Kaspersky Endpoint Detection and Response Optimum

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

kaspersky 25 years

Kaspersky Endpoint Detection and Response Optimum

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

The challenges

Threats evading detection

Evasive malware, ransomware, spyware and other threats are getting smarter at avoiding traditional detection mechanisms – by using legitimate system tools and other advanced techniques to attack.

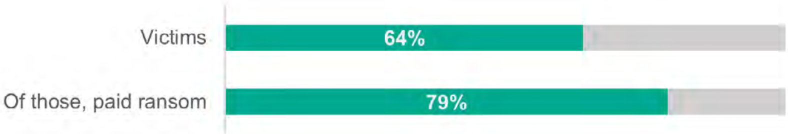
Ransomware-as-a-Service

Hackers can buy ready-built tools on the cheap and attack anyone – stealing data, damaging your infrastructure and demanding ever-growing amounts of ransom.

Limited resources

Infrastructures are becoming ever-more complex and wide-spread, while resources – time, money and attention spans – are falling short. There's no place here for shelfware.

> **64% of organizations have already been victims of ransomware attacks. Of these, 79% have paid the ransom to their attackers.**
>
> **Kaspersky, May 2022**



> **"We value Kaspersky's comprehensive solutions, reliability and prompt service and support. They are guaranteeing the availability of our IT environment."**
>
> **Marcelo Mendes CISO, NEO**
> **read case study**

How we help

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.

Advanced protection

Our advanced detection mechanisms include technologies like machine learning, behavior analysis and cloud sandboxing.

Simple visual analysis tools mean you can fully understand the threat and its scope – and quick response actions stop the attack in its tracks, before any damage is done..

One solution

Next-gen endpoint security is brought together with simple-to-use EDR for the enhanced protection of laptops, workstations, servers, cloud workloads and virtual envrionments.

All this deployment and management happens in one place, through a single cloud or on-premise console.

Simple and efficient

We've built EDR Optimum with smaller cybersecurity teams in mind – for those who are looking to upgrade their incident response capabilities and develop expertise, but don't have that much time to spare.

We automate and optimize most tasks, so you have more time to spend on the really important stuff.

Key benefits

- **Prevent multiple types** of threats
- **Protect your systems and data** against evasive threats
- **Catch current threats** before they act
- **Recognize evasive threats** across your endpoints
- **Understand the threat** and analyze it quickly
- **Prevent damage** with a rapid automated response
- **Save time and resources** with one straightforward tool
- **Defend every endpoint:** laptops, servers, cloud workloads

Key features

- Inherent **next-gen endpoint security**
- **Advanced detection** based on machine learning
- **Indicator of Compromise** (IoC) scanning
- **Visual investigation and analysis** tools
- All the necessary data in a **single alert card**
- **In-built response** guidance and automation
- **Single cloud or on-prem console** and automation
- Supports **workstations, virtual and physical servers, VDI deployments and public cloud workloads**

Key use cases

Am I under attack?

- **Advanced detection** – based on machine learning, including cloud sandboxing – automatically detects threats.
- **Download and scan IoCs** from securelist.com or other sources to find advanced threats.

Can I neutralize it?

- **Utilize multiple response options** – isolate host, prevent file execution or remove it.
- **Scan other hosts** for signs of the analyzed threat.
- **Apply an automatic response** across hosts on discovering a threat (IoC).

How do I get some skills training?

- **Check out the response guidance** in the alert card.
- **Access the Threat Intelligence Portal** and the latest TI.
- **Develop your expertise** as you analyze and respond to threats.

How did it happen?

- Analyze the threat in a **visual process tree.**
- Track its actions in a **drill-down graph.**
- **Understand its root cause and entry point** into the infrastructure.

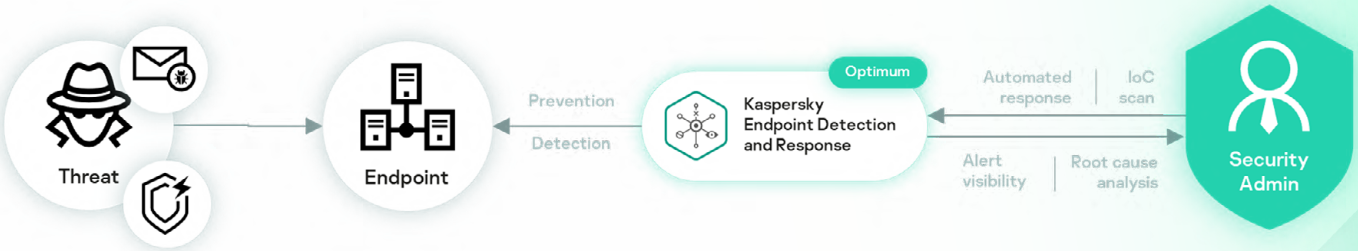
How do I stop it ever happening again?

- **Put learnt information to use –** knowing which IPs and websites to block, policies to modify and employees to train.
- **Create rules for preventing** such threats in the future, e.g. prevent file execution.

What about all the commodity threats?

- **Next-gen endpoint security** is on board to stop most threats right away.
- **Step up your patching** with Vulnerability and Patch Management.
- **Automate your attack surface reduction** and policy adjustment with endpoint controls.

How it works



For a quick demo check out this video.

Where are you coming from?

Got anti-malware, but it's just not enough?

Step up your endpoint protection

Whether you're using Kaspersky or 3rd party endpoint protection, this is the right time to think about implementing EDR.

It's not just about enhanced detection and prevention capabilities, but about being prepared against evasive threats – identifying, analyzing and neutralizing them.

Learn more about how to protect against evasive threats with **A buyer's guide to Optimum Level security**.

Already using Kaspersky?

Optimize your security

We're continuously improving our products, so make sure you're using us to the full with an upgrade – or move to cloud and completely forget about pesky routine tasks.

In the latest version of Kaspersky EDR Optimum:

- Guided response in alert card!
- System Critical Objects check before applying response!
- Threat Intelligence file reputation in alert card!
- Unlimited depth of process tree analysis!

Learn more about new features **here**.

New to Kaspersky?

Optimize your security

Thousands of businesses around the globe use Kaspersky EDR Optimum because it delivers:

- Powerful EPP and basic EDR in a single product
- Simple-to-use EDR capabilities designed for smaller cybersecurity teams
- A lightweight and flexible solution with cloud or on-prem deployment

Check out **Kaspersky Optimum Security** – a compound solution against evasive threats, based on EDR and MDR technology

Go forward with a stage-by-stage approach

The tools you use should be a perfect fit for your cybersecurity and business needs, and for your team and resources. So we've made it simple to choose the level of cybersecurity that's your main focus right now, with three different options depending on your organization's profile.

Kaspersky Security Foundations

Automatically blocking 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.

» Learn more

Kaspersky Optimum Security

Build up your defenses against evasive threats, if you have:

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

» Learn more

Kaspersky Expert Security

Readiness for complex and APT-like attacks for organizations:

- With complex and distributed IT environments.
- Who have a mature IT security team, or an established Security Operations Center (SOC).
- With a low appetite for risk due to higher costs of security incidents and data breaches.
- Who are operating in an arena where regulatory compliance is a concern.

» Learn more

Who we are

We are a global private cybersecurity company with hundreds of thousands of customers and partners around the world, commited to transparency and independence. For 25 years we've been building tools and providing services to keep you safe with our Most Tested, Most Awarded technologies.

IDC

IDC MarketScape Worldwide Modern Endpoint Security for Enterprises 2021 Vendor Assessment

Major Player

Named a Major Player
IDC MarketScape: Worldwide Modern Endpoint Security for Enterprise and SMB 2021 Vendor Assessments
IDC

AV-Test

Advanced Endpoint Protection: Ransomware Protection Test

100% protection

AV TEST
Advanced Endpoint Protection: Ransomware Protection Test
100% protection
Best result among 11 vendors

Radicati Group

Advanced Persistent Threat (APT) Market Quadrant

Top player

The Radicati Group, Inc.
A Technology Market Research Firm
Top Player
Advanced Persistent Threat (APT) Market Quadrant 2022

If you need even more

Check out Kaspersky EDR Expert, a powerful EDR tool to equip your experts with in-depth threat hunting capabilities, far-reaching customization and superior detection mechanisms.

Take a closer look

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

Cyber Threats News: securelist.com
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise

kaspersky.com