Kaspersky Endpoint Detection and Response

kaspersky BRING ON THE FUTURE

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.

With Kaspersky EDR, your organization can:

- Efficiently **MONITOR** threats – beyond malware
- Effectively **DETECT** threats – using advanced technologies
- Centrally **AGGREGATE** raw data and verdicts
- Rapidly **RESPOND** to attacks
- **PREVENT** malicious actions by discovered threats

... all via an intuitive web-interface that makes it easier to investigate and react.

Kaspersky EDR and key takeaways from IDC's Endpoint Security 2020 report*

- A weak EPP solution will destroy the value of an EDR tool

  Kaspersky offers powerful complete endpoint defenses (EPP+EDR) via a single agent

- People and time thus become the new ROI metric for EDR tools

  Kaspersky applies high levels of automation to complex issues, freeing up your security experts' valuable time

- EDR must leverage data that is outside of the endpoints

  Kaspersky boosts EDR effectiveness by adding advanced mail- and web-based threat discovery and visibility through a single tool

Boost your endpoint defenses first

For cybercriminals, corporate endpoints, where data, users and corporate systems all come together to generate and implement business processes, remain the primary target. To protect your corporate endpoints and prevent them being used as entry points into your infrastructure, your IT-security team should be reviewing ways to boost your existing security. Implementing the full endpoint protection cycle, from automatic common threat blocking to responding swiftly and appropriately to complex incidents, requires preventive technologies supplemented by advanced defense capabilities.

Kaspersky Endpoint Detection and Response (EDR) provides powerful security with comprehensive visibility across all endpoints on the corporate network together, with superior defenses, enabling the automation of routine tasks to discover, prioritize, investigate and neutralize complex threats and APT-like attacks.

Highlights

- Kaspersky EDR enhances our most tested, most awarded flagship Endpoint Protection Platform (EPP) – **Kaspersky Endpoint Security for Business –** with powerful EDR capabilities, further strengthening your overall security levels. A single agent for automatic protection against common threats and advanced defenses against complex attacks simplifies incident handling and minimizes maintenance requirements. There's no additional burden on endpoints and no further costs – just the knowledge that your workstations and servers are fully protected against the most sophisticated and targeted threats.

- Kaspersky EDR reduces the time needed for initial evidence collection, provides full telemetry analysis and maximizes the automation of EDR processes, cutting overall incident response times without the need to attract additional IT security resources.

- Kaspersky EDR can be absorbed into the **Kaspersky Anti Targeted Attack Platform**, combining EDR capabilities and network-level advanced threat discovery. IT security specialists have all the tools they need to handle superior multi-dimensional threat discovery at both endpoint and network levels, applying leading-edge technology, undertaking effective investigations, and delivering a rapid, centralized response — all through a single solution.

* IDC PERSPECTIVE, Endpoint Security 2020: The Resurgence of EPP and the Manifest Destiny of EDR

Kaspersky EDR is ideal if your organization wants to:

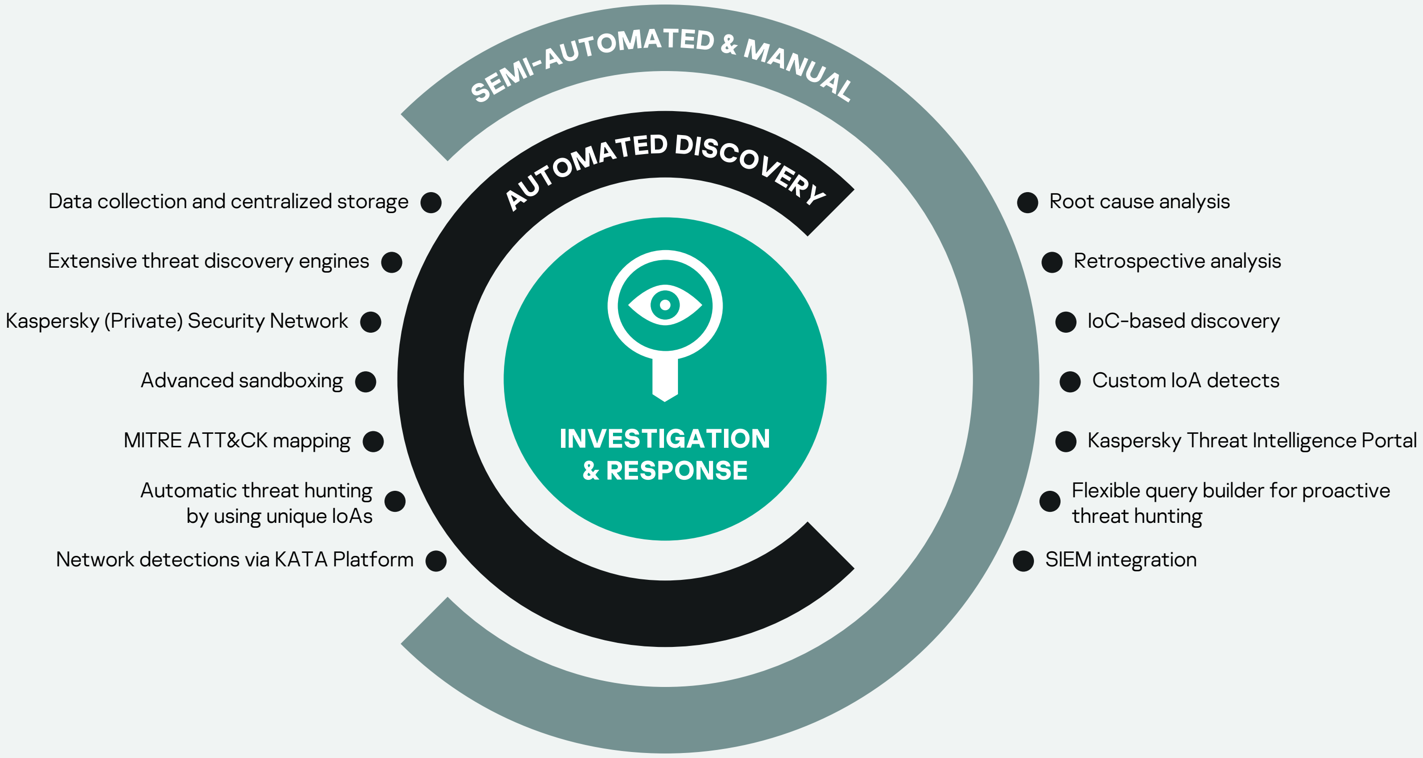
- Upgrade your security with an easy-to-use, enterprise solution for incident response
- Automate threat identification & responses – without business disruption during investigations
- Enhance your endpoint visibility & threat detection via advanced technologies
- Understand the specific Tactics, Techniques,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

Rapidly uncover and contain the most sophisticated threats

Kaspersky EDR provides high-level endpoint protection and increases SOC efficiency, delivering advanced threat discovery and 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 Indicators of Attack (IoAs), MITRE ATT&CK enrichment and a flexible query builder, plus access to our Threat Intelligence Portal knowledge base - all these facilitate effective threat hunting and fast incident response, leading to damage limitation and prevention.

Use cases:

- Proactive search for evidence of intrusion over your entire network
- Rapid detection and remediation of an intrusion – before the intruder can cause major damage and disruption
- Rapid investigation and centralized management of incidents across thousands of endpoints with a seamless workflow
- Validation of alerts and potential incidents discovered by other security solutions
- Automation of routine operations – to help minimize manual tasks, free up your resources and reduce the likelihood of 'alert overload'


SEMI-AUTOMATED & MANUAL
AUTOMATED DISCOVERY
INVESTIGATION & RESPONSE
Data collection and centralized storage
Extensive threat discovery engines
Kaspersky (Private) Security Network
Advanced sandboxing
MITRE ATT&CK mapping
Automatic threat hunting by using unique IoAs
Network detections via KATA Platform
Root cause analysis
Retrospective analysis
IoC-based discovery
Custom IoA detects
Kaspersky Threat Intelligence Portal
Flexible query builder for proactive threat hunting
SIEM integration

Gartner Peer Insights Customers' Choice for EDR Solutions 2020 names Kaspersky Top Vendor

Kaspersky is one of only 6 vendors worldwide to receive the Gartner Peer Insights Customers' Choice recognition for Endpoint Detection and Response solution in 2020, with the highest rating of any vendor for our service and support - the ultimate customer compliment for Kaspersky EDR.

Gartner disclaimer

Gartner Peer Insights Customers' Choice constitute the subjective opinions of individual end-user reviews, ratings, and data applied against a documented methodology; they neither represent the views of, nor constitute an endorsement by, Gartner or its affiliates.

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.

Know more at kaspersky.com/MITRE

Kaspersky EDR business benefits across the enterprise:

- Helps eliminate security gaps and reduce attack 'dwell time'
- Automates manual tasks during threat detection and response
- Frees up IT and IT security personnel for other crucial tasks
- Simplifies threat analysis and incident response
- Reduces the time taken to identify and respond to threats
- Helps enable full compliance

And if you want even more… Kaspersky Managed Detection and Response

Adding a fully managed and individually tailored round-the-clock defenses to Kaspersky EDR means your IT-security resources can be conserved by offloading incident-related processing tasks to Kaspersky, or looking to us for expert judgements and unique threat hunting expertise when your in-house team lacks sufficiently qualified security specialists to meet specific scenarios.

To find out more about Kaspersky EDR, visit:

kaspersky.com/enterprise-security/endpoint-detection-response-edr

Cyber Threats News: securelist.com
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tommorow.

Know more at kaspersky.com/transparency

**Proven.
Transparent.
Independent.**