Feature list

Kaspersky Managed Detection and Response

kaspersky bring on the future

Contents

Kaspersky MDR overview

Kaspersky Managed Detection and Response

Kaspersky Managed Detection and Response (MDR) delivers a fully managed ongoing detection, prioritization, investigation and response service. It delivers all the major benefits of a SOC center without the need to actually establish one.

The main purpose of the MDR service is to detect threats at every stage of a cyberattack, both prior to actual compromise and after malicious actors have penetrated the corporate infrastructure. This is achieved using preventative security systems and threat hunting, both integral components of Kaspersky MDR.

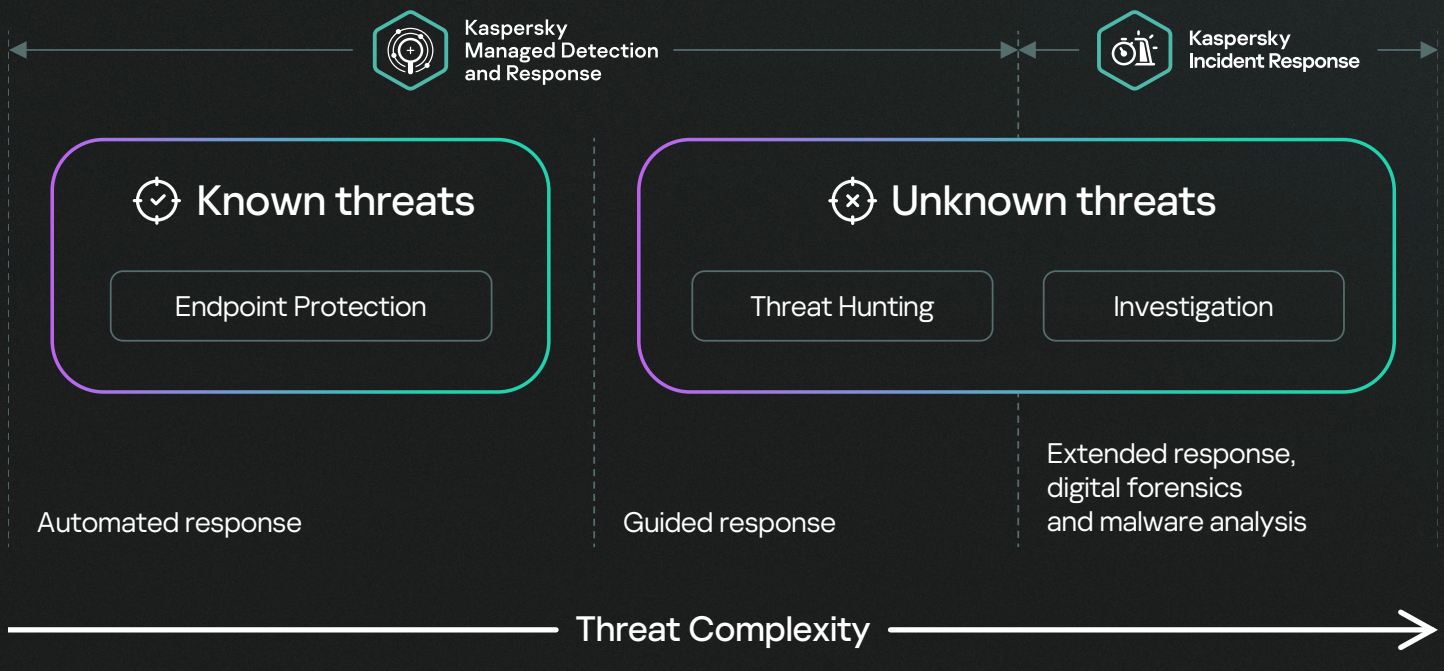
When combined with Kaspersky Incident Response, it covers the entire incident management cycle, from threat detection to post-attack remediation.

Kaspersky Incident Response

Kaspersky Incident Response obtains a detailed picture of the incident. The service covers the full incident investigation and response cycle: from early incident response and evidence collection to identifying additional traces of hacking and preparing an attack mitigation plan.

The synergy between Kaspersky MDR and Kaspersky Incident Response is seamless and user-friendly, supported by a team of experts who monitor your IT infrastructure around the clock and are ready to respond to cyberattacks of any complexity immediately.

The synergy between services



The main components of Kaspersky MDR

Kaspersky SOC

The team of global experts who deliver the service for almost a decade.

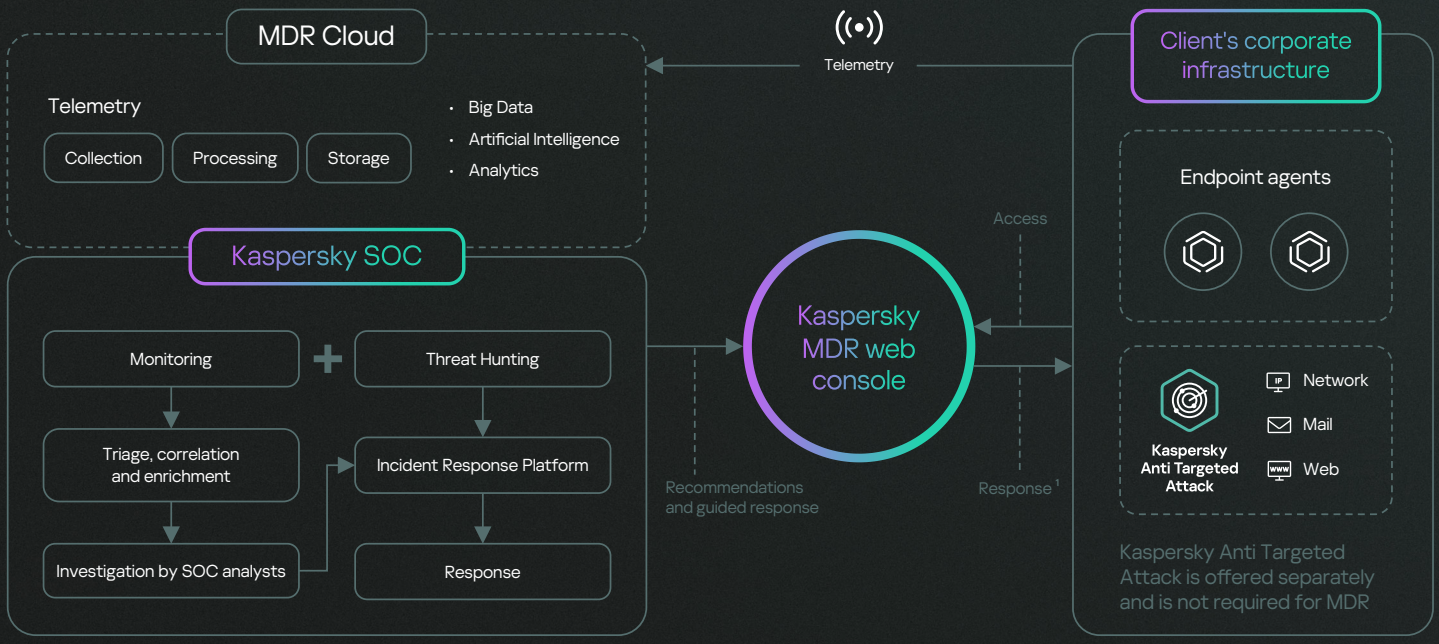
MDR console

Provides interface to manage and maintain the protection system of the customer network managed by Kaspersky MDR.

Endpoint Protection

A Kaspersky application that protects endpoints and the data stored on them from malware and other threats.

Kaspersky MDR architecture



How it works

1

Kaspersky Endpoint Security for Business (KESB) installed on the customer's premises captures and forwards telemetry data to the Kaspersky SOC.

2

Telemetry is analyzed by machine learning tools, with the direct involvement of Kaspersky SOC experts.

3

The Kaspersky SOC team investigates alerts and notifies the customer about any malicious activity, providing recommendations and step-by-step guided response.

[1] Automated response initiates when the customer approves it on the Kaspersky MDR console (If the customer does not do so, the MDR console will ask for the go-ahead before the automated response kicks in).

Kaspersky MDR features

Complete protection:

Feature	Description
 24x7 security monitoring	Kaspersky MDR provides around-the-clock monitoring of your IT environment, ensuring that any suspicious activity is identified and addressed promptly, regardless of when it occurs.
 Threat hunting	The service uses advanced analytics, machine learning, and Kaspersky threat intelligence to proactively search for signs of compromise within your infrastructure. Kaspersky MDR analysts conduct threat hunting activities in your environment to identify hidden threats that automated tools may miss.
 Guided and remote response scenarios	Once a threat is confirmed, Kaspersky MDR provides guided response procedures and can also perform remote response actions to mitigate the threat. If more in-depth response actions are required, Kaspersky Incident Response with digital forensics and malware analysis is available on request (separate purchase).
 Direct access to Kaspersky's expert teams	MDR customers have access to Kaspersky's SOC analysts for expert assistance during an incident. You just need to send a request on the communication tab of the incident. Our analysts provide additional insights, guidance, and support to ensure an effective response to complex threats. If Kaspersky Incident Response subscription is purchased, direct access to Global Emergency Response Team is also included for in-depth incident response and investigations.
 Submit incidents	If you suspect a compromise has occurred in your environment, you can manually report incidents on the Kaspersky MDR console. This is especially useful when a customer notices unusual activity that may not trigger automated alerts, or when insider knowledge suggests something is amiss that external monitoring may not detect.
 Compatibility with third-party EPP applications	This configuration allows installing third-party EPP applications and deploying Kaspersky Managed Detection and Response solution in the infrastructure of the organization.

Enhanced visibility and awareness:

Feature	Description
User-friendly MDR dashboards	Dashboards provide information about active incidents, assets, responses and the right tools to work with them, delivering real-time situational awareness.
Asset visibility	This feature provides clear visibility into all assets within your network, to ensure that all endpoints are accounted for and protected.
MDR Health check	The MDR Health check feature enables you to check which assets are currently protected by Kaspersky MDR and which ones have not been sending telemetry for a certain period of time.
Manage the solution through REST API	To retrieve data from Kaspersky MDR, enabling integration with other systems or custom applications for further analysis or reporting. The REST API operates over HTTP and consists of a set of request/response methods. It enables you to manage Kaspersky MDR through a third-party solution, not only the MDR console.
User notification methods in MDR console	Users with the active status can receive notifications from Kaspersky Managed Detection and Response via email and/or Telegram about registered incidents and their updates.

Location of Kaspersky SOC analysts:

1. Russia
2. Middle East
3. Europe
4. Latin America
5. North America

We protect over 220,000 companies in nearly 200 countries and territories

Supported Kaspersky products

Scenario for Kaspersky MDR activation	Kaspersky products	What it delivers
Existing or new Kaspersky endpoint customers	• Kaspersky Endpoint Security for Windows • Kaspersky Endpoint Security for Mac • Kaspersky Endpoint Security for Linux	Full scale detection and protection of the customer's endpoints.
Existing or new customers with virtual infrastructures	• Kaspersky Security for Virtualization Light Agent for Windows • Kaspersky Security for Virtualization Light Agent for Linux	Full scale monitoring and protection of virtual machines.
Existing or new customers using Kaspersky Anti Targeted Attack	• Kaspersky Anti Targeted Attack • Kaspersky Endpoint Security for Windows • Kaspersky Endpoint Security for Mac • Kaspersky Endpoint Security for Linux	Kaspersky MDR receives critical incidents which can't be delivered by Kaspersky Endpoint Security, such as IPS/IDS/Sandbox detects. Kaspersky MDR allows KATA users to deal with advanced APT-detects from KATA.
New customer with third-party endpoint products	• Kaspersky Endpoint Security for Windows in EDR Agent configuration	Incident monitoring and detection without full antivirus protection.

The combination of products may vary between scenarios.

Kaspersky Endpoint Security for Windows in EDR Agent configuration

Kaspersky Endpoint Security for Windows can now be installed alongside third-party EPP applications in EDR Agent mode, which means that Kaspersky MDR can now be integrated into the customer infrastructure even if it doesn't have KESB. In this case, KES operates as a monitoring agent and doesn't provide endpoint protection capabilities.

To learn more follow the link.

What makes Kaspersky MDR stand out

Developed by a cybersecurity leader

Kaspersky is the world's largest independent IT security company. Our global presence and focus on threat intelligence and technology leadership underpin our technologies and solutions, which protect over 220,000 companies in nearly 200 countries and territories.

For the past 10 years, Kaspersky products participated in 927 independent tests and assessments and were awarded 680 first places.

Learn more

Renowned experts

Kaspersky SOC is a team of experts that have been detecting and investigating complex security incidents for organizations in every industry and different regions for almost 10 years. The team holds numerous certificates and accreditations.

Global presence and industry-wide coverage

Kaspersky MDR operates 24/7 all over the world and helps organizations of all sizes and industries with varying levels of IT security maturity.

Our customers are happy to share their success stories of using Kaspersky MDR.

Learn more

Transparency & actionable insights

The solution doesn't just provide alerts - it also offers actionable insights and recommendations on how to respond to and mitigate detected threats.

Every year we share publicly available MDR analytics covering major trends and the current threat landscape that our customers may face.

Learn more

Compatibility with third-party EPP

Kaspersky Endpoint Security for Windows can be installed alongside third-party EPP applications in EDR Agent mode.

Learn more

Wide OS support

All popular operating systems such as Windows, Linux and Mac are supported.

Windows | Linux | MacOS

Unique threat intelligence

Kaspersky MDR is based on several petabytes of threat data collected continuously around the world, and more than two decades of expert analysis. Kaspersky's intelligence sources are not limited to OSINT sources, and include proprietary technologies gathering intelligence on threats that are currently active in real environments.

Kaspersky Managed Detection and Response

Learn more

www.kaspersky.com

#kaspersky
#bringonthefuture