



# Kaspersky Next: cybersecurity redefined

Kaspersky Next reinforces your security from endpoint protection (EPP) through endpoint detection and response (EDR) to extended detection and response (XDR) - securing your attack surface and mitigating threats before they can harm your organization.



## Kaspersky Next EDR Foundations

Provides powerful ML-based endpoint protection, flexible security controls and EDR root cause analysis for the most straightforward way to build a strong cybersecurity core



## Kaspersky Next EDR Optimum

- Delivers strong endpoint protection, superior controls, training, patch management and more
- Essential EDR functionality includes enhanced visibility, quick investigation and simple and guided response, to rapidly deflect attacks with minimal resources



## Kaspersky Next XDR Expert

- Full-featured Open XDR platform integrates seamlessly with existing security infrastructure, tools and applications
- Provides real-time visibility and deep insights into evolving cyberthreats to deliver advanced threat detection and automated response

## How it works

- Ensures effective protection for all endpoints
- Incorporates basic EDR capabilities for increased understanding of threats and attacks
- Cloud or on-premises console

- Enhances threat visibility and visualization
- Simplifies root cause analysis
- Delivers quick, automated response
- Cloud or on-premises console

- Detects complex threats through cross-correlation of multiple data sources
- Includes powerful EDR functionality with advanced detection and response capabilities
- Allows for proactive threat hunting to discover well-hidden complex attacks

## Business value

- Delivers robust endpoint protection together with increased visibility and IT scenarios in a simple 'launch-and-forget' solution

- Enables IT security teams to work more effectively without having to juggle multiple tools and consoles
- Automates a vast array of processes to speed up routine tasks and avoid reliance on manual remediation processes that might result in downtime
- Makes it easy to monitor, analyze and respond to threats and learn the principles of EDR

- Ecosystem approach, together with open design, maximizes efficiency of the cybersecurity tools involved, saves resources and reduces risk
- Simplifies the work of IT security specialists and gives them the additional context needed to investigate multi-vector attacks
- Minimizes MTTD and MTTR - crucial in combating complex threats and targeted attacks
- Provides holistic protection against the evolving threat landscape

## Who's it best for?

- Businesses with an IT administrator but limited specialist IT security resources

- 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

- Organizations with significant security resources wanting a single platform delivering:
- A coherent picture of what's happening across the protected infrastructure
  - Built-in threat hunting and threat intelligence
  - Superior incident prioritization and fewer false positive alerts

## What do you get?



### Kaspersky Next EDR Foundations

Endpoint protection: File, web and mail antivirus, network protection, AMSI, exploit prevention, remediation, behavior detection, HIPS

- ✔ Security management: Firewall, web, device, application controls
- ✔ Mobile protection and management: Protection, controls and management, iOS MDM
- ✔ IT scenarios: Vulnerability assessment, software/hardware inventory
- ✔ Cloud discovery
- ✔ EDR capabilities: Root cause analysis



### Kaspersky Next EDR Optimum

All the capabilities of Kaspersky Next EDR Foundations, plus:

- ✔ IT scenarios: Patch management, data wipe, third party apps and OS installation, remote connection
- ✔ Encryption and encryption management
- ✔ Cloud blocking, security for MS O365
- ✔ Education: Cybersecurity training for IT administrators
- ✔ EDR capabilities: IoC scan, endpoint response



### Kaspersky Next XDR Expert

Full range of XDR and EDR capabilities including:

- ✔ Alerts aggregation
- ✔ Cross-correlating data from multiple sources
- ✔ Sandbox
- ✔ AD integration
- ✔ Playbooks
- ✔ TI enrichment
- ✔ Third party connectors
- ✔ Investigation graph
- ✔ Log management and data lake
- ✔ Fully automated response and more

Through just three product tiers, Kaspersky Next secures your infrastructure by combining outstanding endpoint protection and controls with the transparency and speed of EDR, and the complete vision and power of XDR. This lets you choose the tools you need right now, then switch up easily when your protection requirements grow.

Learn more



Kaspersky Next EDR Foundations

Learn more



Kaspersky Next EDR Optimum

Learn more



Kaspersky Next XDR Expert

Learn more

Cyber Threats News: [www.securelist.com](http://www.securelist.com)  
IT Security News: [business.kaspersky.com](http://business.kaspersky.com)  
IT Security for SMB: [kaspersky.com/business](http://kaspersky.com/business)  
IT Security for Enterprise: [kaspersky.com/enterprise](http://kaspersky.com/enterprise)  
Threat Intelligence Poal: [opentip.kaspersky.com](http://opentip.kaspersky.com)  
Interactive Pofolio Tool: [kaspersky.com/int\\_portfolio](http://kaspersky.com/int_portfolio)

2023 AO Kaspersky Lab.  
Registered trademarks and service marks are the property of their respective owners.