**Kaspersky Next
EDR Optimum**

# Unpacking Kaspersky Next EDR Optimum

## What is Kaspersky Next EDR Optimum?

Kaspersky Next EDR Optimum provides strong endpoint protection, improved controls, training, patch management and more – all enhanced by essential EDR functionality.

Threat visibility, investigation and response are simple, quick and guided, to help IT and IT security teams deflect attacks rapidly and with minimal resources.

## Why Kaspersky Next EDR Optimum – and why now?

### The evolving threat landscape is making EDR a requirement, not a choice

For years, small-to-medium businesses (SMBs) and low-end enterprises have been able to rely on endpoint protection platforms (EPP) to defend themselves against an extensive range of mass-produced, low-effort commodity threats. But today's attackers are focusing on organizations of all sizes, industries and levels of preparedness – and are mounting more dangerous attacks.

This evolution of the threat landscape means that over time, increasingly sophisticated threats which previously affected only large organizations are cascading down to impact SMBs and smaller enterprises that do not possess the in-house resources needed to deal with them effectively.

In particular, the advent of evasive threats - which use legitimate tools in attacks, include readymade scenarios to bypass EPP, are low cost and readily available on the dark web – has significantly increased cybersecurity risks for organizations using traditional EPP solutions.

If you're used to only needing EPP, enhancing your defenses with endpoint detection and response (EDR) can feel like a significant step up in terms of the necessary tools and skills. But fortunately, it doesn't have to be.

**Adding appropriate EDR capabilities to modern EPP can provide highly effective defense against more advanced evasive threats**

# Upgrading to EDR doesn't have to be a challenge

Many organizations have limited time and resources (or a small IT security department and no plans to expand it), but need to understand what's happening to their infrastructure and be able to respond to evasive threats before damage can occur.

Adding appropriate EDR capabilities to modern EPP can provide highly effective defense against more advanced evasive threats. So if you're new to EDR, you should look for a solution enabling automated and/or fast, accurate 'single-click' responses like quarantining files, host isolation, stopping a process, deleting an object etc.

As you become more proficient - or if you already have IT security specialists and/or EDR - your solution should also provide the information, insights and tools needed for effective investigation, such as root cause analysis, creating custom Indicators of Compromise (IoCs), importing IoCs, and scanning for these across all endpoints.

Through this, the kinds of results you should expect from EDR include:

- Robust protection against more frequent and more disruptive evasive threats.
- Saving time and resources with a simple, automated tool.
- Assessing the scope of an attack by scanning for IoCs across all endpoints.
- Understanding the root cause of each threat and how it actually occurred.
- Avoiding further damage with rapid automated response.

So, if your EPP is failing to stop increasing numbers of new, unknown and evasive threats; you have limited visibility into what's happening on your endpoints; or you're concerned about potential fines, or the threat to your business's reputation resulting from a major security incident; a modern EDR solution like Kaspersky Next EDR Optimum provides the ideal way to begin or progress your EDR journey.

### Your business is under cyberattack so how will you react?

It's your first day in a new IT security job, and you're just getting your feet under the table when it appears the company is under attack.

What would you do? How would you react?

Learn more
www.kaspersky.com/response-game

---

## How Kaspersky Next EDR Optimum can help

### What it does

Delivers strong endpoint protection, superior controls, training, patch management and more

Essential EDR functionality includes clear threat visibility, simple investigation, and guided and straightforward response, to quickly deflect attacks with minimal resources

### How it works

Enhances threat visibility and visualization

Simplifies root cause analysis

Delivers quick, automated response

Cloud or on-premises console

### Business value

Protects your business from dangerous evasive threats and improves your cybersecurity stance with a single solution

Enables IT or IT security teams to work more effectively without having to juggle multiple tools and consoles

Automates a vast array of processes to avoid reliance on traditional remediation processes that might result in downtime

Makes it easy to monitor, detect and investigate threats, and respond to and prevent attacks

### Who it's best for

Businesses with an in-house IT security team (or just 1-3 security specialists) requiring granular endpoint visibility and automated response to reduce manual handling tasks

# What do you get?

### Endpoint protection

File, web and mail antivirus, network protection, behavior detection, remediation, exploit prevention, HIPS, AMSI, anti-cryptor, BadUSB attack prevention

### Security management

Firewall, web, device, application controls, adaptive anomaly control, file integrity monitor, log inspection, system integrity monitor

### Mobile protection and management

Protection, controls and management, iOS MDM

### IT scenarios

Vulnerability assessment, patch management, data wipe, software/hardware inventory, third-party apps and OS installation, remote connection

### Encryption

Encryption and encryption management

### Cloud protection

Cloud discovery and blocking, data discovery, security for MS O365

### Education

Cybersecurity training for IT administrators

### EDR capabilities

Root cause analysis, IoC scan, single-click and automated response, response guidance

**Kaspersky Next EDR Optimum** helps organizations grow their security in step with their IT environments

# What if you're already using Kaspersky security?

As businesses develop and their IT requirements increase in complexity, so their security needs grow and diversify. Kaspersky Next EDR Optimum helps organizations grow their security in step with their IT environments by starting to develop incident response processes and expertise, and counter the advanced threats that come with an expanded attack surface. This enables attacks to be detected, analyzed and addressed quickly and automatically, significantly reducing their impact.

| Your Kaspersky solution | Recommended migration | Additional capabilities you'll get |
|---|---|---|
| **Kaspersky Endpoint Security Cloud** Pro | **Kaspersky Next EDR Optimum** | • File integrity monitor<br>• Log inspection<br>• System integrity monitor<br>• Software/hardware inventory<br>• Third-party applications installation<br>• On-premises OS installation<br>• Ability to use enterprise console on-premises or in the cloud (Expert view) |
| **Kaspersky Endpoint Security for Business** Advanced<br><br>**Kaspersky Total Security for Business** | **Kaspersky Next EDR Optimum** | • Simple cloud console option<br>• Essential EDR functionality including root cause analysis, IoC scan and automated response<br>• Cybersecurity training for IT administrators<br>• Cloud discovery and blocking<br>• Data discovery<br>• MS Office 365 security |
| **Kaspersky Endpoint Detection and Response** Optimum | **Kaspersky Next EDR Optimum** | • Simple cloud console option<br>• Cybersecurity training for IT administrators<br>• Cloud discovery and blocking<br>• Data discovery<br>• MS Office 365 security |

Find out more about Kaspersky Next EDR Optimum

**Kaspersky Next EDR Optimum**

**Kaspersky Next EDR Foundations**    [ Learn more ]

**Kaspersky Next XDR Expert**    [ Learn more ]

Learn more about Kaspersky Next at:
https://go.kaspersky.com/next

Choose the tier that suits you best by taking a short survey in our interactive tool:
https://go.kaspersky.com/Kaspersky_Next_Tool