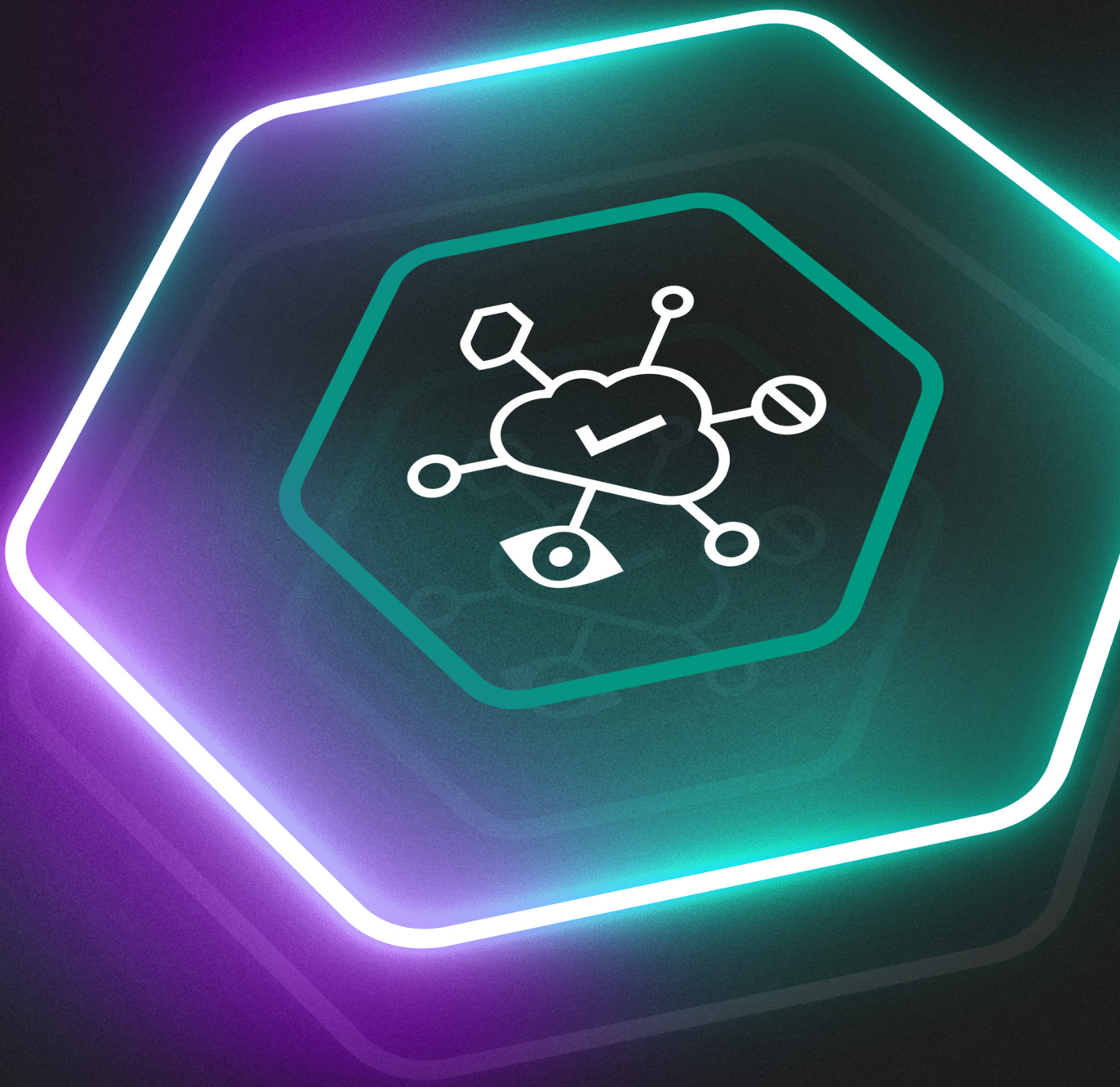

Kaspersky Endpoint Detection and Response

Expert

kaspersky BRING ON THE FUTURE

A single solution

Kaspersky EDR Expert is a single solution that can be managed from both a cloud-based central management platform and from an offline console in air-gapped environments.

Kaspersky Endpoint Detection and Response Expert

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 continue to be 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.

Today's Challenges

IT security teams lack the visibility and transparency they need to effectively monitor endpoints. Detecting an incident may take weeks or even months more than it should, just because it can be so difficult to see and understand exactly what's happened, how it happened and how to fix it.

Inefficiency. Forcing analysts to work across multiple decentralized consoles slows everything down, while creating opportunities for human error. And the same goes for obliging IT security professionals to manually handle routine detection processes.

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.

With Kaspersky EDR Expert, your organization can

1 Effectively control and monitor all your endpoints

By being able to see all aspects of 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.

2 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.

3 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 through access to our Threat Intelligence Portal knowledge base. All this significantly facilitates effective threat hunting and fast incident response, for damage limitation and prevention.

Today's Challenges

Shortfalls in response and investigation. Just understanding that something's happening in the infrastructure and 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 be able to investigate the incident fully to prevent a reoccurrence.

Wastage of expensive resources. 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. As well as being a waste of resources, this can lead to analyst burn-out, and important alerts being missed amid all the 'noise'.

With Kaspersky EDR Expert, your organization can

4 Respond faster — and more effectively

Guided investigation and a faster, more accurate response are crucial in 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.

5 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 based on our most tested, most awarded EPP solution, which automatically handles 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:

- Upgrade your security with an easy-to-use, enterprise solution for incident response.
- Automate threat identification & response without business disruption during investigations.
- Understand the specific Tactics, Techniques, and Procedures (TTPs) used by threat actors to achieve their goals, enabling more powerful defenses and the effective allocation of security resources.
- Enhance your endpoint visibility & threat detection with advanced technologies.
- Establish unified and effective threat hunting, incident management and response processes.
- Increase the efficiency of your in-house SOC so they don't waste their time analyzing irrelevant endpoint logs and alerts.
- Support compliance by enforcing endpoint logs, alert reviews and the documenting of investigation results.

Kaspersky EDR Expert gives you the power to:

- **Detect threats using the best, most advanced methods. Profiling potential threat actors' activity is an efficient way of detecting malicious activity within an infrastructure.**

Kaspersky EDR Expert allows centralized Indicators of Compromise **(IoC)** to be loaded from threat data sources and supports automatically scheduled IoC scanning, streamlining analysts' work

With our Indicators of Attack **(IoA)** engine, Kaspersky EDR Expert can discover suspicious actions using the unique set of IoAs generated by Kaspersky's threat hunters, provisioning real-time automated threat hunting capabilities

To give you a more accurate picture of what's happening, a file or process can be sent to the **Sandbox** for behavioral analysis, either manually or automatically

IoAs and Sandbox detections are mapped to **MITRE ATT&CK** for the further analysis of the adversary's Tactics, Techniques and Procedures. Individual events in the incident's tree are enriched with MITRE knowledgebase context, including the identification of MITRE-defined tactics used and visualization of the event on the incident graph

Counteraction recommendations

The automatic analysis of all endpoint events, correlated with the intelligence data acquired, arms you with clear event descriptions, examples and counteraction recommendations.

- Investigate the causes of the incident and prevent any recurrence. Kaspersky EDR Expert provides high-level endpoint protection and increases the efficiency of your SOC, providing access to retrospective data, even in situations where compromised endpoints are inaccessible or when data has been encrypted during an attack. Boosted investigation capabilities through our unique IoAs, MITRE ATT&CK enrichment and a flexible query builder, plus access to our Threat Intelligence Portal knowledge base - all facilitate threat hunting and fast incident response, leading to effective damage limitation and prevention.
- Choose a convenient telemetry storage option for forensics. A centralized database stores endpoint telemetry for 30 days by default and objects and verdicts with no time limit, meaning that forensic analysis can be performed without relying on endpoint availability. If you find you need more telemetry retention time, this can be increased to 60 or 90 days. In on-prem installations, it's up to you to determine the period of data storage, depending on the capacity and characteristics of your hardware.
- Respond in the way that suits you best. Your IT security experts are equipped with tools that enable a 'one click' response via the central management console, reducing the number of manual tasks and cutting response times from hours to minutes.
- Work smoothly and efficiently. The endpoint activity tree and click-down event tree visualization tools enable your investigators to easily pivot on interesting data elements during threat path evaluation or drill down for more information. Linking events and consolidating alerts helps reveal the full impact of an attack.

How it works

Awards and recognition

Kaspersky products are regularly assessed by global research firms, and our ability to help our customers protect themselves against cyberattacks is widely recognized and proven. We are the most tested, most awarded cybersecurity vendor.

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.

Kaspersky Endpoint Detection and Response Expert

Read more

www.kaspersky.com

To find out more about how Kaspersky EDR Expert can empower your IT Security team – get in touch!