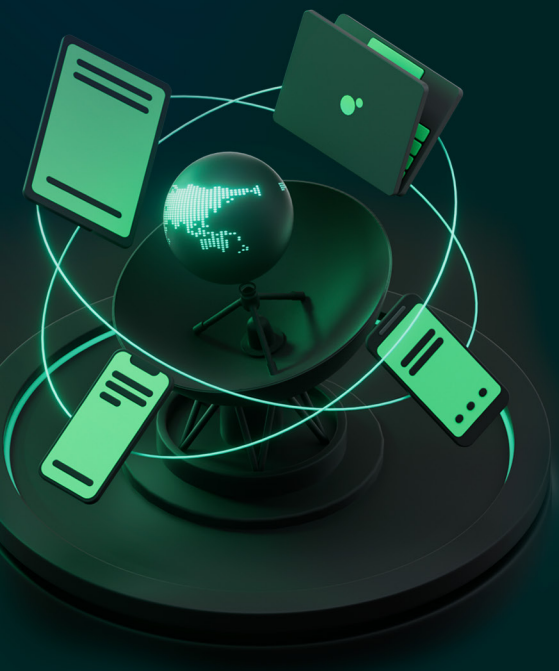
Kaspersky Next XDR Expert

Unpacking Kaspersky Next XDR Expert

What is Kaspersky Next XDR Expert?

As the most advanced of Kaspersky Next's three product tiers, Kaspersky Next XDR Expert integrates seamlessly with an organization's existing security infrastructure, providing real-time visibility and deep insights into evolving cyberthreats to deliver advanced threat detection, automated response and an extensive range of essential XDR capabilities.



Why Kaspersky Next XDR Expert – and why now?

Cybercriminals are continually refining their tactics, and developing ever-more sophisticated ways to target organizations. Today's attackers are increasingly taking a multi-vector approach to staging their attacks, often involving multiple entry points into the infrastructure, and a variety of different tactics and techniques.

Advanced persistent threats (APTs), for example, circumvent traditional endpoint detection, and can stay active for weeks or months – moving laterally through the network, gaining permissions, exfiltrating data, and gathering information from the different layers of the IT infrastructure in preparation for a large-scale attack or data breach.

Achieving effective security against these threats requires a comprehensive and proactive approach combining advanced technologies, robust policies, vigilant monitoring, ongoing training and more. And this is exactly the 360° view of the threat landscape that XDR sets out to deliver.

By breaking down the silos between layer-specific point solutions, XDR gives SOCs and IT security teams the end-to-end visibility and integration they need to identify threats faster, respond to them more quickly, resolve them more effectively and minimize the damage they cause.

How XDR addresses these issues

The 'extended' in extended detection and response reflects the fact that in XDR, an endpoint detection and response (EDR) solution is supplemented by and closely integrated with a variety of other security tools.

With XDR, security solutions that aren't necessarily designed to work together can interoperate seamlessly on threat prevention, detection, investigation and response. These could, for example, include solutions designed to protect mail, web, the network, cloud infrastructure, applications, identity etc., enabling additional kinds of attack scenarios to be detected and investigated, and strengthening the process of combating complex cyberthreats.

By providing a single window into, and full visibility between, cybersecurity tools and layers, XDR enables overburdened security teams to detect and resolve threats faster and more efficiently; and capture more complete, contextual data to help them make better security decisions and prevent future attacks.

To combat increasingly sophisticated cyberthreats, organizations need more than just a unified set of security tools from the same vendor

Find which Kaspersky Next product suits you best with the help of our interactive tool: https://go.kaspersky.com/Kaspersky_Next_Tool

What about the business benefits?

To combat increasingly sophisticated cyberthreats, organizations need more than just a unified set of security tools from the same vendor.

- Amid a global shortage of information security experts, XDR provides holistic protection for an expanding, changing IT infrastructure against a rapidly evolving cyberthreat landscape.
- By automating routine tasks, XDR reduces manual effort and response times, simplifies the jobs of valuable, scarce resources such as IT security specialists, and frees them to engage in the process of working with complex incidents.
- By enabling real-time behavioral and telemetry analysis across multiple security layers, security analysts can better visualize cyberthreats, and target and eliminate threats based on the severity with which they can impact the organization's IT infrastructure.
- XDR helps minimize mean time to detect (MTTD) and mean time to response (MTTR) - crucial for combating complex threats and targeted attacks.

Plus, even if your organization has limited expert resources, XDR can protect against complex attacks through capabilities including:

- Increased process automation.
- The use of a single, unified console.
- Playbooks and automation enabling close interaction between IT security tools as a part of XDR and joint scenarios.
- A single data lake environment.
- Built-in enrichment with trustworthy, relevant threat intelligence data.
- Fewer false positives, and minimized impact of real threats.

How Kaspersky Next XDR Expert can help

What it does

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

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

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 it's best for

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?

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, cloud discovery and blocking, 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 applications and OS installation, remote connection

Encryption

Encryption and encryption management

EDR capabilities

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

Advanced EDR capabilities

Gathering telemetry data, threat hunting capabilities, Indicator of Attack (IoA) detection, MITRE ATT&CK mapping

XDR capabilities

Alerts aggregation, sandbox, AD integration, threat intelligence / Kaspersky Security Network enrichment, case management, manual and automated playbooks, investigation graph, third-party connectors, log management and data lake, fully automated response, threat detection and cross-correlation

What if you're already using Kaspersky security?

Your Kaspersky solution	Recommended migration	Additional capabilities you'll get
Kaspersky Endpoint Detection and Response Standard / Advanced / Expert*	Kaspersky Next XDR Expert	• Cross-asset scenarios • Alerts aggregation • Incident workflow • Investigation graph

* Please bear in mind that you can still purchase or use Kaspersky EDR Expert as a standalone solution, or upgrade and use it as part of Kaspersky Next XDR Expert

Find out more about Kaspersky Next XDR Expert

Kaspersky Next XDR Expert

Kaspersky Next EDR Foundations — Learn more

Kaspersky Next EDR Optimum — Learn more

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

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