kaspersky BRING ON THE FUTURE

Kaspersky Optimum Security

Achieve your optimum level of cybersecurity with managed protection and cloud-enabled endpoint detection and response

The challenge

You need to be able to defend your business effectively against new, unknown and evasive threats, without straining your limited time and resources.

30% of successful cyberattacks involve legitimate system tools[1]

Advanced attacks are on the rise

Today's evasive threats – designed to effectively bypass traditional endpoint protection - bring much more significant risks for business than before now that attacks are becoming harder to detect, analyze and respond to. If an undetected threat takes root in your infrastructure, you could face significant losses, impacting on the business's bottom line:

- interruption of business-critical processes
- significant reputational damage and loss of customers
- fines, penalties and lost profits.

Endpoint protection has to be strengthened

Today's evasive attacks have become much more effective, due to criminals using legitimate system tools and other ready-made methods and technologies, enabling them to gain access, persist and perform malicious actions inside your infrastructure faster and undetected.

This situation is further exacerbated by the dissolving perimeter and the growth of remote working, which puts endpoints – traditionally the most attractive entryway into your infrastructure – even more in the spotlight.

And resources are stretched thin as it is

To provide the extra edge that endpoint security now requires, adequate incident response capabilities need to be developed inside your organization.

But the associated costs of a project like this can quickly get out of hand:

- software and hardware costs can both add up
- siloed and fragmented security tools and processes mean security efficiency gets eroded
- a lot of time can end up being wasted on routine tasks.

The solution

Kaspersky Optimum Security delivers an effective threat detection and response solution backed by 24/7 security monitoring, automated responses and threat hunting, together with support and guidance from Kaspersky experts.

45% of attacks were detected due to suspicious files or suspicious endpoint activity[1]

Advanced threat protection

Reach the optimal balance between simplification and effectiveness, human intelligence and automation, efficiency and functionality - without gambling on your protection!

Kaspersky Optimum Security helps you slash the risks of losing money, customers and your reputation, and fortifies your defenses against new, unknown and evasive threats. So you're ready to face today's rapidly evolving threat landscape.

Fast and scalable turnkey solution

Automatic prevention methods are the foundation of any endpoint protection, but they must be complemented with advanced tools if you want to be able to deal with the more dangerous evasive threats.

Kaspersky Optimum Security provides advanced detection and swift response capabilities – all delivered together from the cloud. Your cybersecurity engineers can now tackle even the threats that used to keep them up at night, with speed and precision.

Optimum investment levels

You don't need to hire more people, re-train staff, or get bogged down with complicated deployment – Kaspersky Optimum Security simplifies and helps automate crucial incident response processes – according to your specific requirements.

It adapts to your needs with on-prem and cloud options and a scalable turnkey security toolset which helps you keep IT system complexity down, user productivity up and implementation costs transparent.

Key benefits

- Stay ahead of the curve and defend your business against the real risk of damage and disruption from the latest wave of lethal evasive threats
- Develop your own incident response capability with a simple to use Endpoint Detection and Response (EDR) toolset
- Lower infection risks significantly by training your employees and raising their security awareness
- Conserve precious resources through operations automation and managed functionality
- Save time and effort with a solution whose diverse features are all managed in a single cloud or on-prem console

Main capabilities

Kaspersky Optimum Security offers a wide range of essential functionality for protection against evasive threats, at the core of which lies detection, analysis and response.

55% of attacks took weeks or longer to detect[1]

Advanced detection

- Machine learning-based behavior analysis algorithms to quickly and accurately expose suspicious behaviors
- Automated threat hunting based on proprietary Indicators of Attack to find concealed complex threats, supported by Kaspersky experts
- Adaptive anomaly control to automatically adjust the configuration of attack surface reduction tools to users' profiles

Simplified investigation

- All information pertaining to an incident is automatically gathered in a single incident card
- Visualization and a straightforward investigation process allow you to quickly and efficiently analyze the incident in a single environment and decide on a further course of action
- At the same time, all detections by Indicators of Attack are prioritized and investigated by Kaspersky to provide you with tailored recommendations

Automated response

- 'Single-click' response allows you to quickly contain an individual incident
- Guided response based on Kaspersky experts' experience means you can take on even the more complex and dangerous threats
- Automated cross-endpoint response helps you find and respond to analyzed or imported threats across the network

How to apply it

As Kaspersky Optimum Security includes a number of tools and major capabilties which together can be effectively used to prevent, detect and respond to threats at various stages of an attack:

Penetration

The user receives a phishing email or accesses a malicious web resource, infecting their host

Installation

Initial infection deploys necessary components, communicates with C&C[1] and explores its surroundings

Rooting

A range of tools is used – including legitimate and system-native ones – to gain persistence and start horizontal movement if needed

Employee security awareness

Attack surface reduction

Automatic threat prevention

Advanced detection mechanisms, including ML-based behavior analysis and sandbox

Automated threat hunting with IoAs[2]

Root cause analysis and IoC[3] scanning

Automated, guided and remote response scenarios

[1] Command and control
[2] Indicators of Attack
[3] Indicator of Compromise

Further protection

You can further enhance your defenses with a variety of tools aimed at different aspects of your security – detection, investigation and awareness.

Malicious emails were a part of 31% of successful cyberattacks, meaning many of them could've been prevented by employees themselves[1]

Additional detection layer

Expose new and unknown threats even more quickly and reliably with **Kaspersky Sandbox** – analyzing threats automatically in an isolated environment, using patented detection algorithms and anti-evasion techniques. Configured responses are applied automatically to discovered threats, significantly raising your detection capabilities without requiring any management beyond initial deployment.

Added edge to investigations

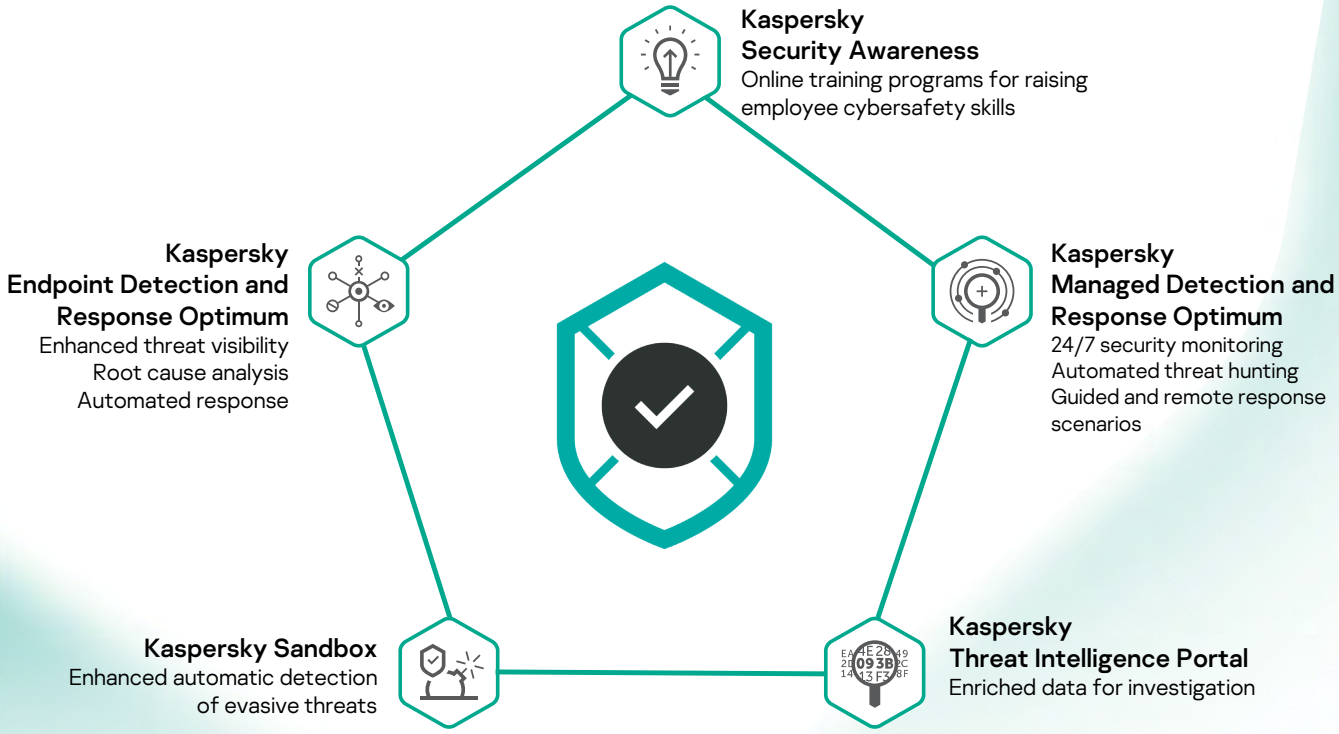
Help your cybersecurity specialists analyze and understand threats more thoroughly and quickly with the latest information on files, hashes, IPs and URLs associated with threats. Gain this extra insight with no additional cost from the easy-to-use **Kaspersky Threat Intelligence Portal**.

People are the key to your security

The key to reducing your attack surface and the number of incidents is training your employees to be aware of the cyberthreats they can unleash on your infrastructure through negligence or a simple lack of knowledge. **Kaspersky Security Awareness** builds the knowledge and skills all employees need to help protect your infrastructure, so they're actively working with you to maintain a cybersafe environment.

How it works

You can choose how to use Kaspersky Optimum Security - as a managed solution to achieve 24/7 protection, as an easy-to-use EDR toolset, or as a mix of both, taking advantage of the experience and knowledge of Kaspersky experts while developing your in-house detection and response capabilities. Kasperky Optimum Security unites several products under a single solution:



In operation

You'll find Kaspersky Optimum Security straightforward to administer from a single console, making the very most of your limited time and resources.

56% of respondents say their organizations are at risk due to cybersecurity staff shortage[2]

Full package

- Part of the Kaspersky security ecosystem, building up your defenses from security foundations to optimized advanced features
- The diverse features of Kaspersky Optimum Security can be managed through a single cloud console
- A solution with multiple layers of protection, addressing commodity and evasive threats as well as opportunities for human error

Ease of management

- The cloud management console allows quick and efficient control from anywhere in the world
- On-prem and cloud-based options provide the same admin experience
- Deployment is quick and hassle-free, whether or not you already use Kaspersky solutions
- All tools can be controlled and managed easily and intuitively, with no need for lengthy familiarization or retraining

Save time and resources

- Managed protection helps organizations with a lack of IT security staff or expertise to build detection and response capabilities without the associated security investments
- Crucial cybersecurity processes are automated, making incident response faster, more accurate and more efficient
- Better employee security awareness means less threats penetrate your defenses – generating fewer incidents for you to process!

Kaspersky's stage-by-stage approach

Together we can build your defenses based on reliable protection with Kaspersky Security Foundations, smoothly scaling up to essential incident response with Kaspersky Optimum Security - and eventually growing to the application of powerful tools aimed at protecting against the most advanced threats,with Kaspersky Expert Security.

Choose which stage is right for you:

Kaspersky Security Foundations

Automatically block the vast majority of threats

- Multi-vector automated prevention of incidents caused by commodity threats – the vast majority of all cyber-attacks.
- The foundation stage for organizations of any size and complexity in building an integrated defense strategy
- Reliable endpoint protection for those with small IT teams and emerging security expertise

Kaspersky Optimum Security

Build up your defenses against evasive threats for those who:

- Have a small IT security team with basic cybersecurity expertise
- Have an IT environment growing in size and complexity, increasing the attack surface
- Experience a lack of cybersecurity resources – in contrast to a need for enhanced protection
- Developing incident response capability has become increasingly important

Kaspersky Expert Security

Readiness for complex and APT-like attacks where:

- IT environments are complex and distributed
- The IT security team is mature or a Security Operations Center (SOC) is established
- Risk appetite is low due to higher costs of security incidents and data breaches
- Regulatory compliance is a concern

To find out more about how Kaspersky Optimum Security addresses cyberthreats while going easy on your security team and resources, please visit: http://go.kaspersky.com/optimum.

1 Kaspersky Incident Response Analyst Report 2019, Kaspersky, 2020
2 (ISC)2 Cybersecurity workforce study, (ISC)2, 2020

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com

www.kaspersky.com