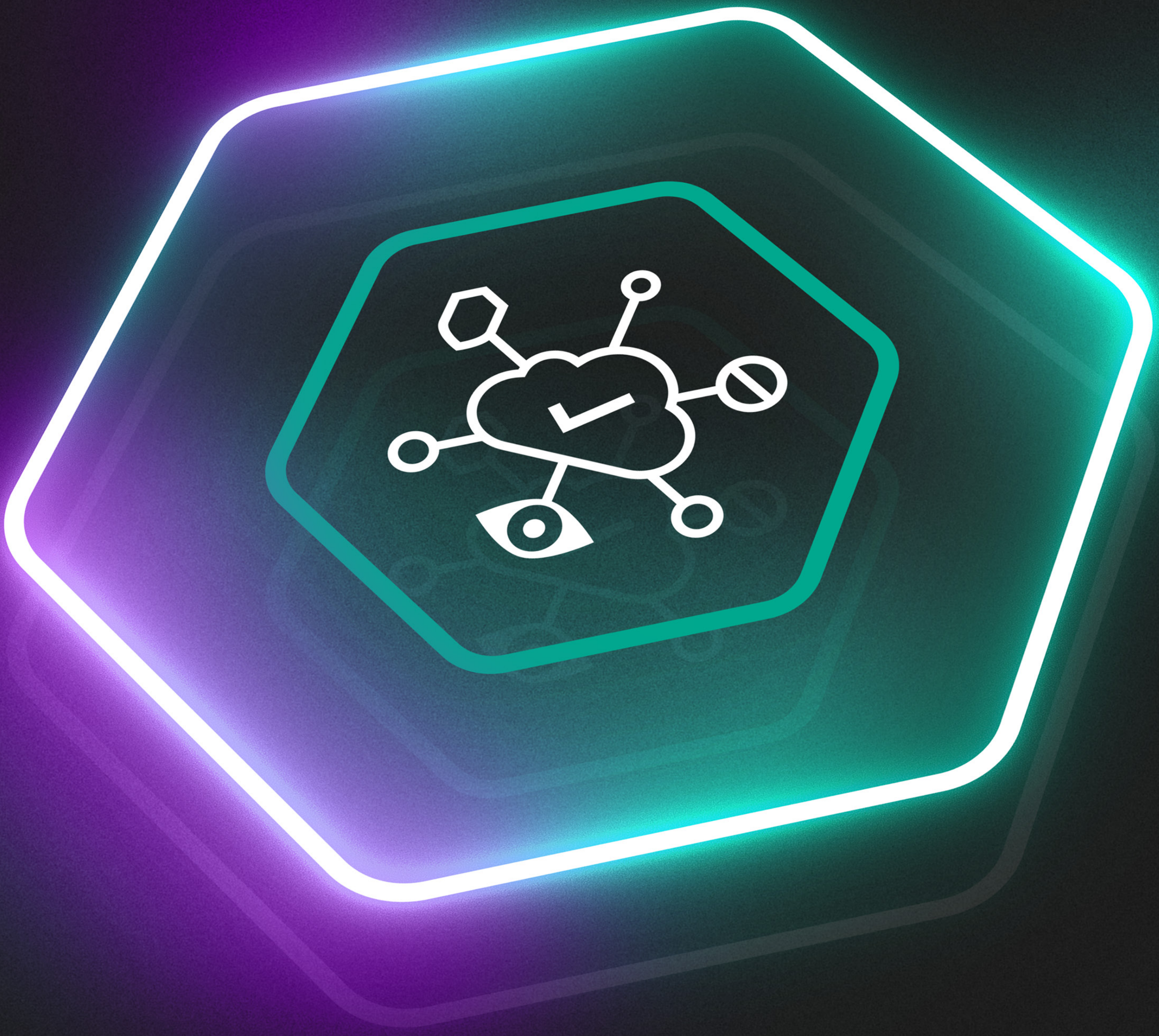


Kaspersky Endpoint Detection and Response (EDR) Expert

kaspersky BRING ON THE FUTURE

Cybercriminals are becoming ever more sophisticated and capable of successfully bypassing existing protection. Every area of your business can be exposed to risk, disrupting business-critical processes, damaging productivity and increasing operating costs.

Boost your endpoint defenses first

Corporate endpoints are where data, users and corporate systems come together to generate and implement business processes. These endpoints are still the primary target for cybercriminals.

Kaspersky Endpoint Detection and Response (EDR) Expert provides comprehensive visibility across all endpoints on your corporate network and delivers superior defenses, automating routine EDR tasks and enabling analysts to quickly hunt, prioritize, investigate and neutralize complex threats and APT-like attacks.

Kaspersky EDR Expert uses a single agent that can be managed from both a cloud-based central management platform and an offline console in air-gapped environments, leveraging threat intelligence and incorporating customizable detections rules.

Top challenges	With Kaspersky EDR Expert, your organization can:
Lack of the visibility and transparency. Detecting an incident may take weeks or even months more than it should, just because they're unable to see and understand exactly what's happened, how it happened and how to fix it.	**Effectively control and monitor all your endpoints** **By seeing the full picture – where the threat originated, how it spread, which hosts it affected, and what exactly can and should be done to prevent the consequences.**
Inefficiency. Forcing analysts to work across multiple decentralized consoles slows everything down and also creates opportunities for human error. The manual handling of routine detection processes can then waste even more time.	**Streamline your IT security team's work** **Fast, accurate threat containment and incident resolution across distributed infrastructures is supported through centralized and automated actions, helping to streamline your IT security team's work. No more costly additional resources needed, no more expensive downtime and no lost productivity.**
A lack of relevant intelligence. The inability to operationalize threat intelligence and no clear view of the adversary's tactics, techniques and procedures can hamper both alert prioritization and further investigation and response.	**Successfully hunt and mitigate threats – fast** **Raw data and verdicts are centrally aggregated, and investigation capabilities boosted through our unique Indicators of Attack (IoAs), through MITRE ATT&CK enrichment and a flexible query builder, and with access to our Threat Intelligence Portal knowledge base. All this significantly facilitates effective threat hunting and fast incident response, for damage limitation and prevention.**
Just understanding that the information security solution has detected a potential threat doesn't guarantee that subsequent actions will be effective. It's important to be able to respond to the threat effectively in real time, and to investigate the incident fully to prevent a reoccurrence.	**Respond faster – and more effectively.** **Guided investigation and a faster, more accurate response are crucial to dealing with complex and APT-like attacks. Kaspersky EDR Expert provides a seamless workflow with centralizing incident management and guided investigation across all endpoints on the corporate network.**
Analysts can't focus fully on complex threats if they're forced to waste time dealing with trivial alerts that should have been automatically handled by an effective endpoint protection solution. This can lead to analyst burn-out, and important alerts being missed amid all the 'noise'. "A weak EPP solution will destroy the value of an EDR tool", Endpoint Security 2020: The Resurgence Of EPP and the Manifest Destiny Of EDR, IDC, 2020	**Get maximum value from your solution – and your experts** **There's no point hiring expensive analysts to work with your EDR solution if your EPP leaves them dealing with alerts that don't require their skills. Our EDR solutions are always based on Kaspersky Endpoint Security for Business. This most tested, most awarded EPP solution established a strong foundation for Kaspersky EDR Expert, automatically handling the vast majority of alerts, and freeing-up analysts to focus on those that really require their attention and expertise. Our EPP and EDR products work together as a single solution, through the same endpoint agent.**

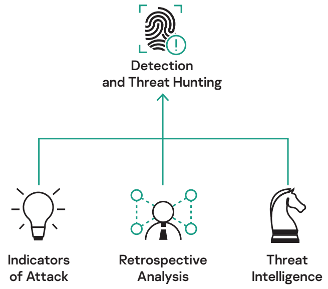
Kaspersky EDR Expert is ideal if your organization wants to:

- Enhance your endpoint visibility and threat detection with leading technologies.
- Upgrade your security with an easy-to-use, enterprise solution for incident response.
- Establish unified and effective threat hunting, incident management and response processes.
- Understand the specific Tactics, Techniques, and Procedures (TTPs) used by threat actors to achieve their goals, enabling more effective defenses and allocation of security resources.
- Increase the efficiency of your in-house SOC so they don't waste their time analyzing irrelevant endpoint logs.
- Support compliance by enforcing endpoint logs, alert reviews and the documenting of investigation results.

Top features

ADVANCED DETECTION

Enhanced threat discovery and a mature investigation process help detect advanced threats.



Fast investigation

Kaspersky EDR enables the ongoing monitoring and visualization of every investigative stage, fast access to data, premium threat discovery and efficient analysis.

Threat hunting

The investigation process is enhanced with retrospective analysis and unique Indicators of Attack with ATT&CK mapping that helps identify tactics and techniques, as well as proactive threat hunting and access to the powerful Kaspersky Threat Intelligence Portal.

Uncover the full scope of an attack

Your experts have all the tools to understand the entire sequence of intruder actions, discover the most sophisticated attacks and respond appropriately – and fast!

RAPID AND ACCURATE INCIDENT RESPONSE

Guided investigation and a faster, more accurate response are crucial to deal with complex and APT-like attacks.

Speed
No downtime

Centralization
No lost productivity

Automation
No additional resources

Quick and accurate incident response

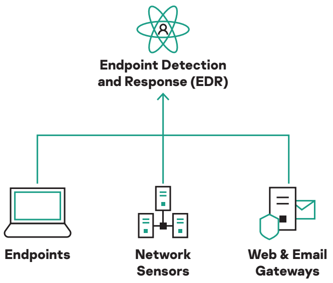
Quality and speed of incident response are Key Performance Indicators commonly applied to today's IT security departments. By centralizing incident management with guided investigation across all the endpoints on your corporate network, Kaspersky EDR provides a seamless workflow.

Centralization and automation

Fast, accurate threat containment and incident resolution across distributed infrastructures is supported through centralized and automated actions, helping to streamline the work of your IT security team. No more costly additional resources needed, no more expensive downtime and no lost productivity.

EXTENDED DETECTION AND RESPONSE (XDR)

Upgrade to a complete suite of Extended Detection and Response functionality effortlessly.



Build up to XDR

Kaspersky EDR can be absorbed into the Kaspersky Anti Targeted Attack Platform, providing extended detection and response capabilities. The Kaspersky Anti Targeted Attack Platform with Kaspersky EDR at its core represents an all-in-one APT protection solution and combines network-level advanced threat discovery and EDR capabilities.

A single solution for your experts

IT security specialists have all the tools they need to handle superior multi-dimensional threat discovery at endpoint and network levels, apply leading-edge technology, undertake effective investigations, and deliver a rapid centralized response — all through the single solution.

Gartner Peer Insights Customers' Choice for EDR Solutions 2020 names Kaspersky Top Vendor

Kaspersky is one of only 6 vendors worldwide to receive the Gartner Peer Insights Customers' Choice recognition for Endpoint Detection and Response solution in 2020, with the highest rating of any vendor for our service and support - the ultimate customer compliment for Kaspersky EDR Expert.

* Gartner Peer Insights Customers' Choice constitute the subjective opinions of individual end-user reviews, ratings, and data applied against a documented methodology; they neither represent the views of, nor constitute an endorsement by, Gartner or its affiliates.

Kaspersky Endpoint Detection and Response wins highest grade in SE Labs test

Kaspersky EDR has achieved the highest AAA award in SE Labs' Enterprise Advanced Security test (previously known as Breach Response Test). The solution was noted for its ability to detect complex targeted attacks, track malicious behavior from the beginning to the end of an attack and generate no false positive results. During the evaluation, the product was exposed to the tools, techniques, and procedures used by advanced threat groups.

Kaspersky named a Major Player in Modern Endpoint Security for Enterprise and SMB by IDC MarketScape

To help organizations evaluate the best endpoint protection platforms and endpoint detection and response solutions for their needs, the IDC MarketScape reviewed data submitted by MES vendors between April and September 2021, to position the capabilities of the companies.

Detection quality confirmed by MITRE ATT&CK Evaluation

Recognizing the importance of Tactics, Techniques and Procedures (TTPs) analysis in complex incident investigation and the role of MITRE ATT&CK in the security market today:

- Kaspersky EDR has participated in MITRE Evaluation Round2 (APT29) and demonstrated a high level of performance in detecting key ATT&CK Techniques from Round2 scope applied at crucial stages of today's targeted attacks.
- Kaspersky EDR's detections are enriched with data from the MITRE ATT&CK knowledge base, for deep analysis of your adversary's TTPs.

Use cases

- Endpoint protection and threat detection
- Incident response
- Proactive threat hunting
- Digital forensics
- Automation of routine operations
- Cloud-based management
- Proactive search for evidence of intrusion over your entire network
- Correlation of incidents across thousands of alerts with a seamless workflow
- Rapid detection and remediation of an intrusion
- Validation of alerts and potential incidents discovered by other security solutions
- Retrospective analysis
- Investigation and centralized management of incidents across thousands of endpoints with a seamless workflow

www.kaspersky.com

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise