Kaspersky Next EDR Expert

Kaspersky Next XDR Expert



Boost visibility, automate response and speed up threat detection

Kaspersky Next XDR Expert

kaspersky

Kaspersky Next XDR Expert is designed for highly advanced enterprises, usually with significant resources and a dedicated cybersecurity team or Security Operations Center (SOC). These organizations take a proactive approach to adopting the latest technologies, staying ahead of threats and implementing comprehensive security solutions.

Helping your team make informed decisions and take swift action

To combat sophisticated targeted attacks, cybersecurity teams must manually analyze and assess high volumes of incidents and alerts, many of which turn out to be false positives. They also rely on security tools managed through separate consoles, forcing analysts to switch between interfaces and systems, which impacts productivity.

This lack of a consolidated view leads to poor decision making, while the growing volume and increasing complexity of attacks, expanding attack surface and the global shortage of skilled cybersecurity professionals make it harder to stay ahead of cybercriminals. The result: business disruption, financial loss and reputational damage.

The ultimate AI-enabled tool for cybersecurity teams

Kaspersky Next XDR Expert automatically protects your infrastructure against mass attacks while empowering your security staff or SOC team to identify and respond to complex, persistent threats.

The solution equips your experts with advanced tools that optimize and streamline workflows, provide a single unified view of security operations and reduce false positives so your business can operate and grow without disruption while keeping advanced threats out.

The platform ships with 3,200+ pre-configured detection rules maintained by Kaspersky SOC, mapped to MITRE ATT&CK and supplied with response guidance, delivering SOC-grade detection without requiring internal rule engineering.

The platform provides tools for protecting your organization at every stage, from automated defense against widespread threats to detecting and containing sophisticated attacks.

Automated protection from mass threats

- Endpoint protection
- Email and hybrid cloud protection
- Security awareness training

Identifying complex & persistent threats

- Monitoring & cross-correlation
- Advanced detection of persistent threats
- Investigation & threat hunting

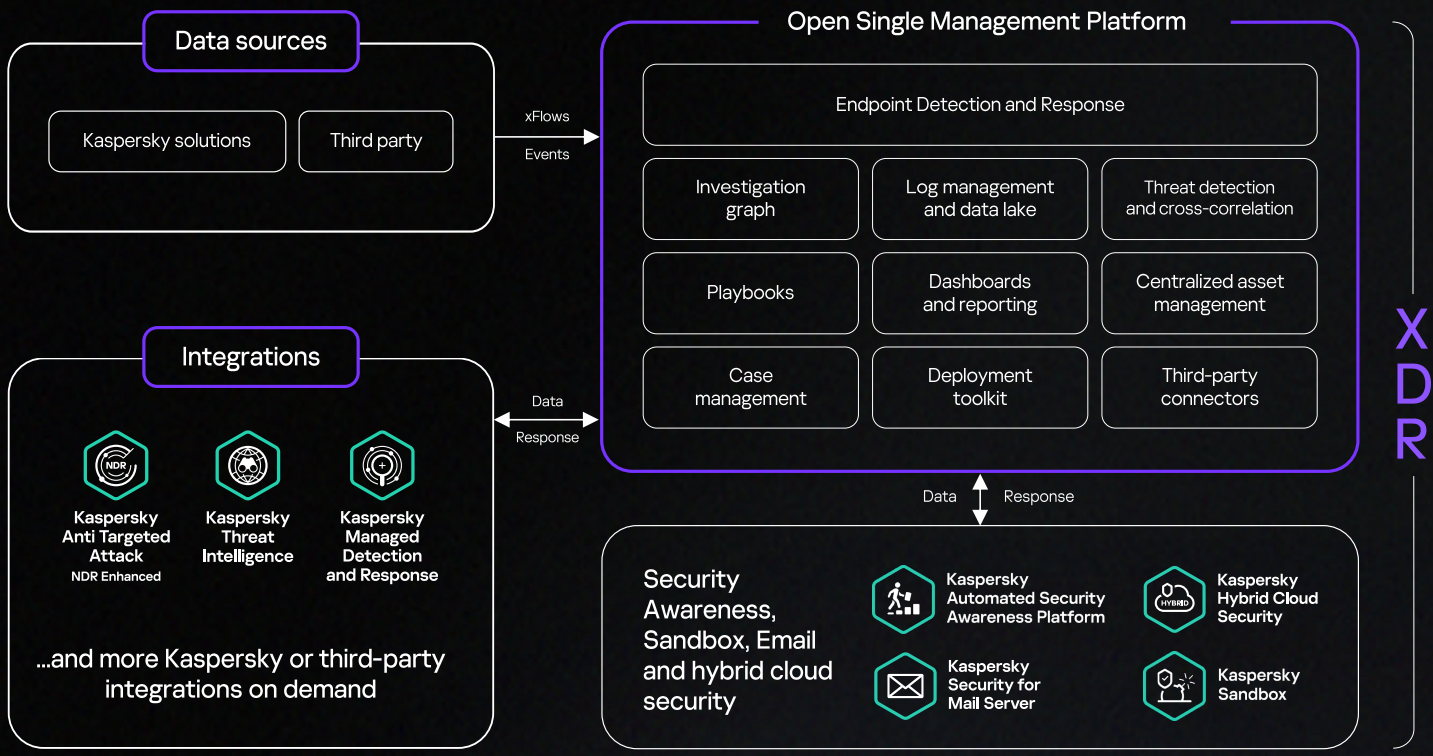
Responding to complex & persistent threats

- Case management
- Response automation & orchestration
- Incident response

How it works

Kaspersky Next XDR Expert is built on our **Open Single Management Platform,** which integrates all solution components (including Kaspersky and third-party tools) and enables interaction between them. It's an integral part of our unified IT-OT XDR technology stack, serving as a central component for incident management and supporting the administration and maintenance of security tasks.

The platform can be deployed on-premises, including in isolated and air-gapped environments, or used as a cloud service operated by Kaspersky. Both models run on the same technology stack and use the same detection content. Feature availability varies by deployment model.



With on-demand solutions for enhanced security, Kaspersky Next XDR Expert enables users to tailor the security system to their enterprise's specific needs. This improves the overall security posture and user experience without overspending or relying on multiple vendor tools to cover every security domain, improve incident response efficiency and enrich data with threat intelligence.

Our technologies help cybersecurity teams maximize the impact of their security operations by:

Introducing stronger endpoint protection that reduces the number of alerts that teams need to analyze

Identifying sophisticated threats using AI, and improving MTTD

Automating operations and accelerating MTTR

Increasing efficiency through advanced case management

Providing 300+ prebuilt integrations and a deployment choice: on-premises or cloud-hosted

Kaspersky Next XDR Expert — part of the Kaspersky Next product line

Kaspersky Next is a tiered product line for businesses of all sizes. It has two offerings, one of which is Kaspersky Next Expert for enterprises with dedicated cybersecurity teams or Security Operations Centers. It delivers advanced EDR and XDR capabilities, powerful automation and flexible expansion through on-demand technologies, helping teams maximize the impact of their security operations.

Why Kaspersky Next Expert?

Multi-layered defense based on AI technology

Kaspersky uses a joint stack of AI-powered detection technologies to boost detection speed and improve accuracy. AI powers asset-based alert prioritization, detection of DLL hijacking and more.

The Kaspersky Investigation and Response Assistant (KIRA) adds a GenAI-based assistant for SOC analysts: deobfuscating command lines, supporting natural-language threat hunting and generating concise incident reports. Together these reduce the impact of cyber incidents and improve MTTD and MTTR.[1]

Deployment flexibility

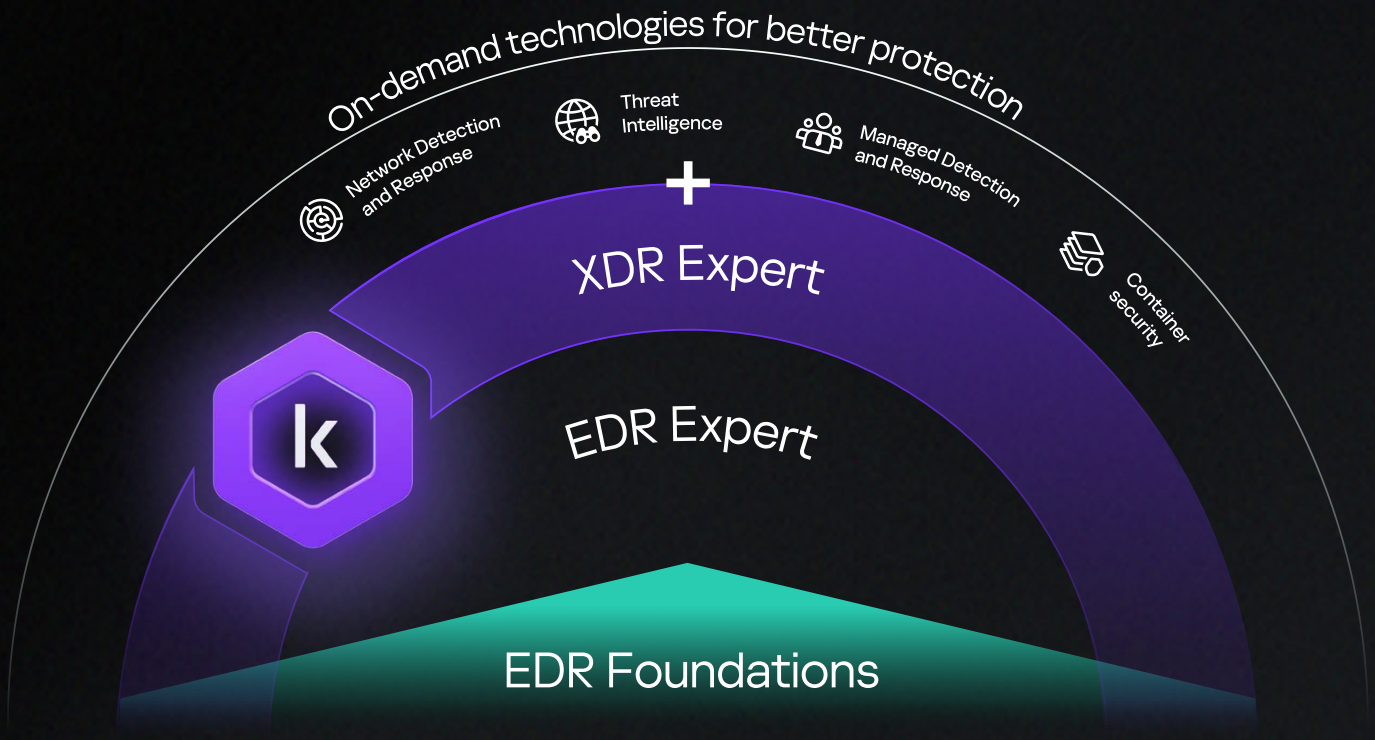
On-premises, hybrid, air-gapped or cloud: one platform, one detection stack. Organizations with data residency or sovereignty requirements keep processing inside their own perimeter; those without them get faster time-to-value.

Backed by deep knowledge, skills and expertise

Kaspersky Next is built on decades of the accumulated experience and deep knowledge of **our global security teams**. Our specialists work collaboratively to address complex cyberthreats, continuously refining the technologies that power our products. This expert-driven approach ensures our solutions are reliable, innovative and aligned with real-world security needs.

Built on our best-in-class endpoint solution

For over a decade, Kaspersky products have consistently ranked at **the top** in independent tests and reviews. Our proven automated endpoint protection reduces the number of alerts security teams need to analyze, improving their efficiency.



1 AI features require an add-on license for on-premises deployments and are included in the cloud license. An LLM provider integration is required.

www.kaspersky.com

© 2026 AO Kaspersky Lab.
Registered trademarks and service marks are the property of their respective owners.

Learn more

#kaspersky
#truetobusiness