kaspersky

Kaspersky B2B portfolio

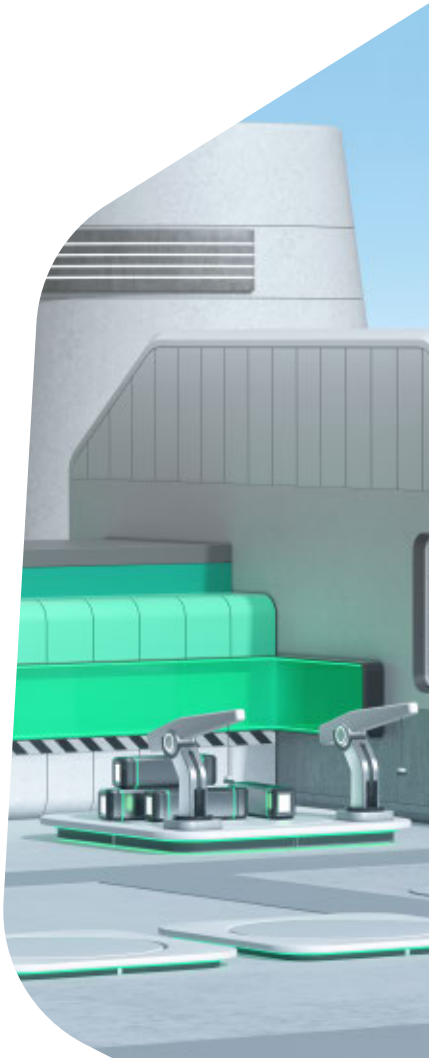
Table of contents

About the Kaspersky B2B portfolio

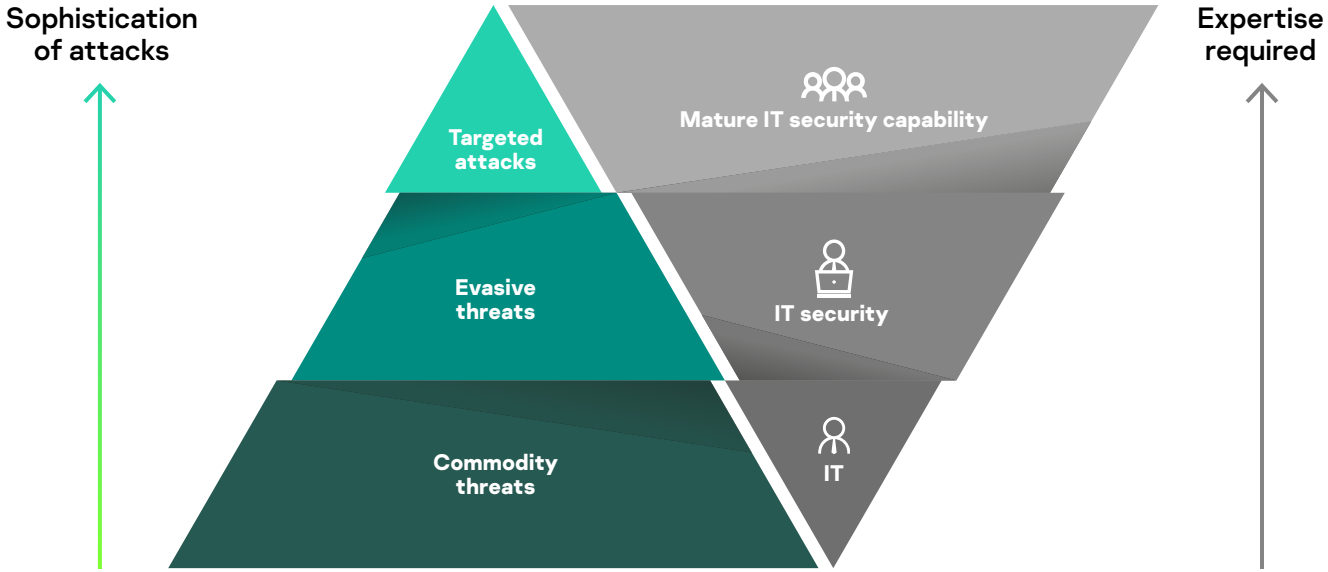
Building a security foundation for your organization by choosing the right product or service is just the first step. Developing a forward-thinking corporate cybersecurity strategy is key to long-term success.

Kaspersky's B2B portfolio reflects the security demands of today's businesses, responding to the needs of organizations of any size and at different levels of IT security maturity with a unique stage-by-stage cybersecurity approach. This approach combines different layers of protection against all types of cyberthreat, helps organizations prevent 90% of threats automatically and then systematically and methodically empowers them to add new and advanced capabilities to counter more sophisticated threats as their business develops.

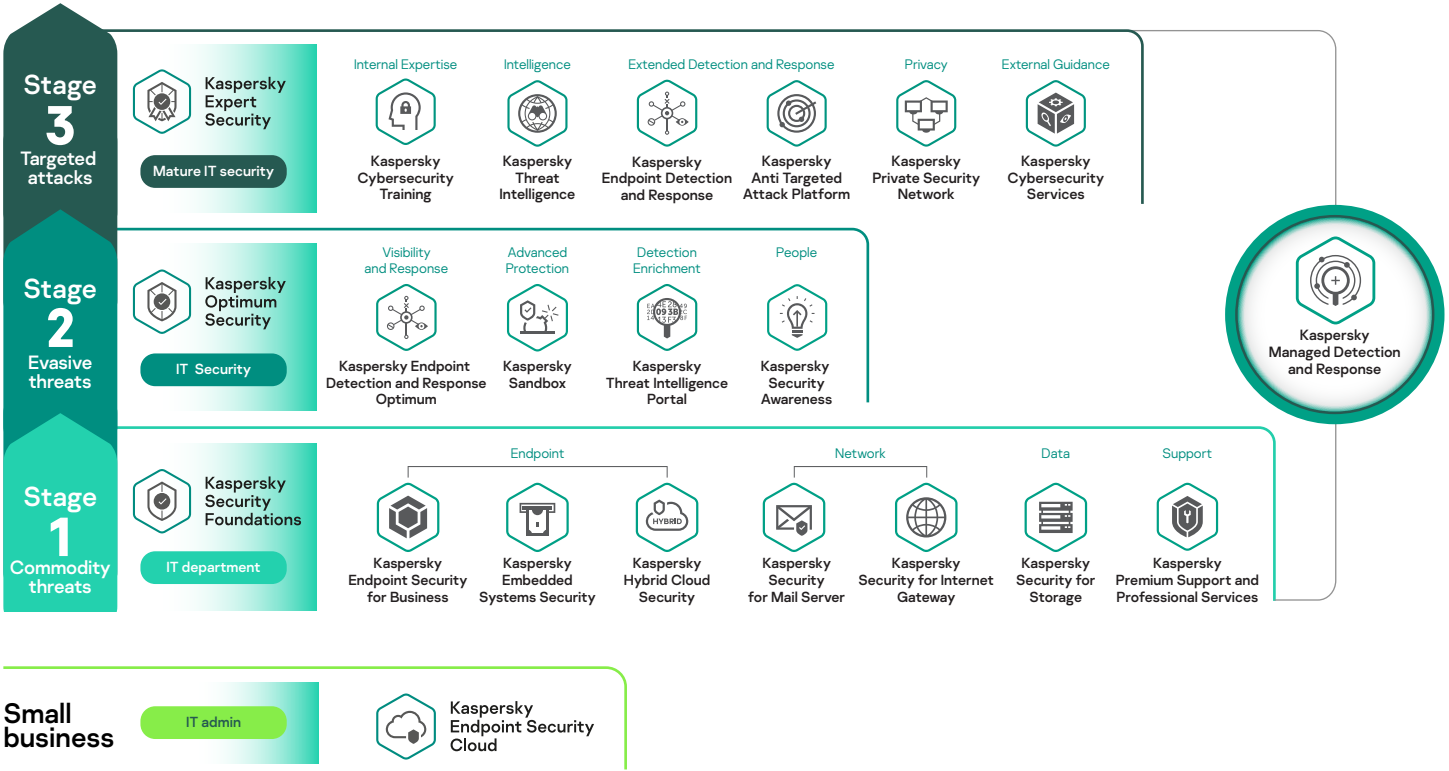
Kaspersky is your one cybersecurity partner who sees the full picture, so you can be fearless and focus on innovation.



Threat types and the expertise required to counteract them



Kaspersky's stage-by-stage cybersecurity approach



The need for long-term security planning

Traditional short-term security planning

Decision-making:

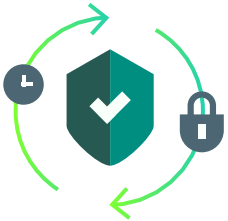
- Market trends
- Siloed security solutions
- 'Firefighter' approach
- Driven by compliance

Leveraging traditional products:

- EPP
- Firewalls/NGFW
- Web Application Firewalls
- Data Loss Prevention
- SIEM

Attributes

- Short-term security planning
- Reliance on technologies and features
- Perimeter-based network defense



Why traditional approaches fail:

- Growing complexity of the threat landscape
- Complexity of the IT infrastructure to be secured
- Complexity of incident response processes

Endpoints are the most common entry points into an organization's infrastructure, the main target of cybercriminals, and key sources of the data needed for the effective investigation of complex incidents.

of incidents were detected after impact

of businesses are concerned with the lack of IT security expertise

Source: Incident response 2021 analyst report by Kaspersky, IT security economics 2021 report by Kaspersky

Kaspersky Security for Enterprises

Back to contents

Stage
3
Targeted attacks

Kaspersky Expert Security

Back to contents

Kaspersky Expert Security

What is it?

Kaspersky Expert Security is a comprehensive defensive approach, designed to meet the day-to-day needs of any IT security-matured enterprise in dealing with the most sophisticated current threats, including APTs (Advanced Persistent Threats) and targeted attacks.

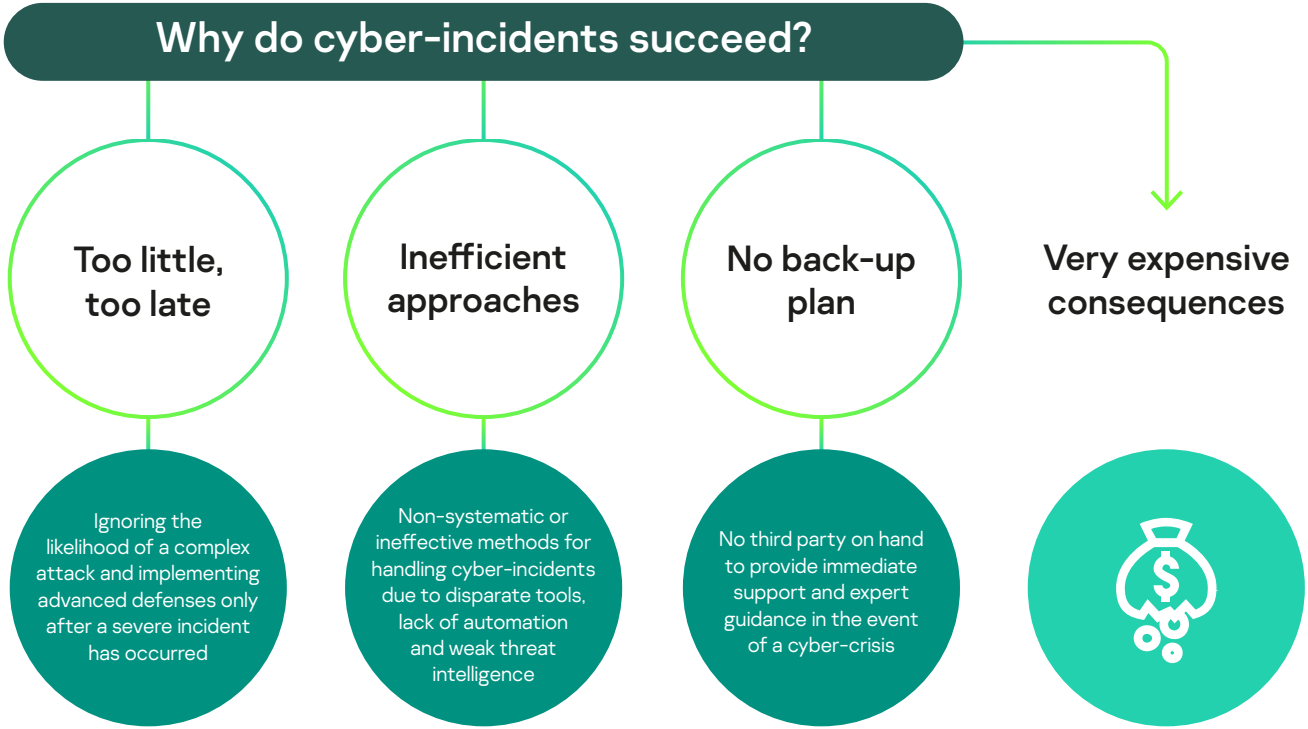
Who's it for?

- Mature and fully formed IT security team or a Security Operations Center
- Organizations with a complex and distributed IT environment
- Companies with a low risk appetite due to the high potential costs of security incidents and data breaches

What does it do?

- Optimizes your experts' workloads
- Uplifts their knowledge and skills
- Backs up your experts

Challenges


Why do cyber-incidents succeed?
Too little, too late
Inefficient approaches
No back-up plan
Very expensive consequences
Ignoring the likelihood of a complex attack and implementing advanced defenses only after a severe incident has occurred
Non-systematic or ineffective methods for handling cyber-incidents due to disparate tools, lack of automation and weak threat intelligence
No third party on hand to provide immediate support and expert guidance in the event of a cyber-crisis

How Kaspersky Expert Security deals with these challenges

Equipped

Equips your in-house experts to address complex cybersecurity incidents and optimize workloads

Informed

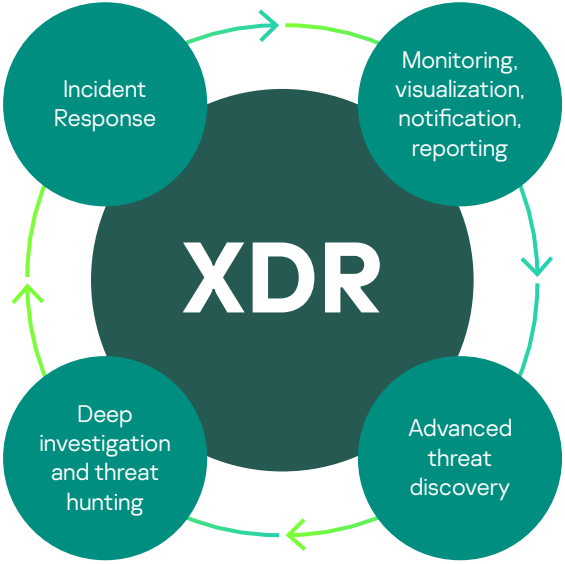
Enriches your knowledge pool with threat intelligence and **upskills** your experts to deal with complex incidents

Reinforced

Backs up your experts and **reinforces** them with trusted guidance

Equipped

Equips your in-house experts



Enterprise-wide visibility of all attack stages enables seamless threat analysis, and robust defenses against complex attacks.

A unified platform reduces alert levels by providing threat intelligence-based context and prevents 'alert fatigue'.

The automation of detection, investigation and response tasks optimizes IT security team workloads.

Integration with existing security products enhances overall security levels and protects your legacy security investment.

Key products

Kaspersky Anti Targeted Attack

Kaspersky Endpoint Detection and Response

Informed

Keeps your in-house experts informed

Threat Intelligence

- **Security Operations** — Unique insights into your adversaries are delivered in various formats to improve the effectiveness of security operations
- **Incident Response** — Global historical data about relationships between threats and their attribution to specific adversaries boosts human-driven investigations
- **Vulnerability Management** — Timely and accurate information on vulnerabilities actually exploited in the wild helps to prioritize patching efforts according to the identified risk levels
- **Security Leadership** — A comprehensive overview of your security posture informs your defensive strategy and helps justify your IT security investment

Key products Kaspersky Threat Intelligence

Upskills your in-house experts

Hands-on training from industry-recognized experts upskills your in-house team to effectively deal with IT security incidents.

Saves time and money on trying to recruit hard-to-find ready-skilled staff.

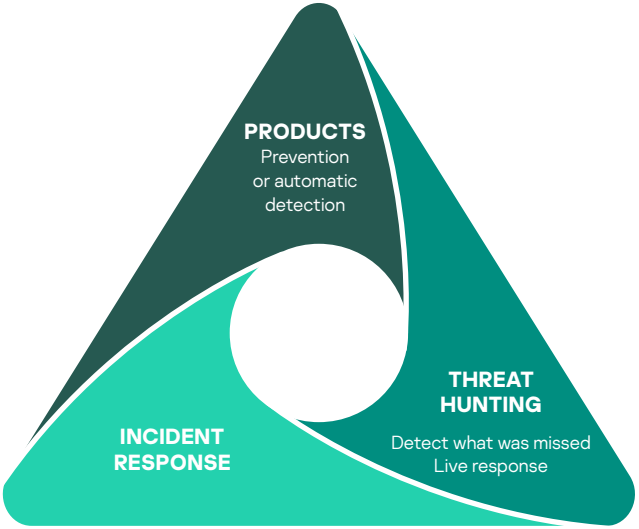
Helps retain and motivate in-house staff through promoting skills-based career development.

Comprehensive training courses are adaptable to your needs and can be delivered on-site, remotely or on-demand.

Key products Kaspersky Cybersecurity Training

Reinforced

Backs up your experts



Completely managed protection means you can outsource routine tasks and focus in-house resources on tasks that really require their involvement.

Superior detection capabilities backed by over 20 years of consistently outstanding targeted attack research filters out misleading false positives and costly false negatives.

Immediate support from deeply experienced cyber-intrusion investigators enables you to resolve even the most complex incidents fast and effectively.

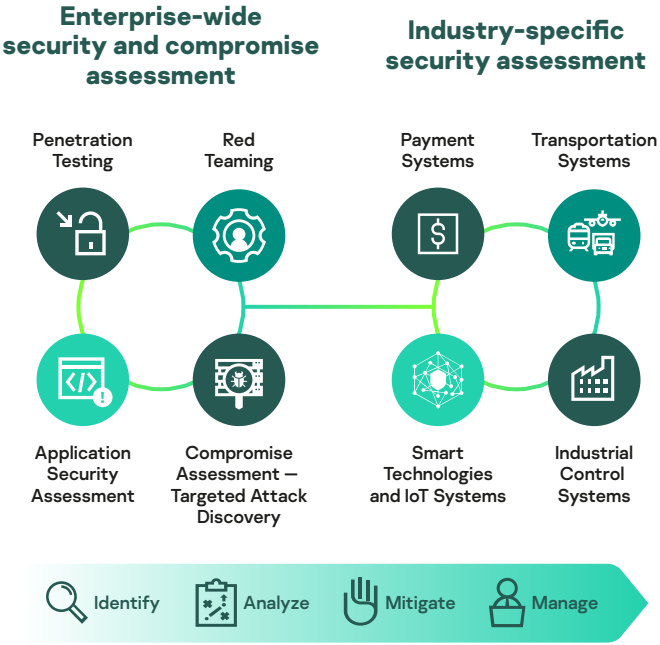
Key services

Kaspersky Managed Detection and Response

Kaspersky Incident Response

Reinforced

Reinforces your experts with trusted guidance



Threat intelligence-driven security assessment engagements provide an overview of your security posture, allowing you to close security gaps before their exploitation.

Compromise assessment delivers timely identification of security incidents, so their impact can be mitigated before they become apparent, and protection enabled against similar attacks in future.

Teams with a deep, current practical knowledge of industry-specific infrastructures can help improve defenses against threats affecting specific specialized IT environments.

Key services

Kaspersky Security Assessment

Kaspersky Targeted Attack Discovery

What's under the hood

Informed | **Equipped** | **Reinforced**

Kaspersky Expert Security

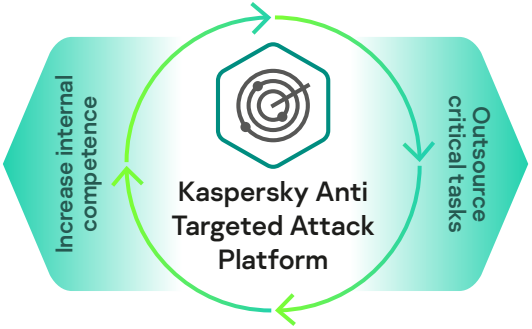
Kaspersky Threat Intelligence

- Threat Data Feeds
- CyberTrace
- Threat Lookup
- Cloud Sandbox
- APT and Crimeware Intelligence Reporting
- Digital Footprint Intelligence
- Industry-specific Intelligence Reporting (ICS, Transport)
- Ask the Analyst
- Takedown Service

Kaspersky Cybersecurity Training

- Incident Response Training
- Digital Forensics Training
- Malware Analysis and Reverse Engineering Training
- Online YARA Training

Kaspersky Extended Detection and Response



Kaspersky Security and Compromise Assessment

- Targeted Attack Discovery
- Penetration Testing
- Red Teaming
- Application Security Assessment
- Industry-specific Security Assessment (ICS, Payment Systems, Transportation, IoT)

Kaspersky MDR and Incident Response

- Managed Detection and Response (MDR) Expert
- Incident Response
- Malware Analysis
- Digital Forensics

Key differentiators

The industry's most comprehensive defensive approach

A complete arsenal of advanced technologies and services to boost the effectiveness of your IT security talents and your SOC team.

A single centralized solution to manage multi-vector detection and response

Specialized solutions, driven by top-rated APT campaign discoveries from the Kaspersky GREeAT team, with unmatched defensive capabilities delivered from a single console.

Leading threat intelligence informing each step of the incident management cycle

Recognized as a Leader in The Forrester Wave™: External Threat Intelligence Services Q1 2021, 'Kaspersky enables significantly increased security operational efficiencies, minimizing attack "dwell time".'

Continuous access to proven IT security expertise

Experienced and industry-recognized experts with a deep, current practical knowledge of the field are at your service, covering your back when you need it most.

Stage 2
Evasive threats

Kaspersky Optimum Security

Back to contents

Kaspersky Optimum Security

What is it?

- Kaspersky Optimum Security helps protect businesses from new, unknown and evasive threats.
- Effective threat detection and response solution, easy on resources.
- 24/7 security monitoring, automated threat hunting and guided and managed responses supported by Kaspersky experts.

Who's it for?

- Small dedicated IT security team, typically of one to three people
- Limited cybersecurity resource
- Emerging cybersecurity expertise

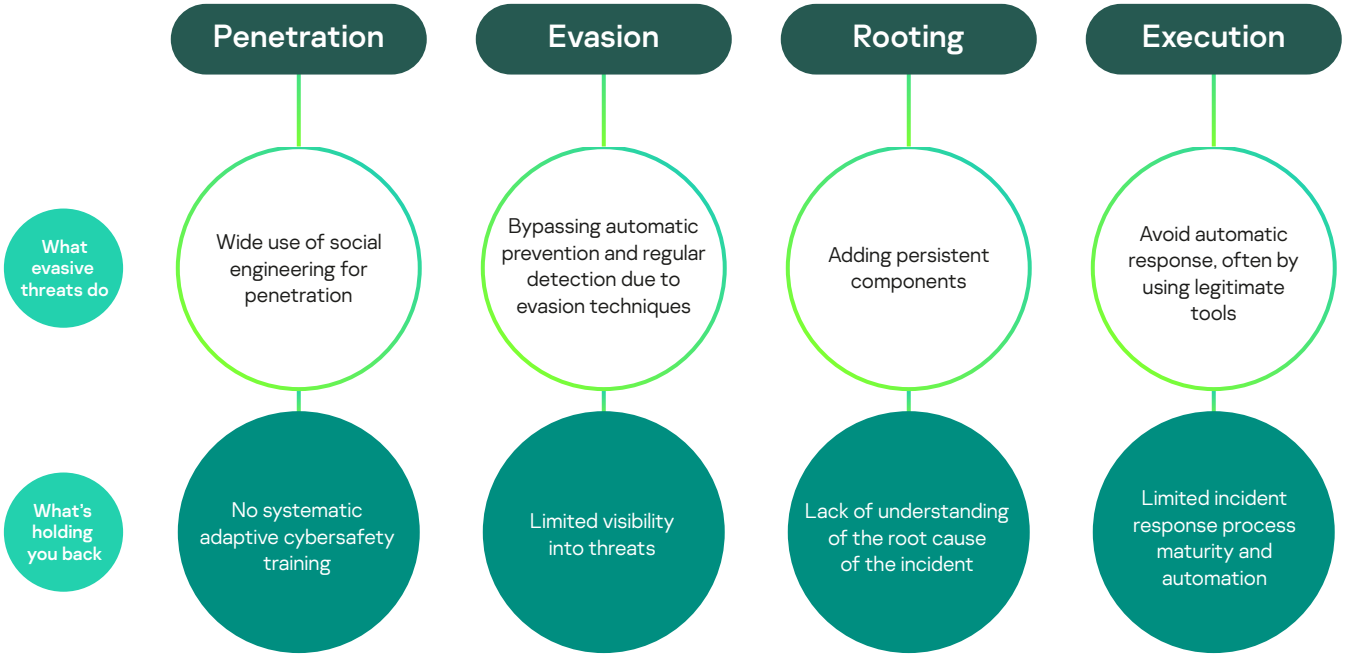
What does it do?

- Upgrades endpoint protection against evasive threats
- Supports building essential incident response processes
- Optimizes cybersecurity resource use

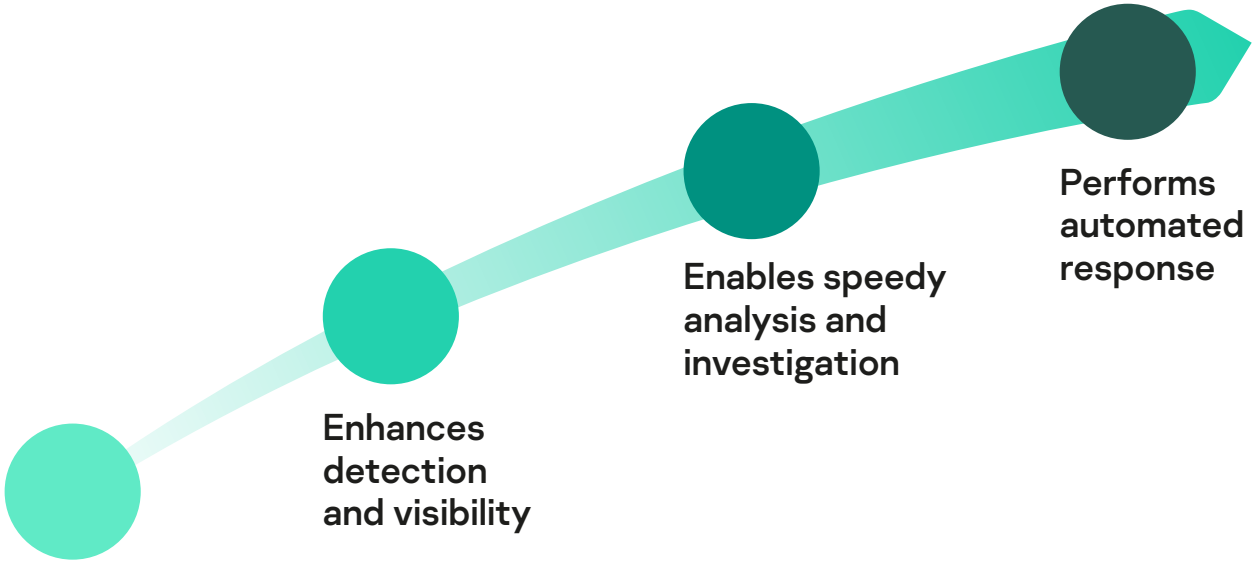
Challenges

New, unknown and evasive threats
Advanced ransomware, malware, cybertheft, etc.

These threats can be present in systems for much longer and cause more damage.



How Kaspersky Optimum Security deals with these challenges



+ Automation features and a streamlined workflow help make the best of limited resources

Raises security awareness

Build a safe working environment throughout your organization by motivating staff to learn specific skills, change habits and behave cyber-safely.

Start with the leadership

Drive security awareness from the top. Engage C-suite with the topic, so they can instill the same priority for all.

Address specialized teams

Cement the role of IT-generalists as the first line of defense. Upskill your PR team, minimize potential reputational damage and mitigate direct financial losses.

Equip all employees

Instill 300+ practical cybersafety skills from experts in the field. Assess and train all employees to become 100% proficient in security awareness.

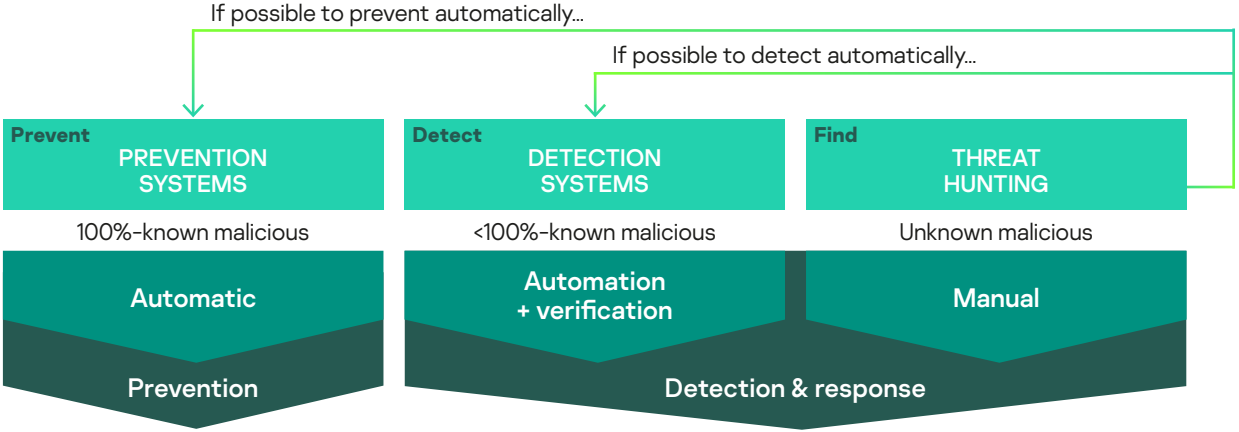
Ensure skills are applied

Use an easy-to-manage integrated solution that ensures both employee engagement and skills acquisition.

Key products: Kaspersky Security Awareness

Enhances detection and visibility

Multiple layers of detection allow for the most effective and timely discovery of threats.



Build-in emulator for pre-execution detection of malicious behavior.

Anti-rootkit technology and firmware scanner.

Threat intelligence used throughout.

Heuristics, smart records, ML-based technologies and **Adaptive Anomaly Control.**

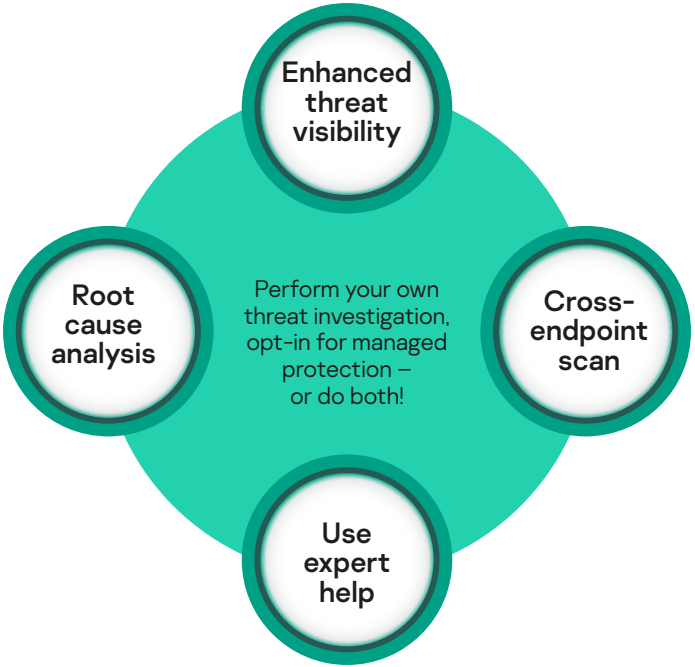
Sandbox for behavior analysis in a safe environment.

Proprietary Indicators of Attack (IoAs) created by Kaspersky experts take your detection capabilities to the next level.

Key products: Kaspersky Endpoint Detection and Response (EDR), Kaspersky Managed Detection and Response (MDR), Kaspersky Sandbox

Enables speedy analysis and investigation

Quick and efficient analysis with all data available from a single alert card



Quickly determine the root cause of a threat with drill-down visualization

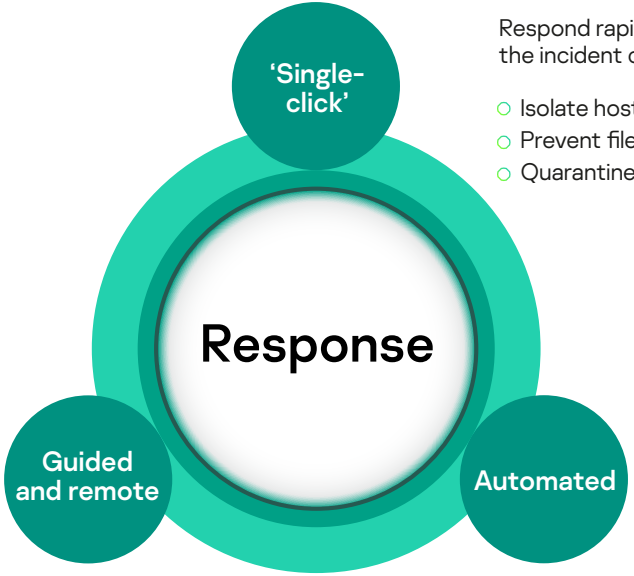
Import or generate IoC[1] and scan endpoints to reveal present threats

Kaspersky experts use leading TI[2] and AI-enabled tools to analyze your threat data

[1]Indicator of Compromise
[2]Threat Intelligence

Key products: Kaspersky Endpoint Detection and Response (EDR) Optimum; Kaspersky Managed Detection and Response (MDR) Optimum

Performs automated response



Respond rapidly right from the incident card:

- Isolate host
- Prevent file execution
- Quarantine file

Get detailed reports and response recommendations – or allow Kaspersky experts to run specific remote responses

Scan the infrastructure for IoCs[1] of identified threats, with automated response applied instantly – all through a simple checkbox

Key products: Kaspersky Endpoint Detection and Response (EDR) Optimum; Kaspersky Managed Detection and Response (MDR) Optimum

[1]Indicators of Compromise

Fights evasive threats on multiple levels

Penetration

The user receives a phishing email or accesses a malicious web resource, which infects the host

Installation

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

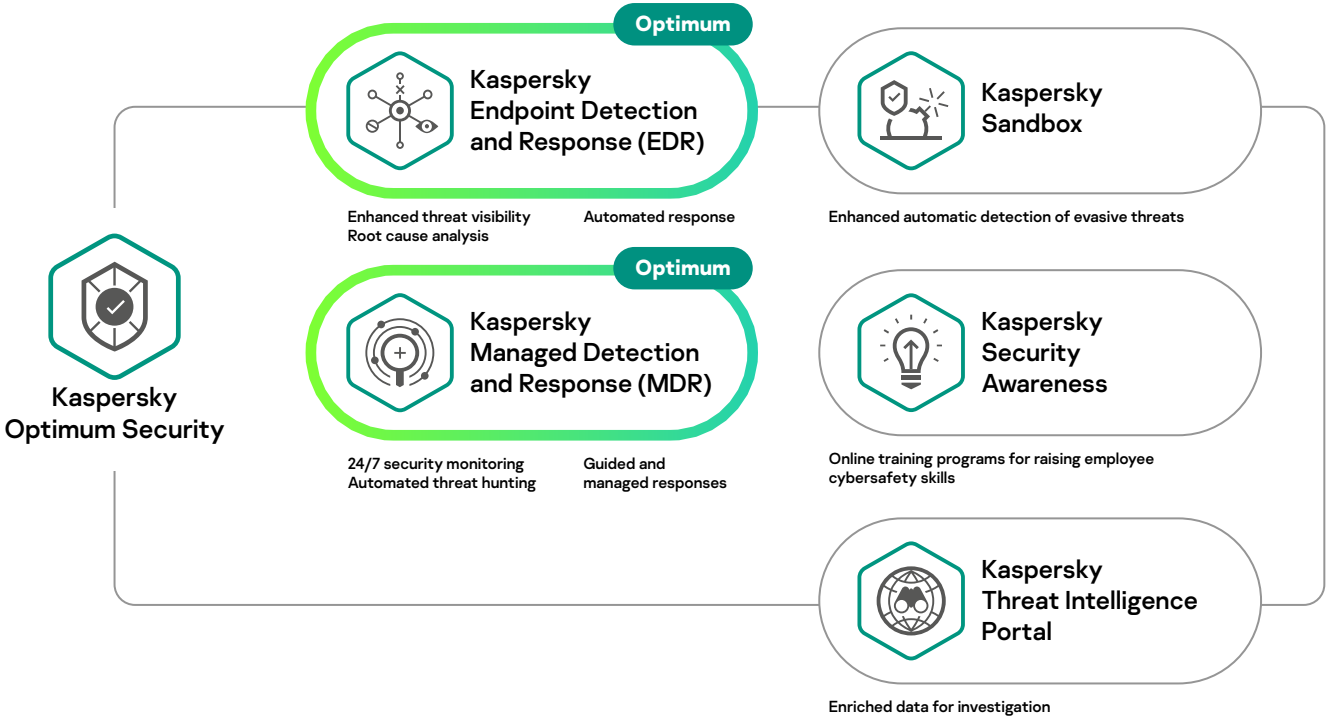
Rooting

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 sandboxing
- Automated threat hunting with IoAs[2]
- Root cause analysis and IoC[3] scanning
- Automated, guided and managed responses

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

What's under the hood



Key differentiators

Supports hybrid environments

- Workstations
- Servers
- Virtual machines
- Public clouds

Simple and automated

All products are built for organizations with limited cybersecurity resources, making streamlined detection, investigation and response a priority.

Centralized management

Unified cloud or on-prem consoles for configuration, analysis and response, all from one place.

Single solution

Essential EDR and managed protection options delivered as part of a single unified solution.

Stage 1
Commodity threats

Kaspersky Security Foundations

Back to contents

Kaspersky Security Foundations

What is it?

The cloud-managed threat prevention stage enabling every organization to automatically stop commodity cyberthreats on any device, VDI and hybrid server infrastructure. Delivers an average 441% ROI as confirmed in Forrester's TEI interviews with customers.

Who's it for?

- IT teams in organizations of every size
- Decision-makers who want to build a solid security foundation now and avoid costly future problems

What does it do?

- Protects every device – including specialized and legacy endpoints
- Delivers visibility and control over every IT asset
- Helps prevent or mitigate user mistakes
- Provides the systems management automation you need, without breaking the bank

Challenges

Is my security keeping up with my IT?

If your infrastructure is large or complex, you're probably having to deal with a multitude of endpoint types, diverse computing platforms and different environments.

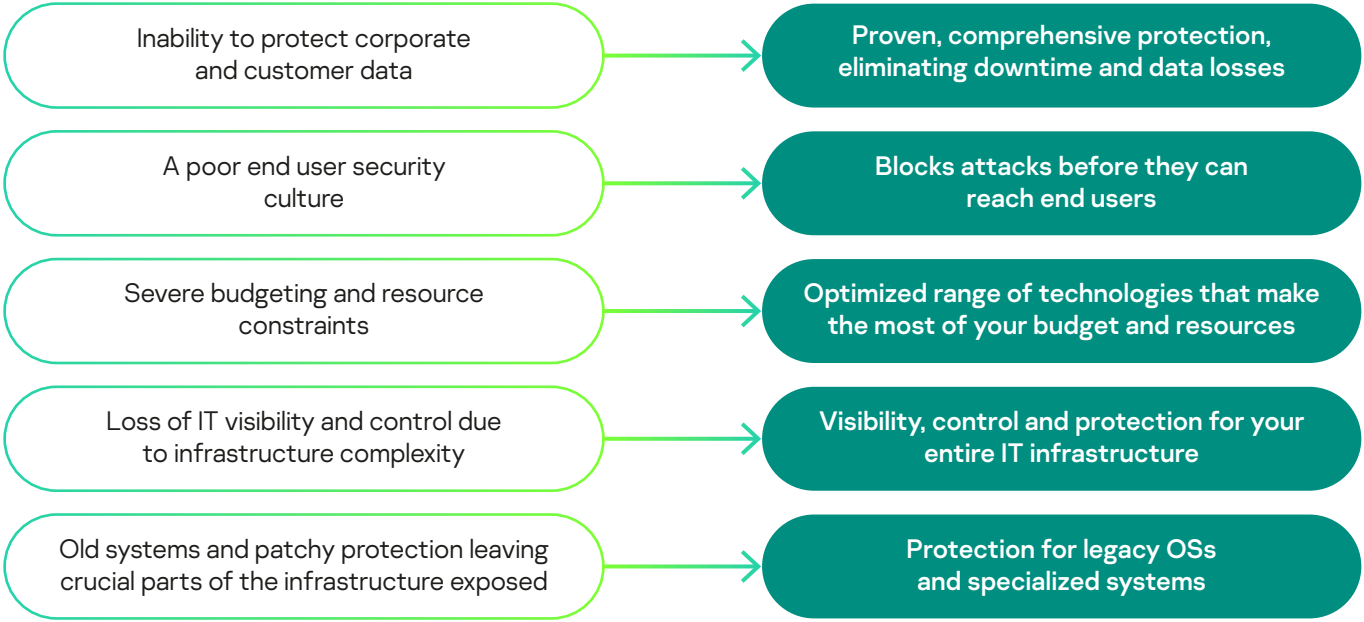
A broad range of devices and IT network functions must be brought together to function as a single – and secure – whole.

Getting all this under control is a constant struggle.

What's holding you back?

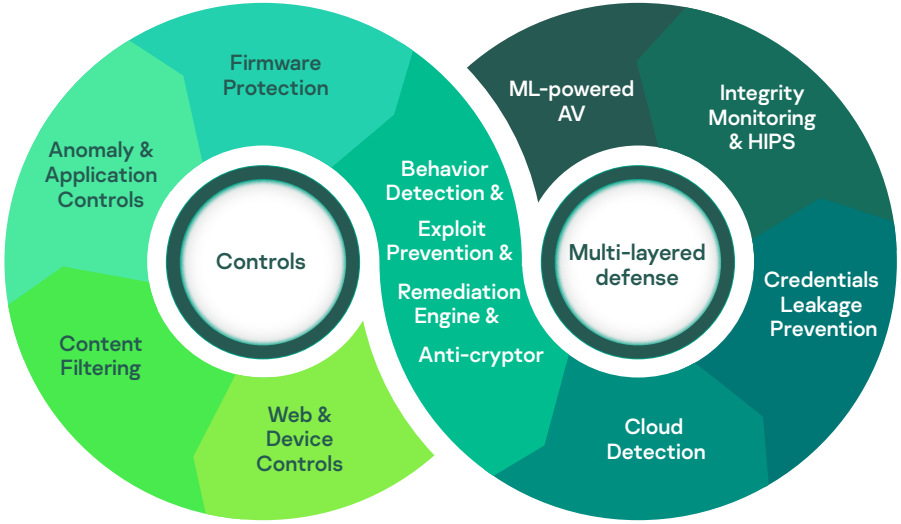
- The inability to ensure protection of corporate and customer data from exposure and loss
- A poor end user security culture
- Severe budgeting and resource constraints
- Loss of IT visibility and control
- Old systems and patchy protection, leaving crucial parts of the infrastructure exposed

How Kaspersky Security Foundations deals with these challenges



Proven, comprehensive protection, eliminating downtime and data loss

Powerful controls mean you can restrict access to valuable data, as well as limiting or blocking the activities of apps capable of threatening the security of that data. The risk of an incident leading to data loss/leakage is massively reduced through multi-layered defense technologies.



Key differentiator

With Kaspersky Security Foundations, your entire IT estate is protected right across the board through a multi-layered approach that provides defense-in-depth, eliminating downtime and data loss.

Key products:

- Kaspersky Endpoint Security for Business
- Kaspersky Hybrid Cloud Security
- Kaspersky Security for Mail Server
- Kaspersky Security for Internet Gateway
- Kaspersky Embedded System Security

Blocks attacks before they can reach end users

Technologies and granular controls let you tailor access to apps, websites etc. according to individual work roles and groups, maxing-out your security by eliminating risk.

Key differentiator

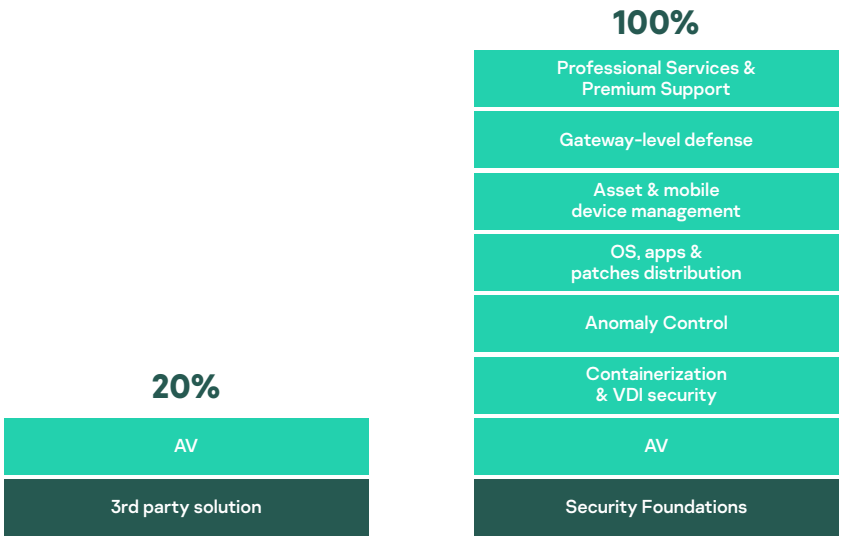
Kaspersky Security Foundations blocks attacks before they can reach end users, preventing your employees from inadvertently exposing the business to an attack. You'll find it's easy to enforce policies dictating which trusted applications your users can run and what devices they can plug into the system.

Key products:

- Kaspersky Endpoint Security for Business
- Kaspersky Hybrid Cloud Security
- Kaspersky Security for Mail Server
- Kaspersky Security for Internet Gateway

Optimized range of technologies that make the most of your budget and resources

We don't force on you technologies you don't need, but all the fully automated technologies you do need are included at no additional cost:



Key differentiator

Kaspersky Security Foundations preselects the award-winning technologies that are right for organizations like yours. So you don't find yourself paying a premium for things you don't need right now, or struggling to deploy and maintain over-elaborate functionality.

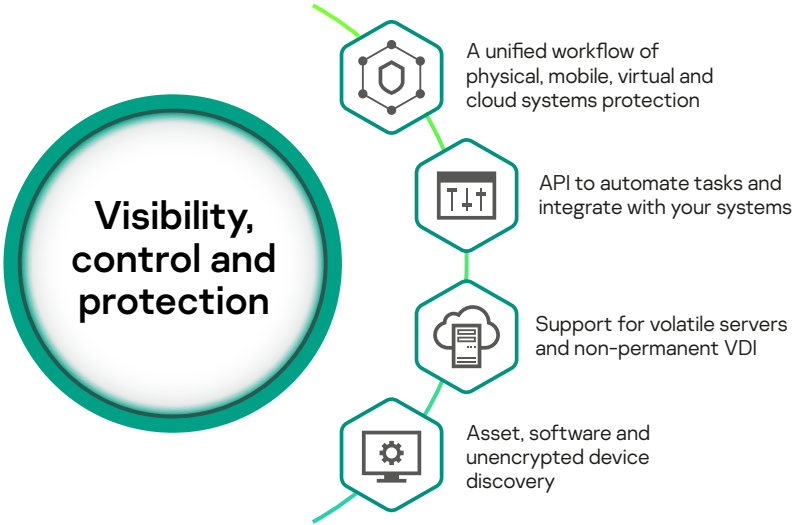
You end up with outstanding security that fits your current needs and budget, knowing that, if and when you're ready, Kaspersky Security Foundations provides the necessary agents for future EDR, MDR and XDR deployment across your entire infrastructure.

Key products:

- Kaspersky Endpoint Security for Business
- Kaspersky Hybrid Cloud Security
- Kaspersky Security for Mail Server
- Kaspersky Security for Internet Gateway

Visibility, control and protection for your entire IT infrastructure

Kaspersky Security Foundations provides a single console to give full visibility across the whole IT estate, encompassing a wide range of OSs and hybrid infrastructures by delivering:



Key differentiator

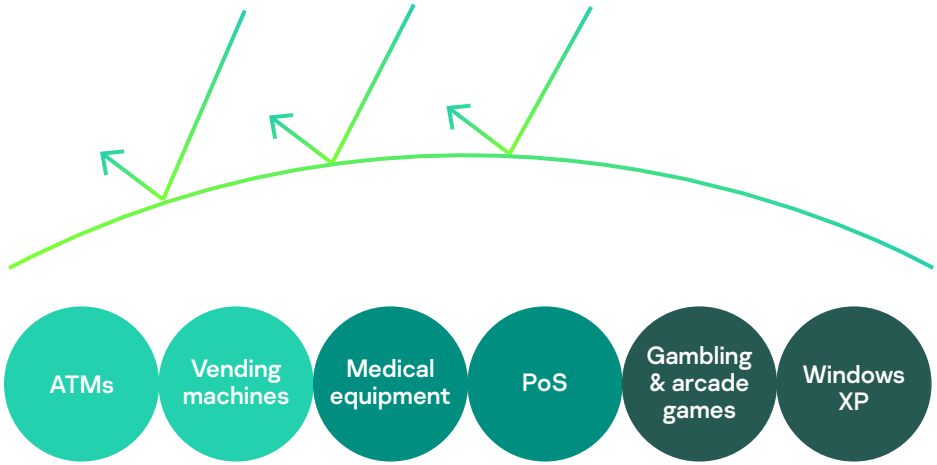
Kaspersky Security Foundations operates as unified security, providing visibility, control and protection of all aspects of your IT infrastructure – from mobile devices and VDI to virtual servers and public cloud infrastructures.

Key products:

- Kaspersky Endpoint Security for Business
- Kaspersky Hybrid Cloud Security
- Kaspersky Security for Mail Server
- Kaspersky Security for Internet Gateway
- Kaspersky Embedded System Security

Protection for legacy OSs and specialized systems

Specialized computing equipment running low-spec hardware and legacy software requires equally specialized protection. That's also true of legacy endpoints not yet ready for upgrading.



The benefits

Kaspersky Security Foundations offers graduated control and award-winning protection for legacy OSs and specialized systems that have very limited CPU and memory resources – which you can manage together with security for all your other endpoints via the same single console.

Key products:

- Kaspersky Embedded System Security
- Kaspersky Security for Internet Gateway
- Kaspersky Security for Mail Server

Key differentiators

Outstanding performance on any device

Kaspersky Security Foundations offers graduated control and award-winning protection for legacy OSs and specialized systems that have very limited CPU and memory resources – which you can manage together with security for all your other endpoints via the same single console.

Unified management of whole IT estate

Our single console and unified security workflow are specifically designed to give 360 degree IT visibility and maximum flexibility, making policy enforcement fast and efficient and minimizing risk.

Maximum automation for any infrastructure

Our products are built for organizations with limited IT resources in mind, automatically preventing cyberthreats on all devices, VDIs, gateways and hybrid server infrastructures.

A high return on investment

Ease of use is confirmed by our high ratings in Gartner Peer Insights reviews from customers of all sizes, and in industry analyst reports. Kaspersky Security Foundations generates high levels of ROI - as confirmed by Forrester TEI interviews with customers.

What's under the hood

Kaspersky Security Foundations

Kaspersky Endpoint Security for Business

Kaspersky Security for Mail Server

Kaspersky Hybrid Cloud Security

Kaspersky Security for Internet Gateway

Kaspersky Embedded System Security

Kaspersky Professional Services

Kaspersky Security for Storage

Kaspersky Premium Support

- Protection for corporate users and mobile devices
- Server security in hybrid environments
- Protection for Virtual Desktops (VDI)
- Protection for specialized endpoints and legacy PCs
- Protection against the most common attack vector: email
- Forefront protection against web-based threats
- Deployment, configuration and maintenance assistance

Kaspersky Security for Small and Medium-sized Businesses

Back to contents

Security challenges faced by SMBs

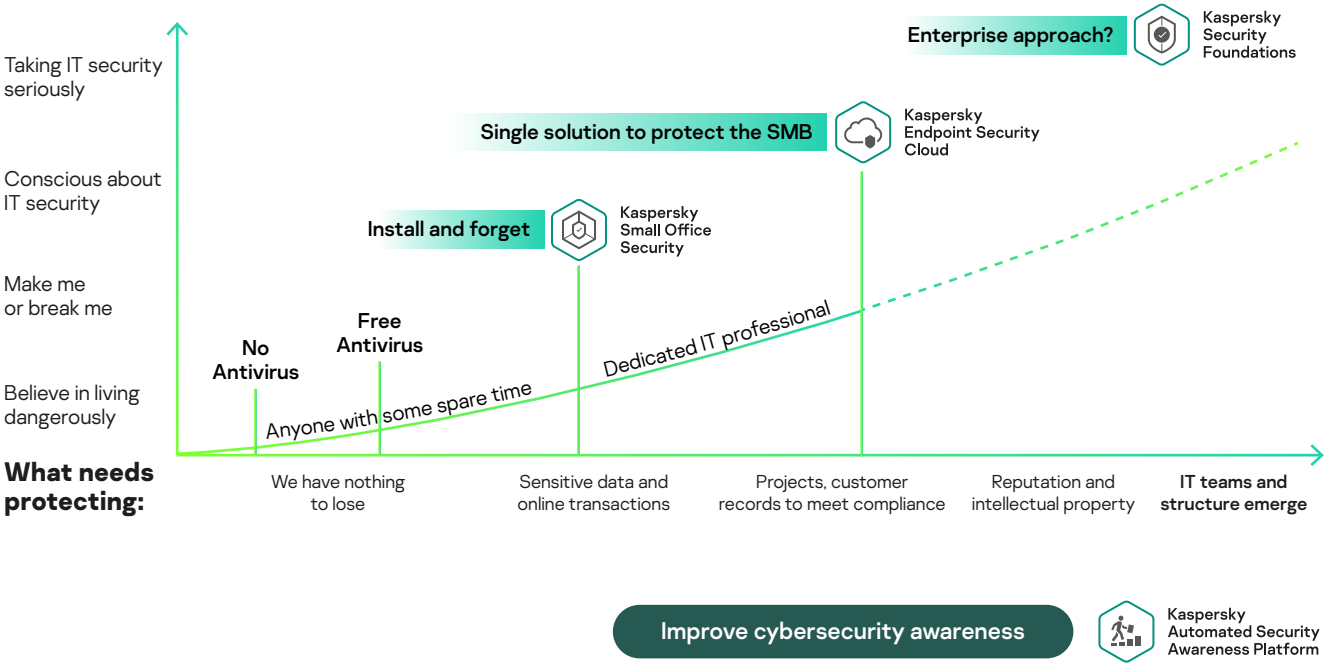
Cyberthreats

One size doesn't fit all. Smaller businesses face many of the same cyberthreats as large enterprises, but don't have the same resources to deal with them.

Overstretched resources

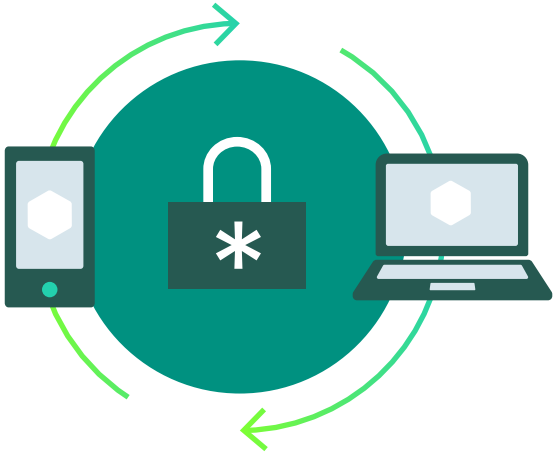
The best security makes life easier, not harder, for overworked IT departments. If you're running a small or medium-sized business, the chances are your resources are always overstretched. So you need to work smart – picking the security solution that delivers instant protection and makes minimal demands on your budget, time and energies.

Kaspersky's lean IT security approach



Kaspersky Small Office Security

Ideal for when there's no IT specialist in your business, and whoever's most IT-savvy sorts things out.



Kaspersky Small Office Security combines the simplicity of home PC protection with special capabilities to keep your business safe. It's easy to install, even easier to manage, and provides the world's most tested, most awarded security for computers, file servers, laptops and mobile devices, while protecting your business from online attacks, financial fraud, ransomware and data loss.

Key differentiators

- Fast - installs in under 10 minutes
- Easy to use - out-of-the-box security you just set and forget
- Effective - secures sensitive data and protects your business from data breaches, fines and lost business

Kaspersky Endpoint Security Cloud

Kaspersky Endpoint Security Cloud provides a single solution for all your organization's IT security needs. You can make sure your business is running smoothly while Kaspersky's blocking ransomware, fileless malware, zero day attacks and other emerging threats. Our cloud-based approach means your users can work securely on any device, and collaborate safely online, at work or at home, from remote offices and in the field.

Ideal for businesses who have an IT administrator who's responsible for all IT tasks, and who are looking to save on resources.

- Protects your business effortlessly, without sacrificing IT resources, time or budget
- Reduces IT costs and frees up resources by automating routine processes
- Supports safe cloud migration with Shadow IT discovery and protection for Microsoft Office 365

Enjoy all-round agility

- Faster time to protection
- No capital investment
- Frees up your IT resources
- Pay-as-you-go
- Outsourcing-friendly

Kaspersky Automated Security Awareness Platform

Kaspersky ASAP is an effective, easy-to-use online tool that shapes employees' cybersafety skills and motivates them to behave appropriately, based on Kaspersky's 20+ years' experience in IT security. User-friendly functionality and automation supports you at every stage, from setting goals to evaluating results.

Ideal if you want safety-conscious employees and increased resilience to online threats.

- Improves employees' security awareness and equips them with skills they can use immediately, right from lesson one
- Effective training that takes very little time and doesn't require dedicated resources or any special cybersecurity knowledge

Key differentiators

- Helps reduce incidents resulting from human error, ensuring business continuity and minimizing the impact of an incident
- Improves the cybersecurity culture in your organization
- Lets you launch and manage training with minimal expenditure on time

Things to remember when building a long-term cybersecurity strategy

A siloed approach to cybersecurity puts businesses at risk

The growing costs of network and data breaches place serious financial pressures on businesses wanting to transform, which is why cybersecurity is such a prominent issue. To succeed in this environment, organizations must make cybersecurity an integral part of their overall business strategy, playing a key role in risk management and long-term planning.

Cybersecurity is not just a destination — it's an ongoing journey

Any enterprise's security plan must be regularly reviewed and adjusted as new knowledge and tools become available. Every security incident should undergo in-depth analysis and result in the creation of new attack handling procedures and measures to prevent similar incidents happening in the future. Existing defenses must be continually improved.

Things to remember when building a long-term cybersecurity strategy

Awareness, communication and cooperation are key to success in a world of rapidly changing cyberthreats

More than 80% of all cyber-incidents are caused by human error. Staff training at every level is essential to raise security awareness across the organization and motivate all employees to pay attention to cyberthreats and their countermeasures – even if they don't think it's part of their job responsibilities.

A proactive 'detection and response' mindset is the best way to counter today's ever-evolving threats

Traditional prevention systems should function in harmony with advanced detection technologies, threat analytics, response capabilities and predictive security techniques. This helps create a cybersecurity system that continuously adapts and responds to the emerging challenges facing enterprises.

Why choose Kaspersky

Most Tested. Most Awarded

Kaspersky has achieved more first places in independent tests than any other security vendor. And we do this year after year. www.kaspersky.com/top3

Kaspersky quality confirmed by MITRE ATT&CK evaluation

MITRE | ATT&CK®

Kaspersky has once again been named a Gartner Peer Insights Customers' Choice for Endpoint Protection Platforms

Kaspersky is a Customers' Choice in the 'Gartner Peer Insights 'Voice of the Customer': EDR Solutions'

Kaspersky has been named a Gartner Peer Insights Customer's Choice of 2020 for Secure Web Gateways

Proven.
Transparent.
Independent.

Most transparent

With five Transparency Centers now active, and statistical processing based in Switzerland, the sovereignty of your data is guaranteed in ways no other vendor can match.

kaspersky