Kaspersky Enterprise Cybersecurity

Kaspersky Endpoint Detection and Response

Enterprises are improving their security strategy for responding to advanced threats and modern cyberattacks. For cybercriminals, endpoints are still the main target – but today's threats are sidestepping traditional endpoint security measures, disrupting business-critical processes, damaging productivity and increasing operating costs.

Delays cost money

Initiating recovery one week after the discovery of an incident costs an enterprise 200% more, compared with immediate response.
Kaspersky Lab Corporate IT Risks Survey

Kaspersky EDR is ideal for organizations that want to:

- Automate threat identification & response – without disruption to the business
- Improve endpoint visibility & threat detection – via advanced technologies, including ML (Machine Learning), Sandbox, IoC scan & Threat Intelligence
- Empower security improving – with an easy-to-use, enteprise solution for Incident Response
- Establish unified and effective Threat Hunting, Incident Management and Response processes.

Aiding compliance:

Real-time Threat Intelligence sharing via on premise Kaspersky Private Security Network.

- No cloud reliance and outbound data flow via KPSN integration.
- All forensics data is centrally stored within Kaspersky EDR on enterprise's own environment.

Actively Hunting Threats:

By adding 24/7 Threat Hunting service – Kaspersky Managed Protection – to a Kaspersky EDR deployment, enterprises gain access to global threat research.
In addition, Kaspersky Lab threat researchers can:

- Review data collected in the enterprise's environment;
- Rapidly notify the enterprise's security team – if malicious activity is detected;
- Provide advice on how to respond and remediate.

Highlights

Adaptive Threat Response

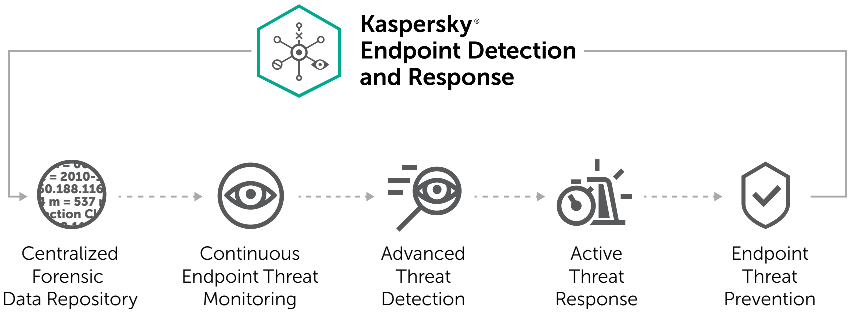
Kaspersky EDR includes a vast array of automated responses that help enterprises to avoid the use of traditional remediation processes – such as wiping and reimaging – that can result in expensive downtime and loss of productivity.

Proactive Threat Hunting

With fast-search, using a centralized database – plus Indicators of Compromise (IoC) search – Kaspersky EDR can radically change security workflow. Instead of having to wait for alerts, your security team can actively hunt for threats – proactively scanning endpoints to spot anomalies and security breaches.

Intuitive Web-Interface

Kaspersky EDR's easy-to-use, browser-based interface gives security personnel unified visibility and control of: Detection, Investigation, Prevention, Alerting and Reporting. Because a vast range of functions can be monitored and controlled via a single interface, your security team can perform security tasks more effectively and efficiently – without having to flip between separate tools and multiple consoles.



Kaspersky® Endpoint Detection and Response
Centralized Forensic Data Repository
Continuous Endpoint Threat Monitoring
Advanced Threat Detection
Active Threat Response
Endpoint Threat Prevention

Rapidly uncover and contain advanced threats

Kaspersky Endpoint Detection and Response (Kaspersky EDR) helps enterprises to detect, investigate and respond:

- Improving visibility over endpoints
- Automating manual response tasks
- Boosting investigation capabilities

... and it's compatible with traditional endpoint security solutions.

Kaspersky EDR helps security teams – and less experienced responders – to triage an endpoint with the precision of a cyber-response specialist. With Kaspersky EDR, your organization can:

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

... all via a powerful web-interface that makes it easier to investigate and react.

Use cases:

- Proactive search for evidence of intrusion – including indicators of compromise (IoC) – over an entire network in real time
- Rapid detection and remediation of an intrusion – before the intruder can cause major damage and disruption
- Integration with SIEM – to help correlate alerts plus activity at the endpoint
- Validation of alerts and potential incidents discovered by other security solutions
- Rapid investigation and centralized management of incidents – across thousands of endpoints – with seamless workflow
- Automation of routine operations – to help minimize manual tasks, free up resources and reduce the likelihood of ‘alerts overload‘.

Advanced endpoint security

Kaspersky Lab demonstrates our continuing leadership in endpoint protection by combining in one single solution five crucial elements:

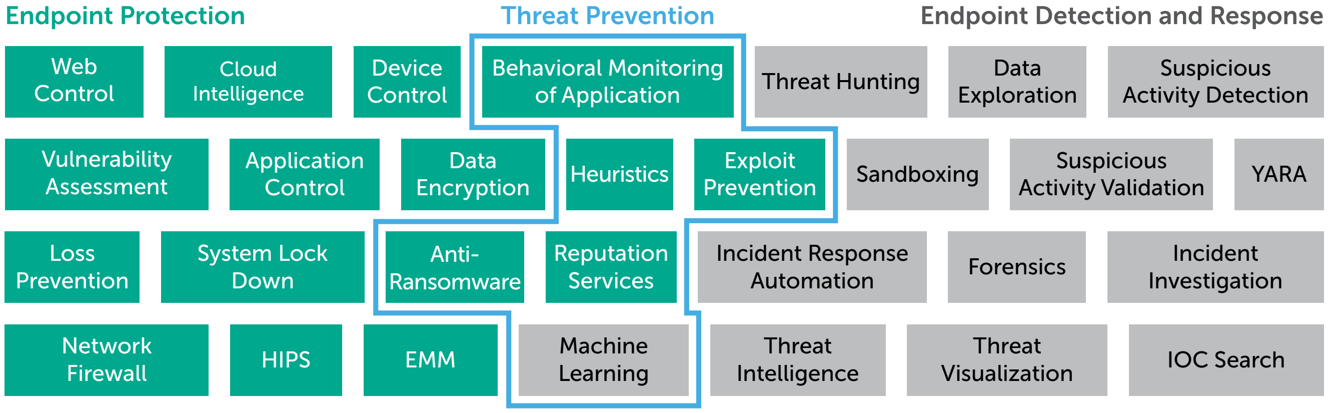
- A powerful, next-gen anti-malware engine – with machine learning
- Endpoint detection and response (Kaspersky EDR)
- A 24/7 threat hunting service – Kaspersky Managed Protection
- Real-time threat intelligence access – via Kaspersky Security Network
- Advanced endpoint controls (device/web/app, encryption and more).

Empowering traditional endpoint security

Because Kaspersky EDR is compatible with a wide range of traditional security products – from various vendors – it can also work alongside an enterprise’s existing endpoint security, helping to add:

- Next-Gen functionality – for advanced detection and prevention;
- Centralized investigation and response processes.

... without the enterprise having to replace its current security solution.



Endpoint Protection

Threat Prevention

Endpoint Detection and Response

Web Control

Cloud Intelligence

Device Control

Behavioral Monitoring of Application

Threat Hunting

Data Exploration

Suspicious Activity Detection

Vulnerability Assessment

Application Control

Data Encryption

Heuristics

Exploit Prevention

Sandboxing

Suspicious Activity Validation

YARA

Loss Prevention

System Lock Down

Anti-Ransomware

Reputation Services

Incident Response Automation

Forensics

Incident Investigation

Network Firewall

HIPS

EMM

Machine Learning

Threat Intelligence

Threat Visualization

IOC Search

Object analysis in an isolated, virtual environment

Kaspersky EDR includes an on-premise Advanced Sandbox that provides automated extraction of any file – on any endpoint – for deep analysis. It effectively gives the enterprise an in-house virus lab – without sending any data outside the network.

Advanced Detection – with Machine Learning

Kaspersky EDR’s machine learning engine – Targeted Attack Analyzer (TAA) – creates a baseline of endpoint behavior. This enables a historical record that can be used to discover how a breach occurred. In addition – by correlating forensic data, threat intelligence and security engine verdicts – it helps to detect anomalies.

Business benefits across the enterprise:

Reduces costs

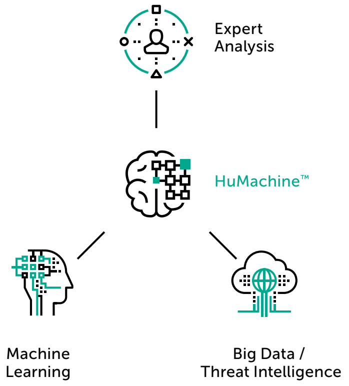
- Automates manual tasks – during threat detection and response
- Helps speed up threat containment – to save money and resources
- Frees up IT and security personnel for other tasks
- Helps minimize business disruption during investigations

Speeds return on investment

- Enables efficient workflow
- Reduces the time to identify and respond to threats
- Helps to enable compliance – (PCI DSS and more) – by enforcing endpoint logs, alerts review and documentation of investigation results

Mitigates attack risks

- Helps to eliminate security gaps and reduce attack ‘dwell time’
- Simplifies Threat Analysis and Incident Response
- Empowers existing security with threat validation



Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com