Expand your Endpoint Security without expending resources

Industry- and customer-acclaimed cybersecurity technologies, with EDR at their core, empower you to detect and prevent evasive attacks at lightning speed – with no additional demands on your team.
A fully automated solution, with EDR at its core

Cyberattacks are rising year-on-year in terms of their numbers, level of complexity and their financial impact. And this isn’t a problem that’s going to go away on its own.

This is a fact, and it’s also a fact that the main target for cybercriminals right now is your endpoints.

So how do you deal with this?

By building strong, responsive endpoint security, which we believe means employing process automation and adopting a multi-layered approach:

- Visibility across all endpoints
- Root cause analysis
- IoC scan
- Range of response actions
- Enhanced anti-malware
- Vulnerability and patch management
- Strong EPP

EDR

- Suspicious object emulation
- Shared verdict cache
- Create or import an IoC for scanning
- Automated response
- Extended hardening
- Behavior analysis
- Data protection

The chances of catching a threat are that much higher if you’re armed with a number of different ways to detect and prevent attacks. Our new automated detection and response technologies mean that very large numbers of incidents can be dealt with fast and effectively without human involvement, leaving IT Security Specialists free to focus only on those that really require their expertise.

This approach means you can:

- Reduce your risk of falling victim to a targeted attack
- Harden your systems and prevent employees from exposing themselves, and you, to an attack
- Maximize the number of incidents processed, without increasing your manpower costs

We’ve created an integrated solution for endpoint security with three components: Endpoint Protection Platform (EPP), a Sandbox, and Endpoint Detection and Response (EDR).

We’re not just claiming to be good at what we do – we have the results, agency ratings and happy customers to prove it.

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. https://www.gartner.com/reviews/customers-choice/endpoint-protection-platforms

Cybersecurity you can trust

Our Integrated Endpoint Security solution comprises tightly-integrated layers of tools and technologies essential to effective endpoint protection, detection and response.

**Robust endpoint protection and control**

**Kaspersky Endpoint Security for Business** provides robust protection based around one of the best anti-malware engines on the market. The risk of human error is minimized by systems hardening and by automating routine tasks such as Vulnerability and Patch Management, OS and 3rd party software installation. And our Security Policy Advisor feature monitors modifications to optimized security settings, alerting administrators to any potentially negative consequences.

**Defense against complex threats**

**Kaspersky Sandbox** complements endpoint protection with functionality that can easily detect even new, unknown and complex threats that are specifically designed to bypass even the most sophisticated protection technologies. It does this by creating a virtualized environment, where suspicious objects are sent, analyzed with a variety of methods (like simulating user activity, behavior analysis, monitoring outgoing connections, etc), and their reputation recorded. If an objects are identified as malicious, the whole infrastructure can be scanned and their malicious activity prevented, ensuring an automated response across all endpoints.

**Automated visibility and response**

**Kaspersky Endpoint Detection and Response Optimum** is an EDR tool working together with endpoint protection and providing endpoint visibility, root cause analysis capabilities and varied response options. It brings a powerful yet highly automated layer of defense to the integrated solution, provides attack spread path visualization, and delivers full information on the incident, the host, suspicious objects etc.
Solution highlights

**Protect against modern threats**
Prevent disruption and damage to the business by reducing your risk of both commodity and more complex cyberthreats

**Lower the risk from human factors**
Reduce the opportunity for human error by employing granular controls and automation

**Minimize team workload**
Maximize your ROI by automating tasks, so you can process more incidents without any increase in manpower costs

%  

A high Return on Investment

Forrester’s TEI interviews with customers and their subsequent report found that organizations using our solution experienced an average ROI of 441%.

Experience for yourself

Visit this page to request free demo of the solution.

The bigger picture – Kaspersky IT security products for business

Endpoint protection, though critical, is just the beginning. Whether you operate a best-of-breed or single-source security strategy, Kaspersky offers products for hybrid cloud infrastructures and for legacy Windows XP systems that interlock or work independently, so you can pick and choose without sacrificing performance efficiency or freedom of choice. Learn more on our website.