From reactive response to proactive approach in continuous cyber defense

Kaspersky Managed Detection and Response

Kaspersky Incident Response

kaspersky cybersecurity true to business

Attack duration and time needed for Incident Response[1]

Rapid 20h to respond	51%
Average 50h to respond	16%
Long-lasting 50h to respond	33%

Modern attacks outpace traditional response models

Today organizations face an increasing number of sophisticated threats, yet many security teams still operate in reactive mode — responding only after an incident has already occurred.

According to Kaspersky research, human-driven targeted attacks account for around 24% of all high-severity incidents.1 These attacks can bypass automated defenses and require continuous expert-led detection, investigation and response.

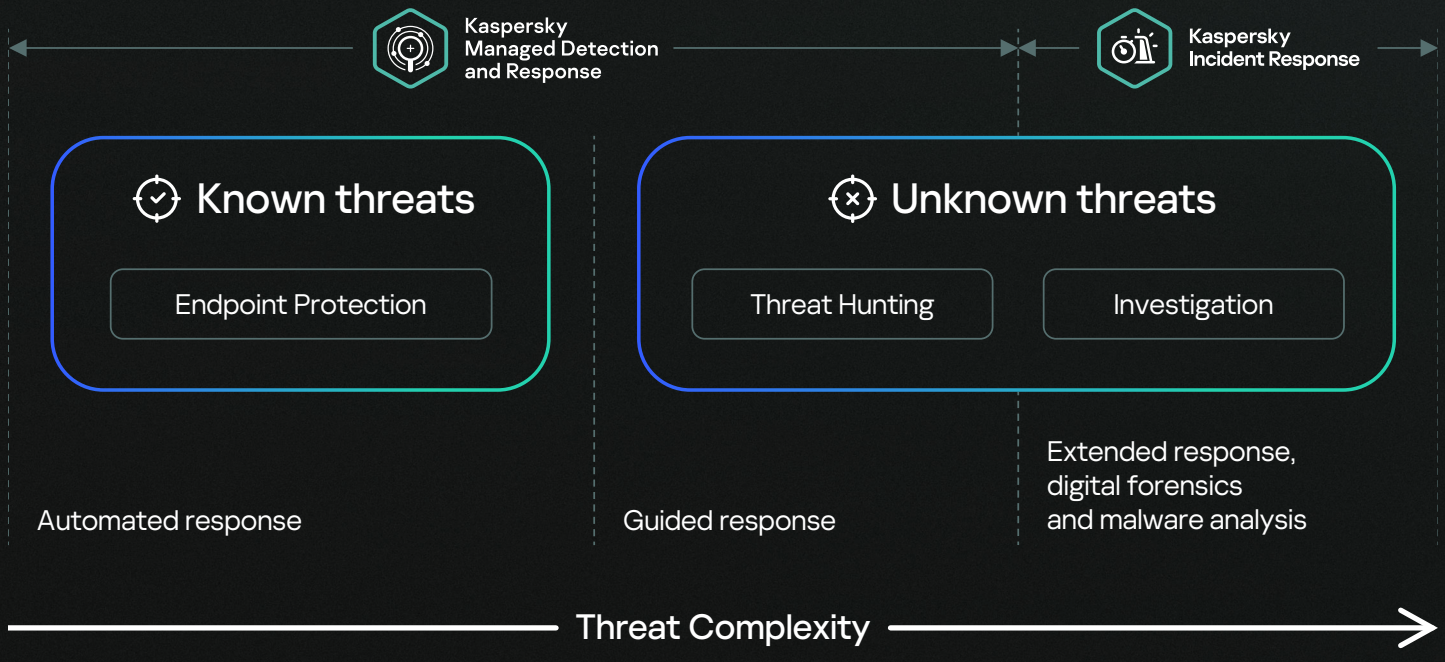
When Incident Response is used only as a reactive measure, investigation and containment often begin after suspicious activity has already escalated. By that time, attackers may have exploited vulnerabilities, established persistence or moved laterally across the environment.

This creates critical security gaps:

- Delayed detection of advanced attacks
- Longer attacker dwell time and higher impact
- Increased recovery costs and operational disruption
- Greater risk of data loss and compliance violations

To stay ahead of today's threat landscape, cyber defense must evolve from reactive response to continuous, expert-driven incident management.

Kaspersky Managed Detection and Response (MDR) and Kaspersky Incident Response (IR) close this gap by covering the full incident management lifecycle: from continuous threat detection and investigation to containment, remediation and post-attack recovery.



1 According to Anatomy of a Cyber World: Global Report by Kaspersky Security Services 2026

Full incident lifecycle protection

The combined Kaspersky MDR and Incident Response model creates a connected security process from 24/7 threat monitoring and expert investigation to incident containment, remediation and post-attack recovery.

How it works in practice

MDR detects, investigates, and initiates response

Kaspersky SOC analysts monitor security telemetry 24x7, enrich alerts with Kaspersky Threat Intelligence, classify threats by severity, and perform initial investigation and root cause analysis. AI Auto Analyst helps reduce false positives and accelerate event handling.

MDR conducts rapid containment (~30 min MTTR)

Response actions can be automated, pre-approved, manually approved through the MDR portal, and delivered as clear recommendations for the customer's security team.

Seamless escalation for complex incidents

Kaspersky MDR detects, investigates, classifies, and responds to threats across the whole infrastructure covered by the service. When a high-severity incident occurs or extends beyond the MDR coverage, the incident with all relevant information can be escalated directly from the MDR portal in just one click to Kaspersky Incident Response experts for further in-depth investigation, malware analysis and remediation guidance.

Together, the services reduce handover delays, accelerate containment and help organizations manage incidents across the full lifecycle and the whole infrastructure.

Kaspersky Managed Detection and Response

An expert-led service offering around-the-clock monitoring, detection, investigation and a rapid response to sophisticated cyberattacks — augmenting your existing security controls with human-led detection and global threat intelligence.

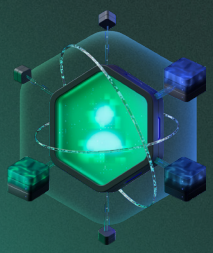
Learn more

Kaspersky Incident Response

The service covers the full incident investigation and response cycle, from initial response and evidence collection to identifying the primary attack vector and preparing an attack mitigation plan.

Learn more

Escalation is simple: all known incident context can be transferred, including telemetry, affected assets, indicators of compromise, investigation findings, and recommended actions. This gives IR experts a clear starting point and helps accelerate in-depth investigation, containment, recovery and mitigation planning.



Neither automated threat detection and prevention tools nor cyberthreat hunting alone is a silver bullet for the entire spectrum of today's threats. Only a combination of 24/7 proactive monitoring, detection and in-depth response can help organizations build stronger cyber resilience.

How Incident Response complements MDR capabilities

	MDR	IR
24/7 threat monitoring and detection	•	
Threat hunting, analysis and response based on Kaspersky products	•	
Standard incident report with recommendations	•	
Recovery coordination and guidance	•	•
Restores the full attack chain using Kaspersky products	•	•
Restores the full attack chain using the entire existing infrastructure, including third-party products		•
In-depth investigation, analysis and response based on the entire existing infrastructure		•
Digital forensics investigation		•
Malware analysis		•
24/7 direct phone number to IR experts		•
Tailored incident response report with recommendations		•

Why MDR and Incident Response are stronger together

Modern attacks develop across multiple stages, systems and infrastructure layers. MDR and Incident Response address different parts of this lifecycle.

Kaspersky MDR provides continuous 24/7 monitoring, threat hunting, investigation and rapid response across the infrastructure covered by the service. It helps identify suspicious activity early, validate threats, reduce false positives and initiate containment before the threat causes broader impact.

For high-severity incidents, Kaspersky Incident Response can extend the investigation beyond the MDR scope. IR experts analyze the full attack chain across the entire existing infrastructure, including third-party products; perform digital forensics and malware analysis; identify the root cause; and prepare tailored remediation recommendations.

Together, Kaspersky MDR and Kaspersky Incident Response create a connected approach to incident management: MDR helps detect and contain threats faster, while IR provides deeper investigation and recovery support when the incident requires broader expertise.

Expert teams

Kaspersky SOC

A cybersecurity operations center that provides 24/7 monitoring and continuous analysis of security data to ensure timely and accurate threat detection, as well as guided response actions and expert recommendations.

Global Emergency Response Team (GERT)

A team of internationally certified experts that has been investigating complex cybersecurity incidents across organizations of all industries and regions for more than a decade.

Benefits of MDR and Incident Response integration

From early detection to full-scope investigation

MDR helps detect and validate threats across the infrastructure covered by the service, while Incident Response can extend the investigation across the entire environment when a complex incident requires in-depth investigation.

Faster escalation with full available incident context

When IR involvement is recommended, MDR findings can be transferred directly from the MDR portal to IR experts, including telemetry, affected assets, indicators of compromise, investigation results and recommended actions.

Stronger containment decisions

MDR supports rapid response to detected threats, while IR experts provide deeper forensic analysis, malware analysis and attack-chain reconstruction to guide containment and remediation of complex incidents.

Reduced operational pressure during a crisis

MDR analysts handle continuous monitoring and alert investigation, while IR experts focus on high-severity incidents that require hands-on expertise.

Continuous improvement after every incident

Insights from IR investigations help strengthen MDR detection logic, threat intelligence, response playbooks and automated workflows, improving readiness for future attacks.

Konstantin Sapronov
Head of Global Emergency Response Team

> Anticipating risks and building resilience against business disruptions should start in advance of any incident

www.kaspersky.com

© 2026 AO Kaspersky Lab.
Registered trademarks and service marks are the property of their respective owners.

#kaspersky
#truetobusiness