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

Endpoints remain the primary entry point for cyberattacks. Preventive controls can stop mass threats, but fileless, targeted and human-driven attacks need more. Effective endpoint security combines prevention with detection, investigation and response.

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 across the enterprise. A single agent delivers both endpoint protection and EDR, reducing operational complexity and preserving system performance. It runs on the Open Single Management Platform, where functions operate natively through one console.

Two deployment models

Kaspersky Next EDR Expert runs on-premises in your own infrastructure, including isolated and air-gapped segments, or in the cloud, provisioned and operated by Kaspersky. Both share the same platform, detection content and response logic.

Feature availability varies by deployment model.

Recognition

Kaspersky products undergo regular independent assessments by leading research institutions. Kaspersky products have taken part in 1,122 tests and reviews, 861 first places, 965 top-three finishes.

Learn more

Equip your team with world-class EDR

- Boost the effectiveness of your security with multi-award-winning EPP and powerful EDR functionality
- Help establish threat detection, incident management and response processes through optimized allocation of resources
- Support your compliance with regulatory requirements and standards

EPP

1 Prevention

Powerfull detection engine

Multiple security controls and data protection

Vulnerability and patch management

Behavior analysis and adaptive anomaly control

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

Key capabilities

Kaspersky Next EDR Expert provides a comprehensive overview of all endpoints with visualization of every stage of threat investigation. Detections are mapped to MITRE ATT&CK, covering more than 55% of the matrix, so analysts see the tactics and techniques rather than just isolated alerts.

Learn more

Retrospective analysis, proactive threat hunting and access to the Kaspersky Threat Intelligence Portal help experts reconstruct the attacker's sequence of actions.

Automated protection from mass threats

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

VAPM and human-risk reduction

- Advanced patch management
- Vulnerability assessment
- Security awareness training with simulated phishing campaigns
- Centralized application and OS deployment
- Remote management tools
- Asset inventory

Identifying and responding to complex & persistent threats

Automatic detection of advanced threats

- Endpoint telemetry collection and storage
- 2,300+ Indicators of Attack developed by Kaspersky SOC experts
- Advanced sandbox with automatic and manual submission
- AI-enabled detection of DLL hijacking
- Retrospective analysis and MITRE ATT&CK mapping

IoC search and threat hunting

- Scheduled and real-time IoC scanning
- YARA and Sigma rule support
- AI assistant: plain-language threat-hunting queries, incident summarization and command-line deobfuscation
- AI-enabled alert and incident summarization
- Access to Kaspersky Threat Lookup

Response

- Host isolation, process termination and execution prevention
- File retrieval, deletion, quarantine and restore
- Forensics: process and file lists, registry keys, memory dumps, disk images
- Live Shell remote console for Windows and Linux
- Playbooks and a built-in response recommendation engine

Feature availability may vary depending on the deployment method and chosen license

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 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) extends these capabilities with GenAI-based support for SOC analysts, including command-line deobfuscation, natural-language threat hunting and concise incident reports. Together these capabilities reduce the impact of cyber incidents and improve MTTD and MTTR.[1]

Deployment flexibility

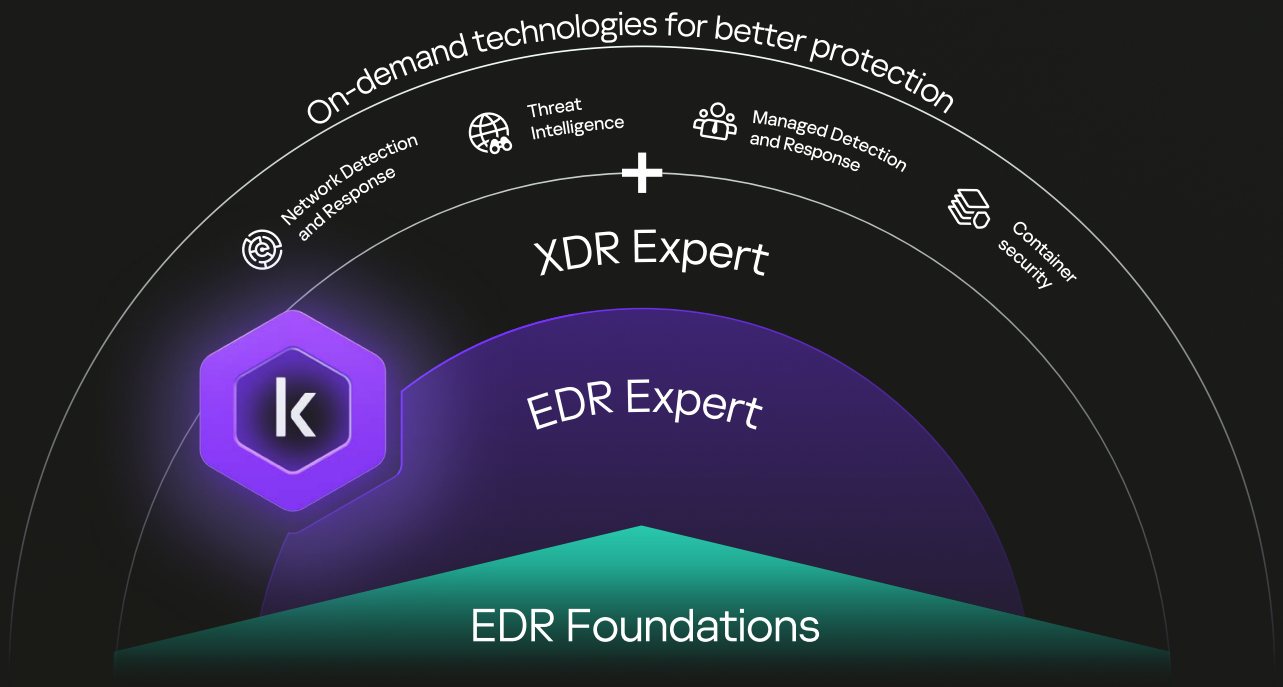
On-premises, hybrid, air-gapped or cloud: one platform, one detection stack. Organizations with data residency or sovereignty requirements keep processing inside their own perimeter, while organizations without those requirements can get faster time-to-value.

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