kaspersky 25 years

Kaspersky Optimum Security

Stay ahead of the curve on evasive threats – with full EDR[1]/MDR[2] that won't strain your resources.

Kaspersky Optimum Security

30% of successful cyberattacks involve legitimate system tools

Kaspersky Incident Response Analyst Report, 2020

The challenge

Ransomware, malware and financial spyware have all become better at evading detection and are easy and cheap to buy through the darkweb - creating a perfect storm for many organizations today.

Advanced attacks are on the rise

Today's evasive threats are designed to effectively bypass traditional endpoint protection, bringing significant new risks for all businesses. 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 and data loss
- significant reputational damage and loss of customers
- fines, penalties and lost profits.

Endpoint protection has to be strengthened

These latest attacks **avoid detection** by hiding inside legitimate system tools and other readily available methods and technologies, using them to **gain access, persist and perform malicious actions inside your infrastructure, fast and undetected**.

Then there's remote working, puttingendpoints – 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 you now need, your organization must develop adequate incident response capabilities.

But a project like this can cost, bigtime:

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

45% of attacks were detected due to suspicious files or suspicious endpoint activity - making their detection a priority

As above

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.

Optimum protection

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

Kaspersky Optimum Security provides advanced detection based on **Machine Learning** and swift response capabilities – all delivered from the cloud. Your team can now tackle even the threats that used to keep you up at night, with speed and precision.

Optimum investment

No need to hire more people, re-train staff, or wrestle with complicated deployment – Kaspersky Optimum Security simplifies and helps automate crucial incident response processes – according to your specific requirements.

On-prem and cloud options and a scalable turnkey security toolset adapt to your needs, helping you keep IT system complexity down, user productivity up and implementation costs transparent.

Optimum balance

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.

Key benefits

- **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 EDR (Endpoint Detection and Response) toolset.
- **Take your detection to the next level with ease –** through powerful and hassle-free MDR (Managed Detection and Response).
- Lower your infection risks significantly by **training your employees and raising their security awareness.**
- Conserve precious resources through **operations automation and managed protection.**
- Save time and effort with a solution whose diverse features are all managed **in a single cloud or on-prem console.**

55% of attacks took weeks or longer to detect

As above

Main capabilities

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

Advanced detection

- **Machine learning-based behavior analysis** algorithms to quickly and accurately expose suspicious behaviors.
- **Automated threat hunting** based on proprietary Indicators of Attack (IoAs) to find concealed complex threats, all supported by Kaspersky experts.
- Adaptive Anomaly Control to **automatically adjust the configuration of attack surface reduction tools** based on your users' profiles.
- Cloud detection, including an **in-built cloud sandbox**.

Straightforward analysis

- All information relating to an incident is automatically gathered in **a single incident card**.
- **Visualization and a straightforward investigation** process mean you can quickly and efficiently analyze the incident in a single environment, then 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 our expert 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.

What's inside

Choose how you 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:

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

As above

But wait – there's more...

Further enhance your defenses with tools aimed at different aspects of your security – detection, investigation and awareness.

Educate your users

The key to reducing your attack surface and the number of incidents is training 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.

Get the latest information

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 at no additional cost from the easy-to-use **Kaspersky Threat Intelligence Portal**.

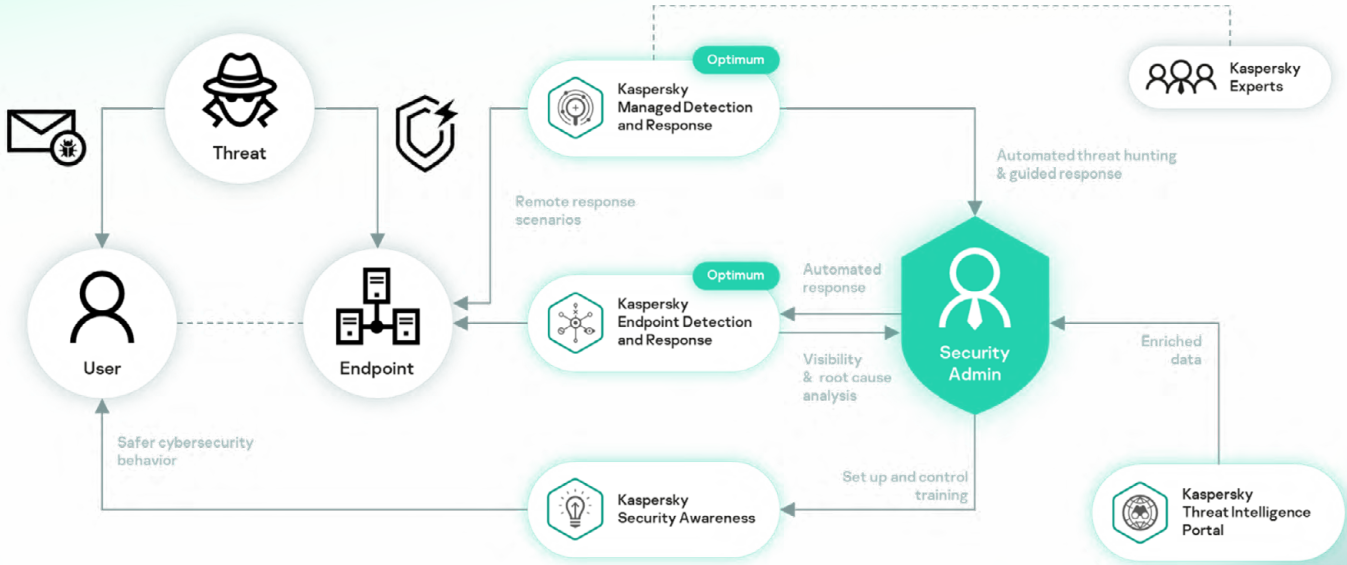
Let us help you out

To ensure the efficient protection of your IT infrastructure, you need to implement and configure your products according to best practices and your unique security requirements.

Maximize the ROI from your security solution, and ensure it's performing at 100% capability, by letting our experts at **Kaspersky Professional Services** help you health-check, implement, maintain and optimize your security solution.

How it all works together

Prevention, detection, analysis, response and employee training are all united in Kaspersky Optimum Security. Any component brings its own value and can be used separately, but all work together to cover all your evasive endpoint protection needs in a single integrated solution.



44% of organizations see the cost of securing increasingly complex environments as one of the top issues

IT security economics 2021, Kaspersky

Ease of operation

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

Full package

- Part of the Kaspersky security ecosystem, building up your defenses from Security Foundations to optimized advanced. capabilities.
- The diverse features of Kaspersky Optimum Security can be managed through a single cloud console.
- Multiple layers of protection, address both commodity and evasive threats, as well as risk from human error.

Ease of management

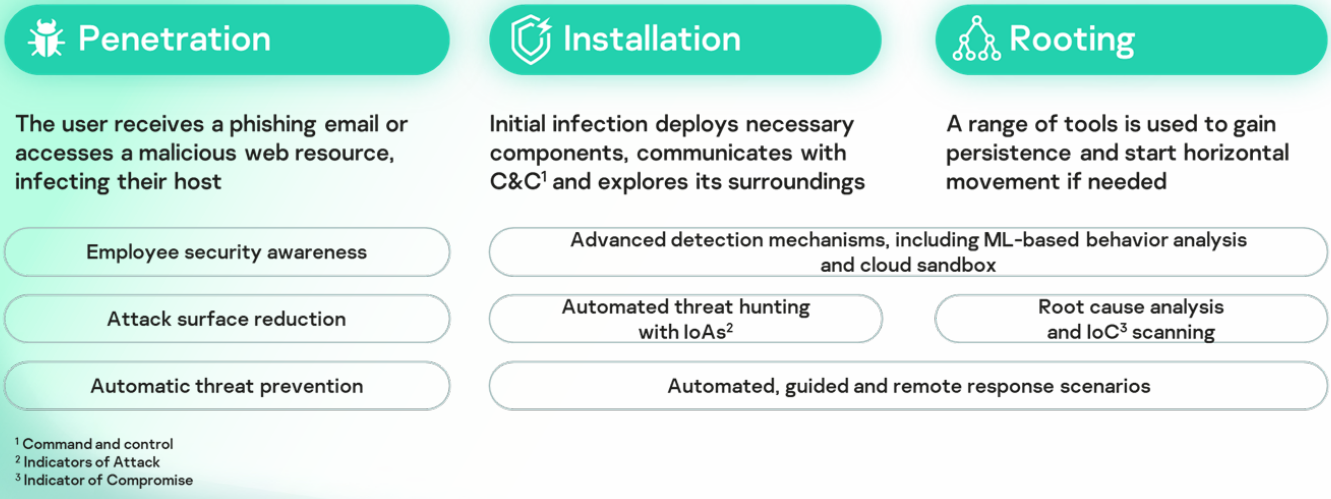
- Our cloud management console gives you quick and efficient control from anywhere in the world.
- On-prem and SaaS options provide the same admin experience.
- Deployment is quick and hassle-free, whether or not you already use Kaspersky solutions.
- Your team can control and manage all tools easily and intuitively, with no need for lengthy familiarization or retraining.

Save time and resources

- Managed protection helps you to build detection and response capabilities without associated levels of security investment, even if you lack cybersecurity staff or expertise.
- Crucial processes are automated, making incident response fast, accurate and efficient.
- Better employee security awareness means less threats penetrate your defenses – and fewer incidents for you to process!

In practice

How it all comes together in practice.



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

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 blocking the vast majority of threats.

» Learn more

Kaspersky Optimum Security

Build up your defenses against evasive threats,

» Learn more

Kaspersky Expert Security

Readiness for complex and APTlike attacks.

» Learn more

Who we are

We are a global private cybersecurity company with hundreds of thousands of customers and partners around the world, commited to transparency and independence. For 25 years we've been building tools and providing services to keep you safe with our Most tested, Most awarded technologies.

IDC

IDC MarketScape Worldwide Modern Endpoint Security for Enterprises 2021 Vendor Assessment

Major Player

AV-Test

Advanced Endpoint Protection: Ransomware Protection Test

100% protection

Radicati Group

Advanced Persistent Threat (APT) Market Quadrant

Top player

Take a closer look

To find out more about how Kaspersky EDR Optimum addresses cyberthreats while going easy on your security team and resources, visit www.kaspersky.com/enterprise-security/edr-security-software-solution

[1] Endpoint Detection and Response
[2] Managed Detection and Response

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

kaspersky.com