Continuously hunting, detecting and responding to threats targeting your enterprise

Kaspersky Managed Detection and Response

kaspersky bring on the future

Today's challenges

55%

of companies report that their owned devices were infected with malware[1]

20%

of companies face APT-threats[2]

18%

of respondents report that the cause of incidents in their company was due to a lack of qualified cybersecurity personnel[3]

$2.5 billion

extreme losses due to a successful cyberattack[4]

Boost your cybersecurity resilience with round-the-clock managed protection

Remote working, the rapid development of information exchange methods, the widening global skills gap and the growing number of cyberthreats capable of bypassing traditional automated prevention and detection controls are putting organizations of every size under relentless pressure. It's essential that they can respond quickly and effectively.

Kaspersky Managed Detection and Response (MDR) is a service offering round-the-clock managed protection against cyberthreats and sophisticated attacks that traditional automated security measures miss.

The service boosts the level of IT security for organizations of every size and in every industry. It gives customers with a lack of IT security expertise a turnkey service for rapid deployment, and for experienced teams with advanced cybersecurity expertise, it offers additional flexibility, enabling them to delegate incident detection and classification tasks to Kaspersky experts or get an additional professional opinion on incidents they've detected themselves.

Kaspersky MDR fortifies and improves organizations' resilience against cyberthreats, optimizing existing resources so you can focus your attention on other business issues and maximize IT security investments overall.

Key features

- 24/7 continuous monitoring and threat hunting
- Overview of all protected resources with their current status
- Automated and guided response
- Communicate directly with the SOC team about incidents
- REST API for integration with IRP / SOAR
- Web console with dashboards and reports
- Storage of raw telemetry for 3 months
- Submit incidents
- Compatibility with third-party EPP applications

[1] IT Security Economics, 2022
[2] Kaspersky MDR analyst report, 2023
[3] Kaspersky Human Factor 360 Report, 2023
[4] Global financial stability report. The Last Mile: Financial Vulnerabilities and Risks, 2024

Telemetry and alerts sources for Kaspersky MDR

- **Kaspersky Endpoint Security for Windows**
- **Kaspersky Endpoint Security for macOS**
- **Kaspersky Endpoint Security for Linux**
- **Kaspersky Virtualization Light Agent**
- **Kaspersky Anti-Targeted Attack**

How it works

1

Kaspersky SOC analysts investigate security alerts and proactively analyze telemetry events received from Kaspersky products installed in the customer's network. This telemetry is correlated with Kaspersky's cyberthreat intelligence - based on more than 25 year of experience investigating some of the world's most notorious cyberattacks and targeted campaigns - to identify known, new and emerging tactics, techniques, and procedures used by attackers. Unique IoAs enable the detection of hidden malwareless threats that mimic legitimate activity.

2

As part of the event handling process in Kaspersky MDR, artificial intelligence (AI) mechanisms help reduce the number of false positives and accelerate incident investigation by the SOC team.

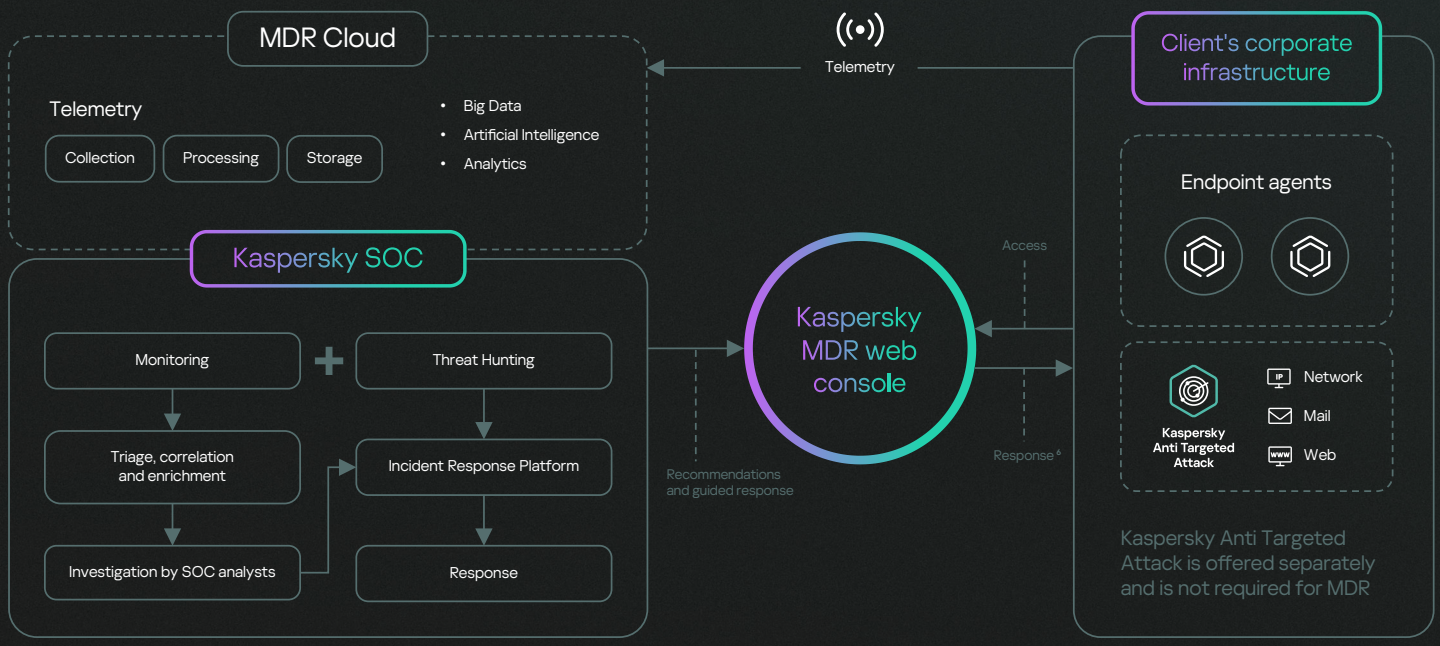
3

When a potential threat is detected, Kaspersky MDR classifies it by severity level and notifies the customer via email and / or Telegram. Where possible, root cause analysis helps identify the source of the attack and informs recommendations on how to contain, respond to and mitigate detected threats.

4

Customers can opt to partially or fully delegate response[5] capabilities to the Kaspersky SOC team. Any questions relating to the incident can be discussed with experts in a chat in the Kaspersky MDR web console.

Kaspersky MDR architecture



Kaspersky MDR is compatible with third-party antivirus solutions.

[5] If more in-depth analysis of incident is required and you have an active subscription to Kaspersky Incident Response, the incident can be handed over to the Kaspersky GERT team for investigation.

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

Value propositions

The peace of mind gained from having continuous protection against even the most complex, sophisticated threats

All the benefits of having your own SOC without the trouble and expense of establishing one yourself

Reduced security costs overall – no need to hire and train multiple, expensive IT security professionals to cover every base

Refocus your in-house IT security resources to deal with other business-critical issues

Global recognition and an unmatched track record

Kaspersky participates in a wide range of independent tests and works closely with leading global analyst firms. Kaspersky is globally recognized as a cybersecurity leader, and Kaspersky MDR, like all our products, has received numerous awards. The powerful detection and response features in Kaspersky MDR are complemented by the globally renowned expertise of one of the most successful and experienced threat hunting teams in the industry — the highly qualified and experienced Kaspersky SOC team.

Kaspersky Managed Detection and Response

Learn more

www.kaspersky.com

#kaspersky
#bringonthefuture