while utilizing the same agent.

Data is gathered and analyzed from these hosts, and reporting, detailed incident information and response options on the incidents are provided via the Kaspersky Security Center console.

Response to incidents can be either automated or 'single click'. Automated response is set up in order to respond to similar incidents on many hosts without human involvement, and is triggered after a self-created or imported IoC has been detected on those hosts.

We've made Kaspersky EDR Optimum as simple to operate as possible. After deployment, your IT security staff only need to check the console once in a while, to process the incidents arising, perform root cause analysis and respond to incidents.

This high level of automation and visibility eliminates the need for the security officer to go through massive amounts of data each day. Instead, it helps them focus their attention on suspicious activities, giving them all the information they need.

To find out more about how Kaspersky EDR 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 SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise

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. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tomorrow.

Know more at kaspersky.com/transparency

Proven.
Transparent.
Independent.