kaspersky



Kaspersky
Managed Detection
and Response

We stop incidents before they stop your business

Kaspersky Managed Detection and Response is an expert-led service offering round-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. The service immediately strengthens your IT and OT security posture, regardless of your organization's size or industry.

Key benefits

Continuous advanced protection across your attack surface — endpoints, network, cloud and beyond — from day one.

A ready-to-use 24/7 SOC with a global team of experts — removing the need to build, staff and maintain your own in-house security operations.

A reduced workload for your internal security team, as you delegate monitoring, triage and investigation to us.

Outcome-driven security that combines human expertise, threat intelligence and AI to stop incidents before they can impact your business.

Boost your cybersecurity resilience with 24/7 managed protection

Remote working, the rapid growth of digital information exchange, the widening global skills gap and the rising number of cyberthreats capable of bypassing traditional automated controls are putting organizations of every size under relentless pressure. In this environment, responding quickly and effectively to every incident is critical.

An overview of today's cyberthreats[1]

1 Initial attack vectors



31% valid accounts



13% trusted relationship



39% exploit of a public-facing application

2 Move around and get things done

Attackers often use legitimate tools (such as Mimikatz, PsExec, SoftPerfect Network Scanner) in infrastructures that lack proper system configuration controls.



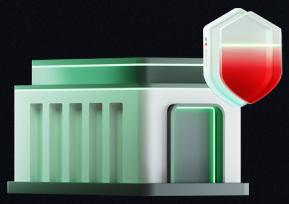
3 Impact

42% files encrypted

17% data leakage

11% persistence installed for future impact

Evidence shows that attackers frequently return after a successful attack.



Attack duration



Rapid	Average	Long-lasting
45%	20%	35%
up to 1 day	13 days	253 days

> Kaspersky MDR successfully detected and halted a zero-day attack that could otherwise have caused severe disruption to our operations.

GTO Grandeza de México

Daniel Huerta Santos
Cybersecurity Manager, Guanajuato State Government

Read more

1 Kaspersky MDR and Incident Response report

What Kaspersky MDR delivers

Continuous protection against advanced threats from day one

Kaspersky MDR activates in minutes with no additional infrastructure required, using our SOC analysts and threat intelligence to deliver multi-layered detection across multiple domains. Informed by billions of telemetry signals, it enables proactive threat hunting, root-cause investigation, and full, rapid remediation — protecting against known and zero-day threats from day one.

Use cases

- Turnkey 24/7 protection for organizations without SecOps
- Co-managed SecOps to augment in-house cybersecurity teams
- Advanced protection for OT infrastructure
- Dedicated ongoing protection of embedded systems

Security operations led by experts, enhanced by intelligence

With Kaspersky MDR, your security operations are managed by global experts with deep frontline experience and industry-leading certifications. Their work is amplified by market-leading Threat Intelligence and AI mechanisms embedded in the service, helping enrich every alert, accelerate detection and reduce Mean Time to Respond (MTTR).

30-minute
that's our average MTTR[2]

30%
of all received alerts processed by AI Auto Analyst[1]

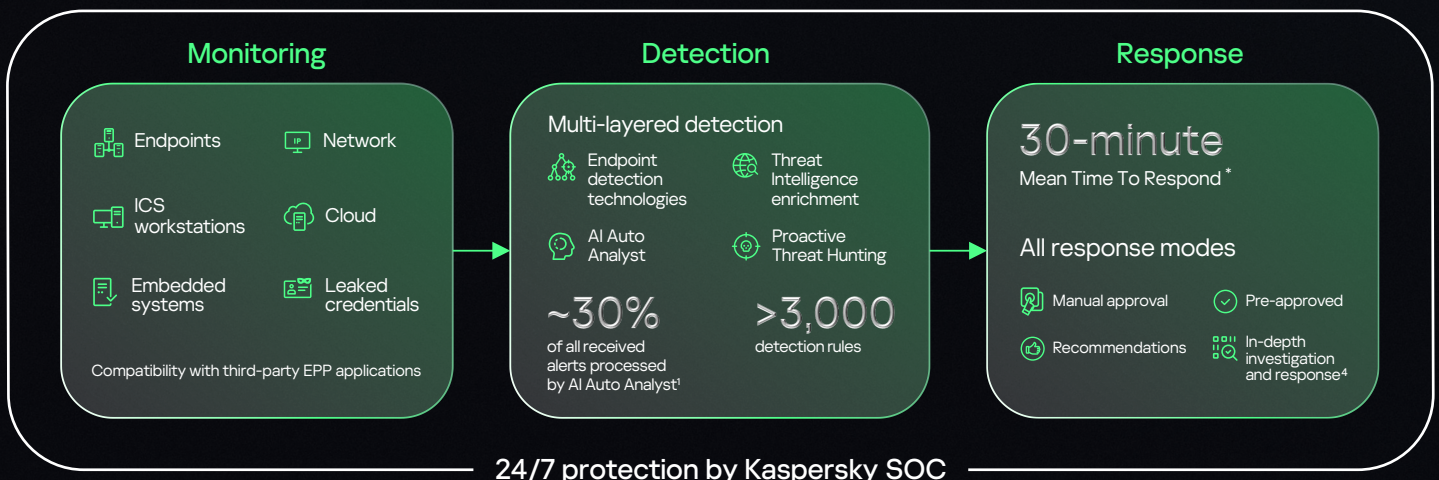
Operational efficiency and cost predictability

- Kaspersky MDR eliminates the complexity and cost of building an in-house SOC from scratch — a process that can drain your budget and delay meaningful security improvements for months or even years.
- If you already have your own SOC, the service takes on the burden of 24/7 monitoring, alert triage and incident classification, freeing your analysts to focus on higher-value, strategic work.

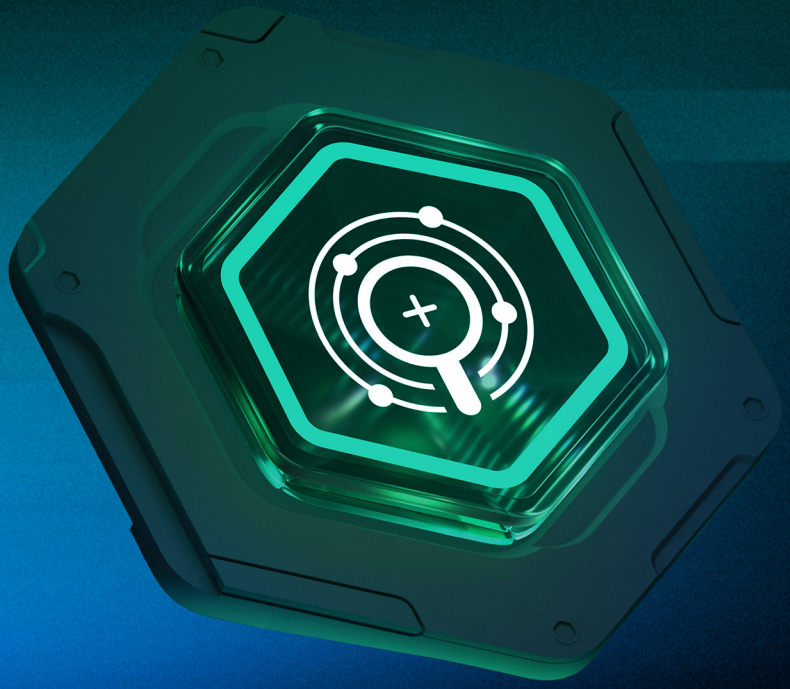
up to 15 minutes
is how long it takes to activate Kaspersky MDR

up to 2 years
is how long it takes to build in-house security operations from scratch

70%
of security teams struggle to keep up with the number of alerts generated by their security tools[3]



2 According to our annual MDR analyst reports
3 A portrait of the modern information security professional, 2024
4 If Kaspersky Incident Response Retainer is purchased



Kaspersky Managed Detection and Response

Schedule a demo

www.kaspersky.com

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

#kaspersky
#bringonthefuture