Kaspersky Next EDR Expert

Kaspersky Next XDR Expert

Powerful, advanced protection for your endpoint infrastructure

Kaspersky Next EDR Expert

kaspersky

Comprehensive endpoint defense against advanced threats

In today's highly interconnected digital environments, endpoints remain the primary entry point for cyberattacks. To stay ahead of modern threats, organizations need more than traditional preventive controls — they require advanced detection, investigation and response capabilities.

Kaspersky Next EDR Expert is a powerful Endpoint Detection and Response solution that works seamlessly with endpoint protection to stop mass attacks and identify advanced threats. It automatically detects suspicious activity, enables incident investigation and equips security teams with the tools they need to respond quickly and effectively.

Designed for large, distributed infrastructures, Kaspersky Next EDR Expert helps rapidly contain threats and eliminate incidents across the enterprise. A single agent delivers comprehensive endpoint protection, reducing operational complexity, minimizing maintenance and support effort, and preserving system performance — while strengthening the overall security posture.

Kaspersky Next EDR Expert is perfect for organizations across all industries of any size and with internal IT security expertise, who are looking to enhance their detection and investigation depth, speed up response and gain forensic visibility across a large number of endpoints.

Recognition

Our technologies are regularly tested by independent testing labs and the quality of our products is recognized by leading analytical agencies. We have won numerous international awards.

Equip your team with world-class EDR

- Boost the effectiveness of your security with multi-award-winning EPP and powerful EDR functionality
- Strengthen the control you have over your endpoint infrastructure
- Improve detection and remediation of advanced threats
- Help establish threat detection, incident management and response processes through optimized allocation of resources
- Support your compliance with regulatory requirements and standards

EDR

2 Detection

Threat discovery based on IoC, IoA and custom rules

Enhanced detection with global threat intelligence

Proactive threat hunting and retrospective analysis

3 Investigation

Deep investigation and root cause analysis

Base digital forensics toolkit

4 Response

Support for a variety of response action

EPP

1 Prevention

Powerfull detection engine

Multiple security controls and data protection

Vulnerability and patch management

Behavior analysis and adaptive anomaly control

Key capabilities

Kaspersky Next EDR Expert provides a comprehensive overview of all endpoints in the corporate infrastructure together with visualization of every stage of threat investigation. Powerful detection engines and root cause analysis tools ensure that threat detection and investigation are efficient and effective.

Retrospective analysis and correlation of detections with the MITRE ATT&CK knowledge base make it possible to identify the tactics and techniques used by attackers. The product also provides proactive threat hunting and access to the Kaspersky Threat Intelligence portal, enabling experts to reconstruct the sequence of attacker actions and counter even the most sophisticated attacks.

EPP

Leading prevention technologies, including those based on ML

- Automatic threat blocking
- Automatic recovery
- Protection against encryption attempts
- Protection against exploitation of vulnerabilities
- Protection against credential theft

Security and data controls

- Application control
- Web control
- Device control
- Adaptive anomaly control
- Encryption and policy management
- Encryption of portable devices

Vulnerability assessment and patch management

- Advanced patch management
- Vulnerability assessment
- License management
- Centralized application and OS deployment
- Remote management tools
- Asset inventory

EDR

Automatic detection of advanced threats

- Data collection and storage
- Advanced detection mechanisms based on IoA rules
- Automatic access to Threat Intelligence (KSN)
- Retrospective analysis
- MITRE ATT&CK mapping

IoC search and threat hunting

- Full visibility and control
- Incident prioritization
- IoC scanning
- YARA rules
- Access to Threat Lookup
- Flexible query builder for proactive threat hunting

Response

- Incident response tool
- Automated response task setting
- Response recommendations
- Threat containment
- Centralized localization of incidents

Kaspersky Next EDR 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 based on statistical, structural and behavioral principles capable of detecting threats automatically to boost detection speed and improve accuracy. AI also powers risk scoring for assets. These technologies help reduce the impact of cyber incidents and improve MTTD and MTTR.

Backed by deep knowledge, skills and expertise

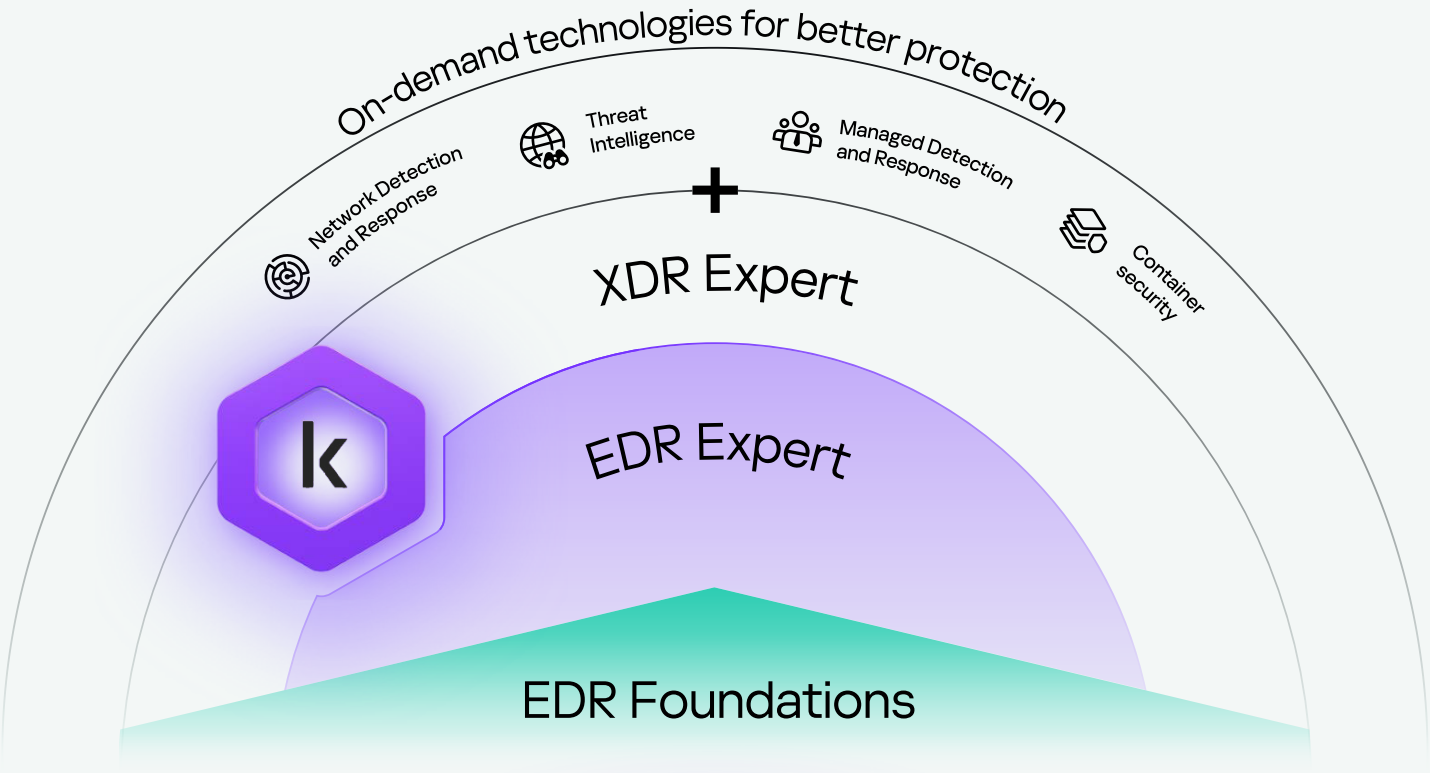
Kaspersky Next is built on decades of the accumulated experience and deep knowledge of our global security teams. Our specialists work collaboratively to address complex cyberthreats, continuously refining the technologies that power our products. This expert-driven approach ensures our solutions are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

Cybersecurity that grows with you

Kaspersky Next protects businesses of all sizes. As your needs grow, you can easily scale from essential endpoint protection to advanced, expert-level solutions available in higher tiers.

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.



www.kaspersky.com

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

Learn more

#kaspersky
#truetobusiness