

Kaspersky B2B portfolio

kaspersky

Table of contents

| | |
|--|-----------|
| Kaspersky Security for Enterprises | 8 |
| Kaspersky Expert Security | 9 |
| Kaspersky Optimum Security | 21 |
| Kaspersky Security Foundations | 34 |
| Kaspersky Industrial CyberSecurity | 45 |
| Kaspersky SASE | 51 |
| Kaspersky Security for Small and Medium-sized Businesses | 55 |

About the Kaspersky B2B portfolio

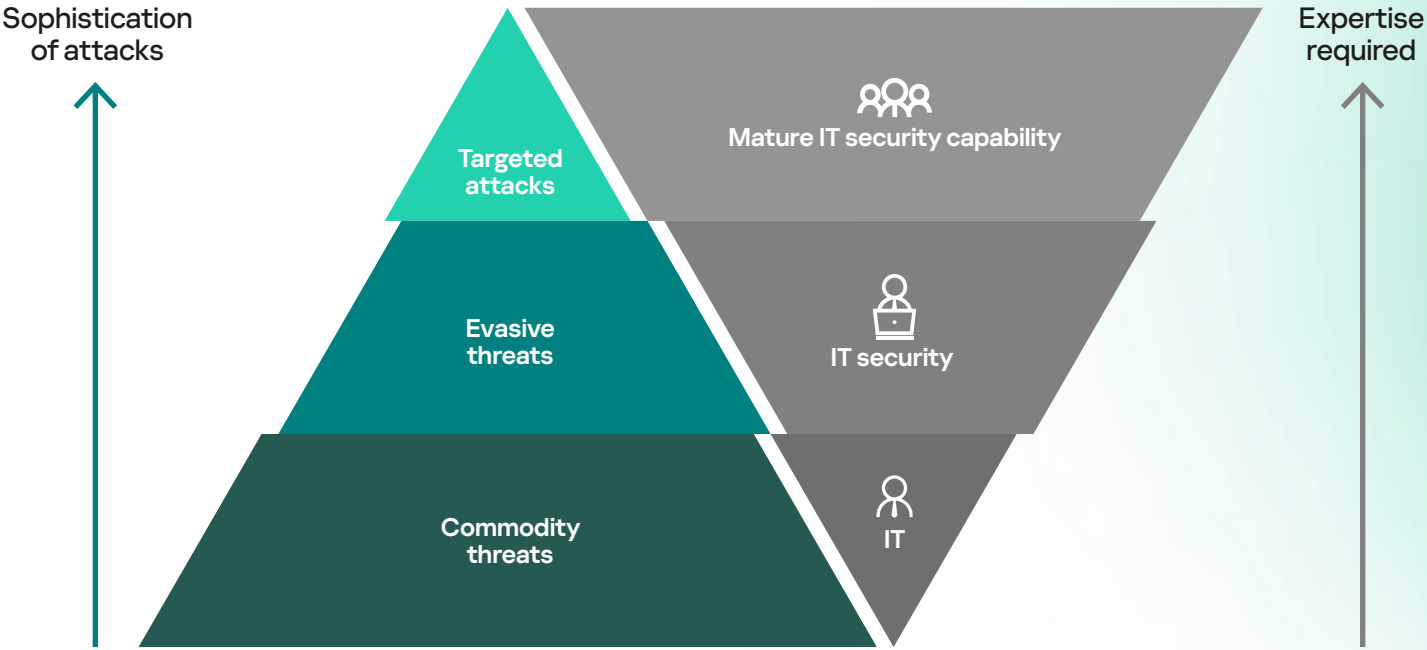
Building a security foundation for your organization by choosing the right product or service is just the first step. Developing a forward-thinking corporate cybersecurity strategy is key to long-term success.

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

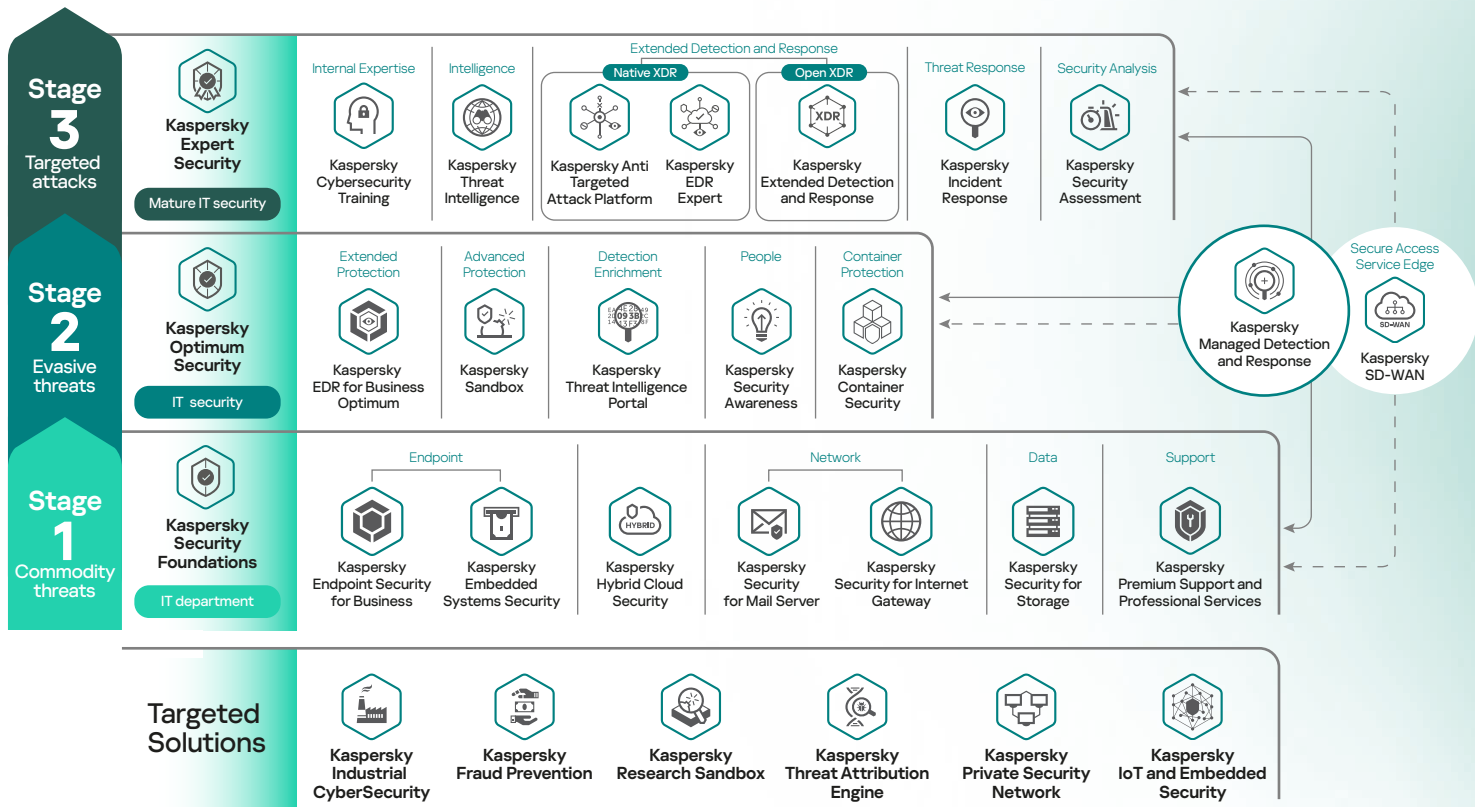
Kaspersky is your one cybersecurity partner who sees the full picture, so you can focus on fearless innovation and success.



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

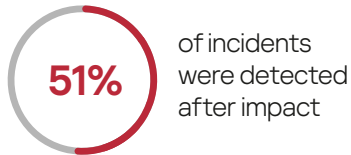
- Short-term security planning
- Reliance on technologies and features
- Perimeter-based network defense



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.



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 cybersecurity approach; designed to meet the needs of any IT security-matured enterprise in managing the most sophisticated current threats, including advanced persistent threats (APTs) and targeted attacks.

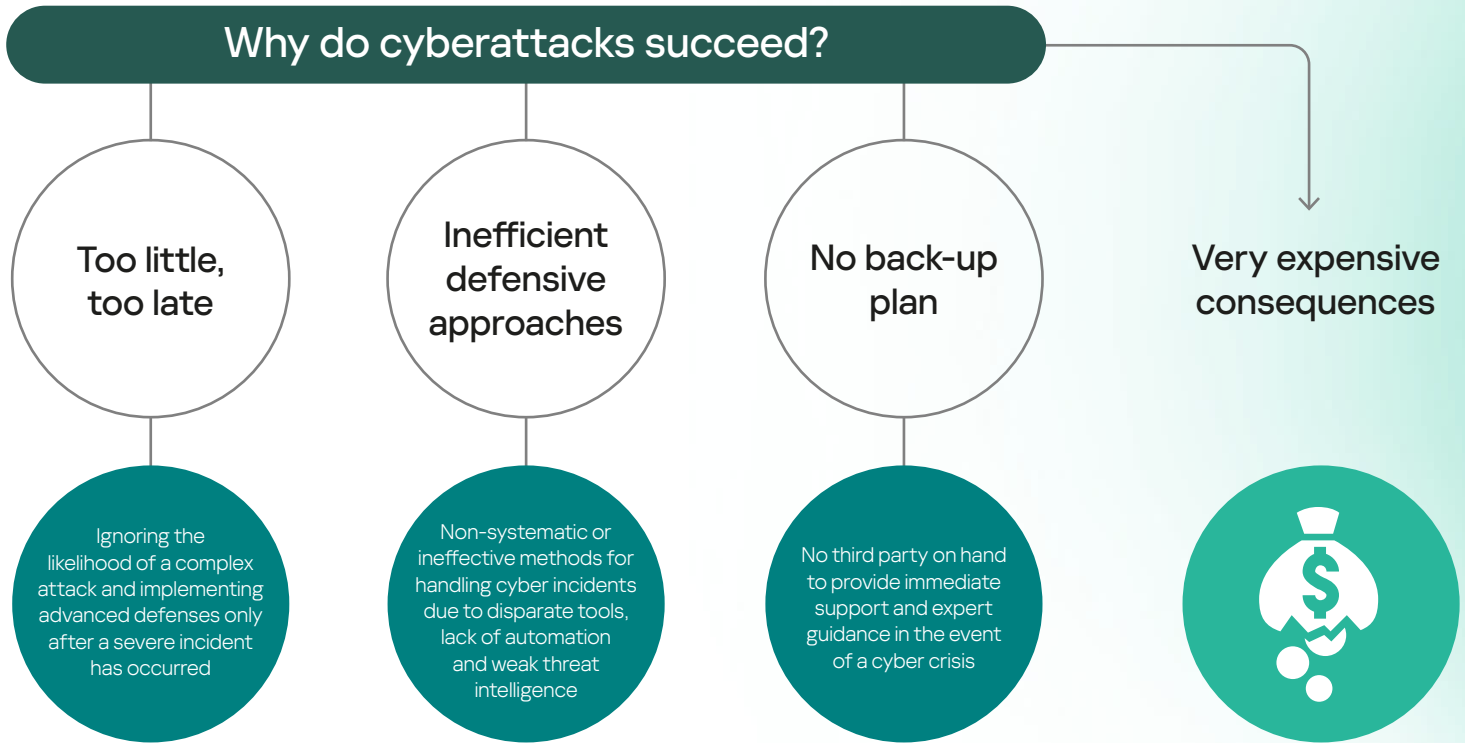
Who's it for?

- Mature and fully formed IT security team or a security operations center (SOC)
- 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



How Kaspersky Expert Security deals with these challenges



Equipped

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



Informed

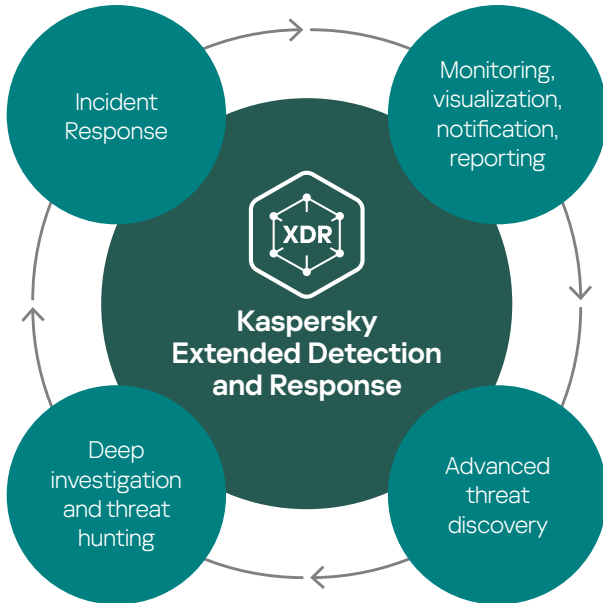
Enriches your knowledge pool with threat intelligence and **upskills** your experts to deal with complex incidents



Reinforced

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

Equips your in-house experts



Proactive protection of critical assets



All-encompassing view of corporate security



Data from endpoints, network and cloud



Automated response & real-time visibility



Insights into evolving cyberthreats



Investigation capabilities

Key products:



**Kaspersky
Extended Detection
and Response**



**Kaspersky
Anti Targeted
Attack**

[Read more](#)



**Kaspersky
EDR
Expert**

[Read more](#)



Manage IT security risks

- Comprehensive visibility
- Contextual insights
- Real-time threat detection
- Proactive threat hunting capabilities



Make informed decisions

- Data-driven approach
- Actionable intelligence
- Real-time insights into security events



Provide end-to-end IT security ops

- Unified visibility
- Centralized incident detection and response
- Incident management & documentation



Support business continuity

- Incident response automation
- Early threat detection & proactive threat hunting
- Continuous monitoring
- Compliance support

Ensures that no potential threat goes unnoticed



Kaspersky
Extended Detection
and Response

Keeps your in-house experts informed



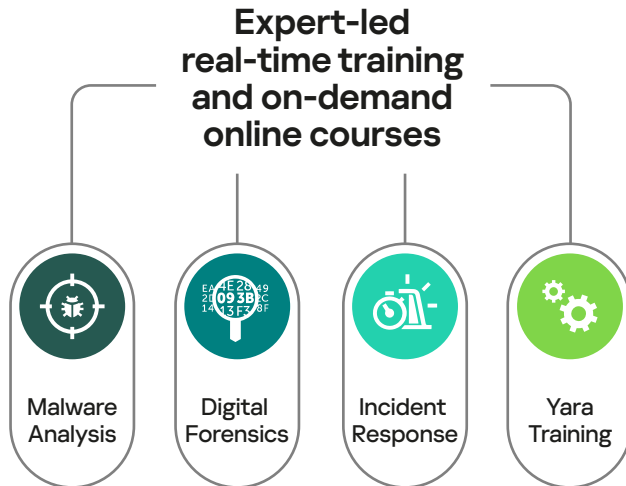
Key products:



Kaspersky
Threat
Intelligence

[Read more](#)

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.

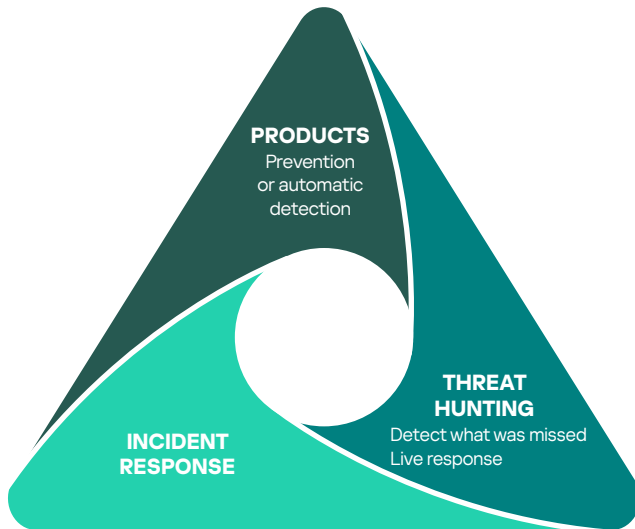
Comprehensive training courses are adaptable to your needs and can be delivered on-site, remotely or on-demand.

Key products:  Kaspersky
Cybersecurity
Training

[Read more](#)

 Kaspersky
Tabletop
Exercise

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 filter out misleading false positives and costly false negatives.

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

Key services:



Kaspersky
Managed Detection
and Response

[Read more](#)

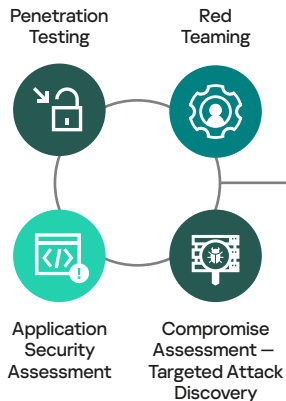


Kaspersky
Incident
Response

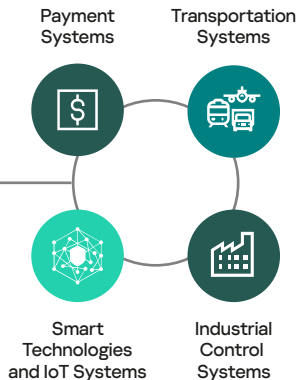
[Read more](#)

Reinforces your experts with trusted guidance

Enterprise-wide security and compromise assessment



Industry-specific security assessment



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, with 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 specialized IT environments.



Key services:



Kaspersky Security Assessment
[Read more](#)



Kaspersky for Security Operations Center
[Read more](#)



Kaspersky Targeted Attack Discovery
[Read more](#)



Kaspersky Adversary Attack Emulation

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
- Tabletop Exercise

Kaspersky Extended Detection and Response

Open XDR



**Kaspersky
Extended Detection
and Response**



**Kaspersky
Anti Targeted
Attack**



**Kaspersky
EDR Expert**

Native XDR

Increase internal
competence

Outsource
critical tasks

Kaspersky Security and Compromise Assessment

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

Kaspersky MDR & Kaspersky 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.

Get on-demand support from the world-leading threat intelligence analysts

Guidance and insights into the specific threats you're facing or are interested in without the need to invest in hiring full-time specialists.

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.

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?

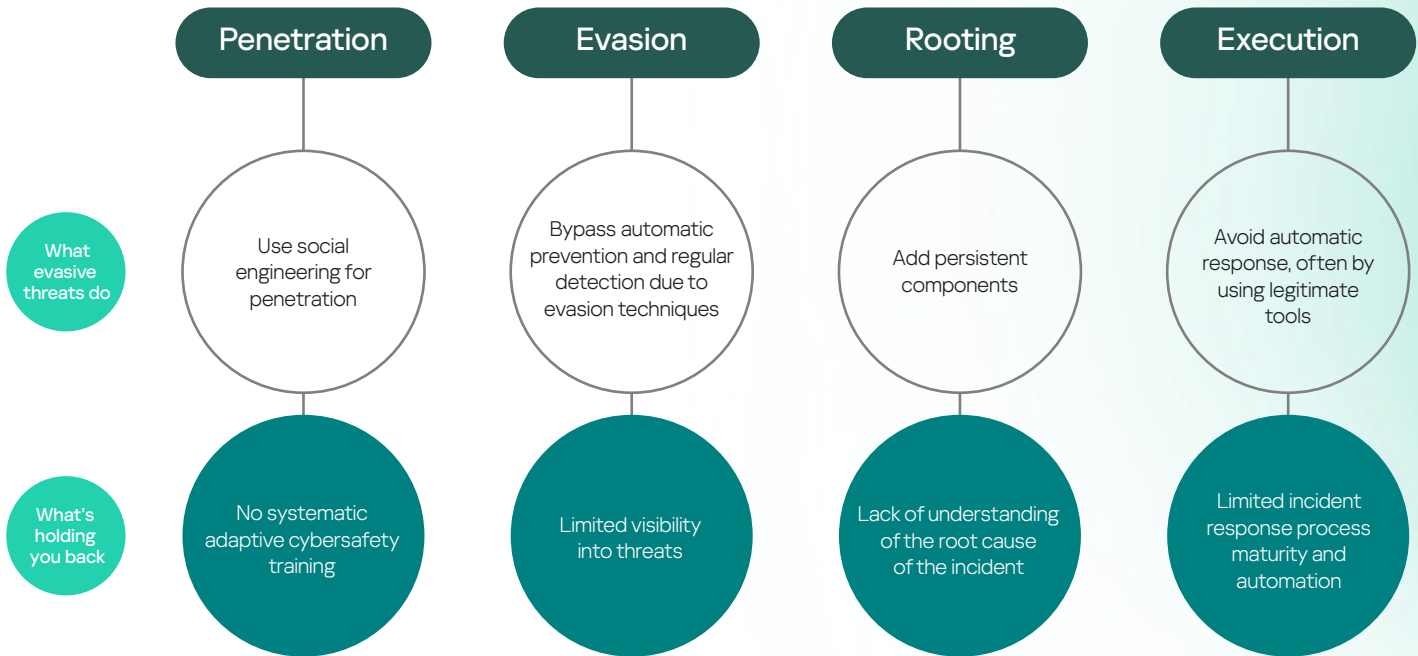
- Upgrades endpoint protection against evasive threats
- Supports development of essential incident response processes
- Optimizes cybersecurity resource

Challenges

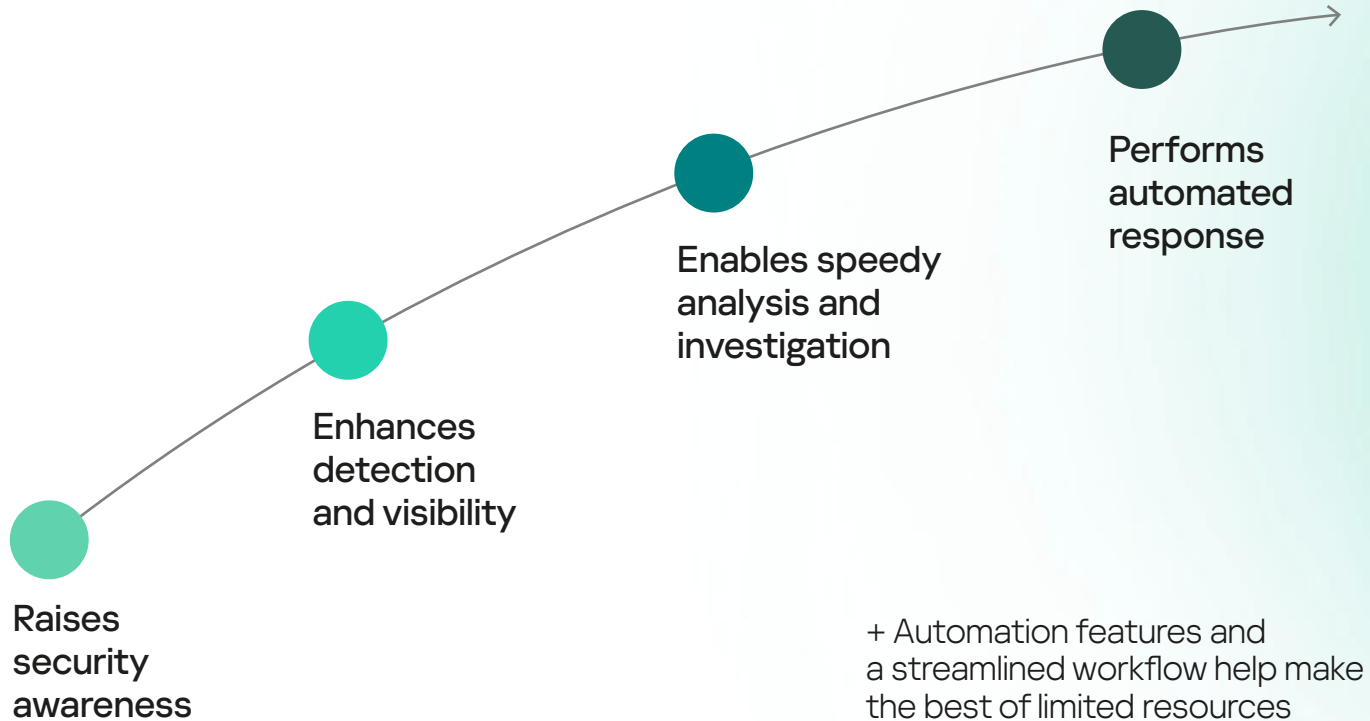
New, unknown and evasive threats

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





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

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.

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.

Raises security awareness

Address specialized teams

Equip generalist IT professionals with practical skills on how to recognize a possible attack and how to collect incident data for handover to IT Security.

Ensure skills are applied

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

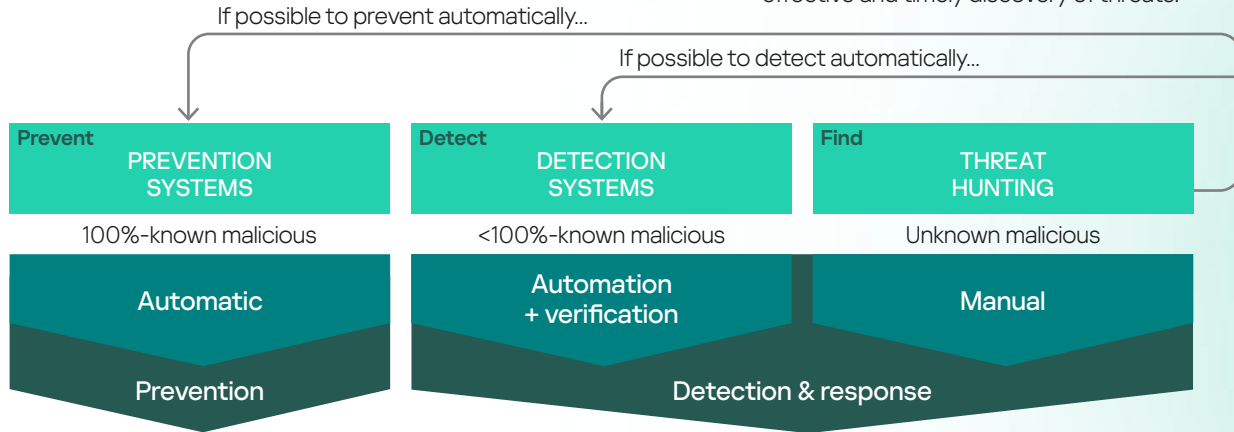
Key products:



Kaspersky
Security
Awareness

[Read more](#)

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



Built-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:

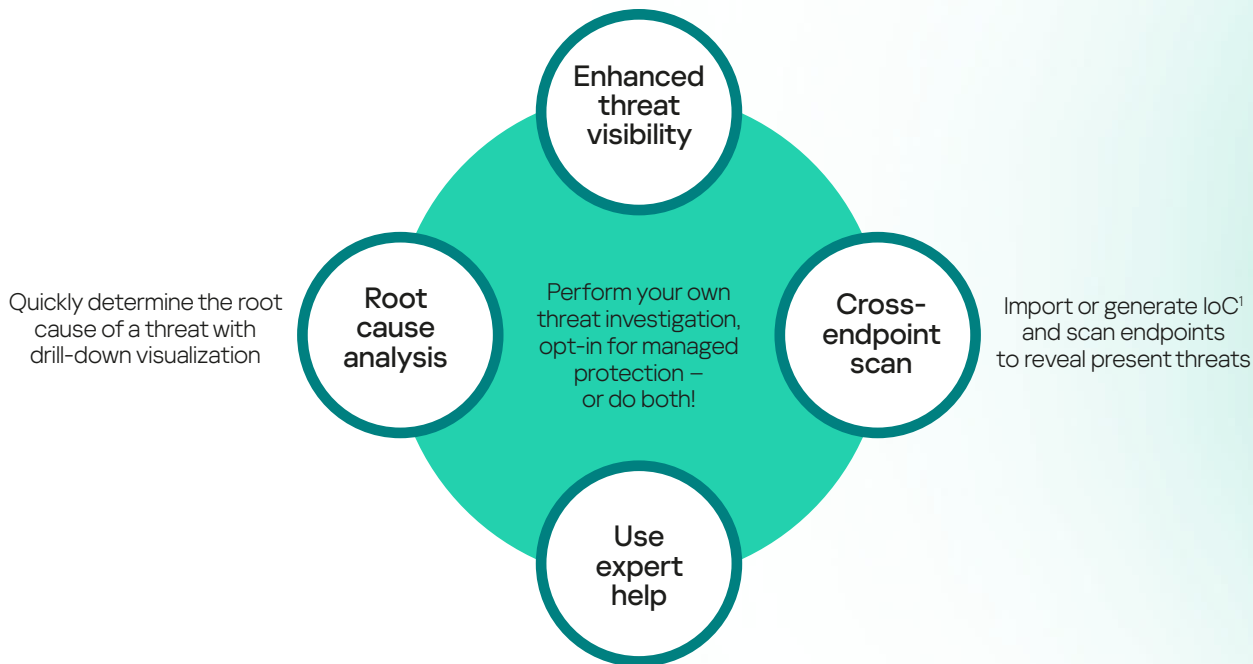


Kaspersky Endpoint Detection and Response (EDR)



Kaspersky Security Awareness

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



Kaspersky experts use leading TI² and AI-enabled tools to analyze your threat data

¹Indicator of compromise
²Threat intelligence

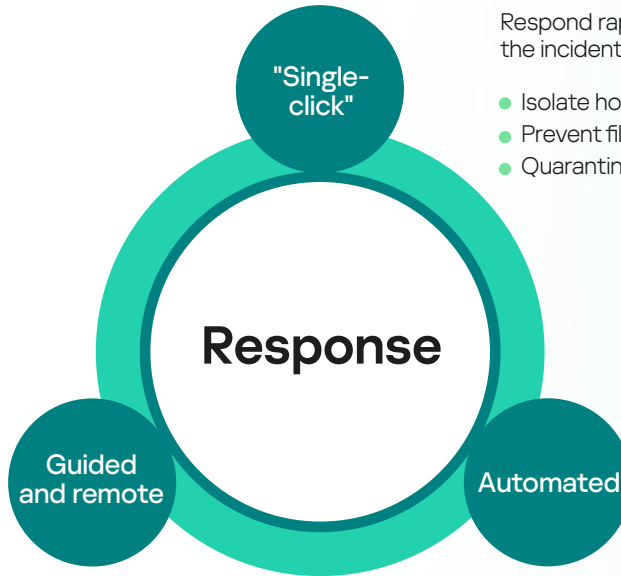
Key products:



Kaspersky
Endpoint Detection
and Response (EDR)
Optimum



Kaspersky
Managed Detection
and Response (MDR)
Optimum



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 IoCs¹ of identified threats, with automated response applied instantly – all through a simple checkbox

¹Indicators of compromise

Key products:



Kaspersky
Endpoint Detection
and Response (EDR)
Optimum



Kaspersky
Managed Detection
and Response (MDR)
Optimum

Fights evasive threats on multiple levels



Penetration

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

Employee security awareness

Attack surface reduction

Automatic threat prevention



Installation

Initial infection deploys the necessary components, communicates with C&C¹ and explores its surroundings

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

Automated threat hunting with IoAs²

Automated, guided and managed responses



Rooting

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

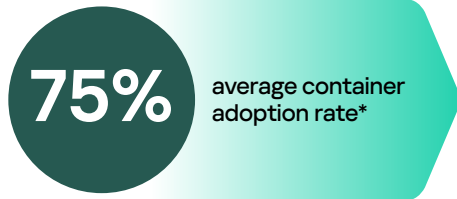
Root cause analysis and IoC³ scanning

¹Command and control

²Indicators of attack

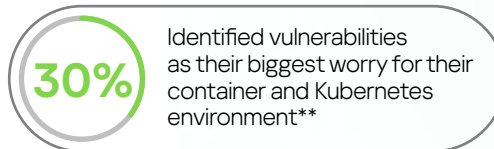
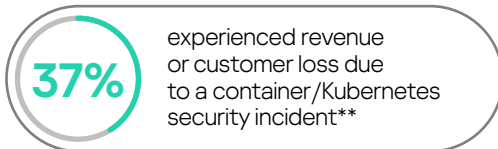
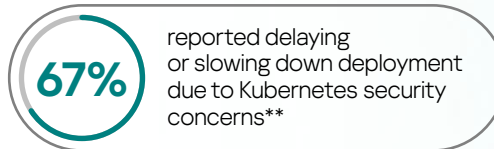
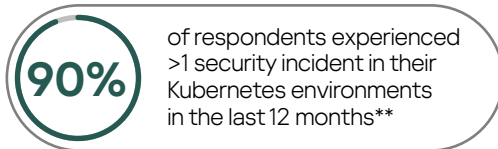
³Indicators of compromise

Containerization is the new normal



- Speeds up coding, debugging and launching a release
- Improves application stability
- Reduces infrastructure requirements for both the developer and the customer
- Simplifies scaling

But:



Traditional application protection tools were developed for other platforms (VM, bare metal) and cannot protect container platforms due to differences in architecture – in particular, the lack of an operating system in each container.

* CNCF 2023

** Red Hat Summit 2023

How Kaspersky Container Security deals with these challenges



VCS & Registry

- Checks images from a registry
- Scans configurational files (IaC, Dockerfile) for errors and confidential information



CI tools

Scans images for vulnerabilities, malware and confidential information



CD tools

Ensures delivery of images that comply with security policies



Orchestrator

- Checks network interaction for security policies compliance
- Behavioral analysis of containers

Who's it for?

Company profile

- Medium and large businesses with internal or custom development of containerized apps for various industries

Audience

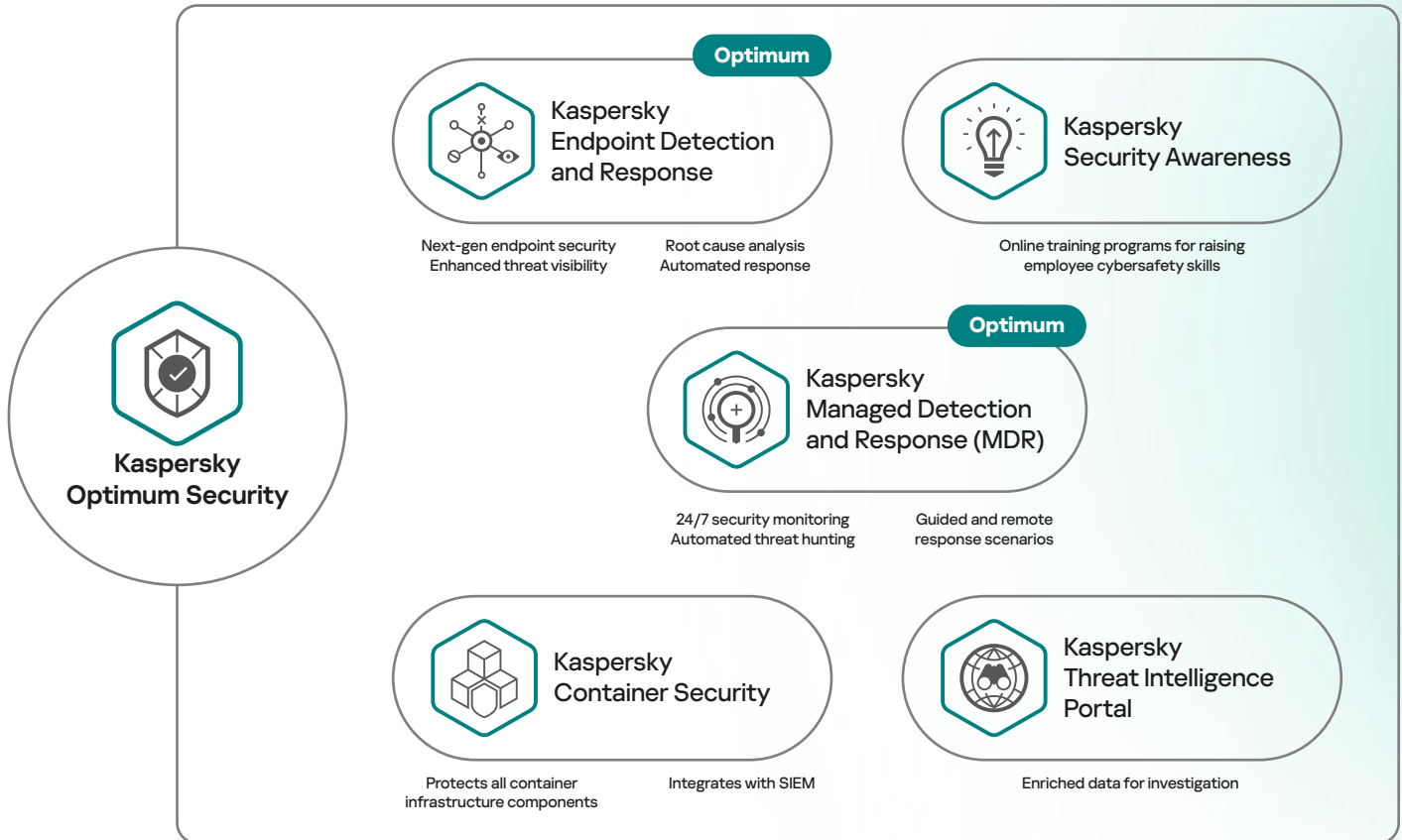
- IT security or allocated DevSecOps (CISO) teams
- DevOps and/or IT (CIO) teams

Key products:



Kaspersky
Container
Security

Kaspersky Optimum Security is built to protect against evasive threats



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 stop commodity cyberthreats on any device, VDI and hybrid server infrastructure automatically. 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
- Limited cybersecurity resource
- 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
- Relieves corporate IT teams of tedious deployment and maintenance tasks while ensuring better ROI thanks to optimized configurations

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.

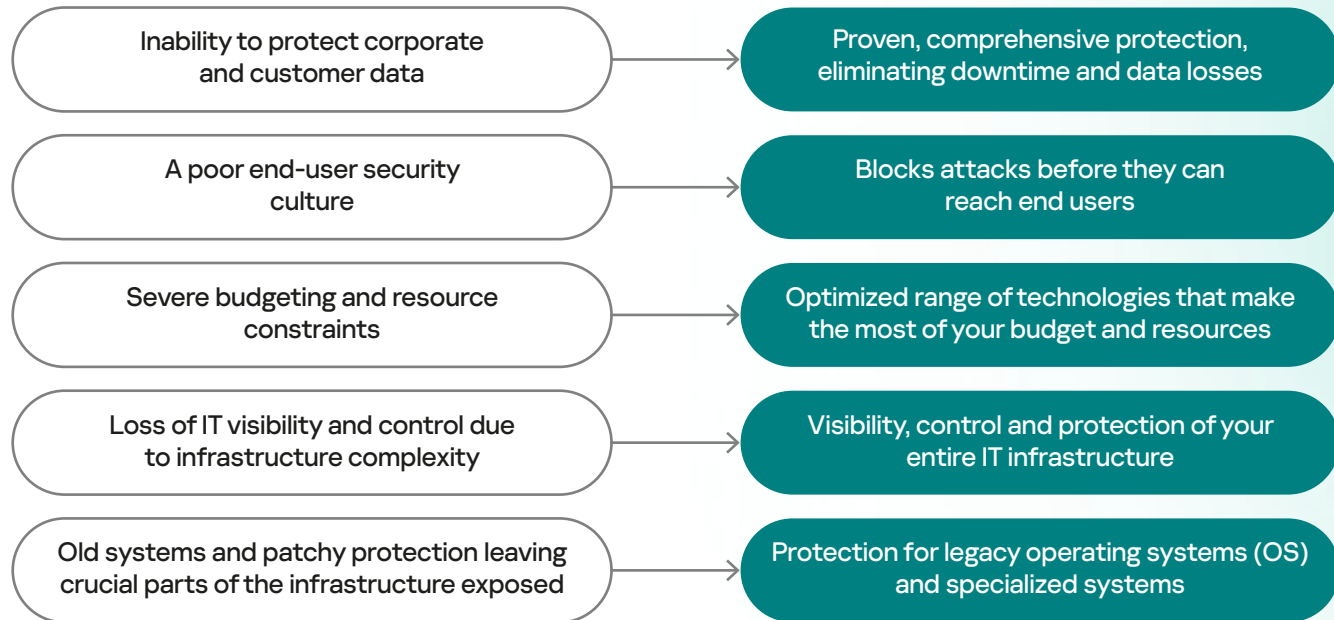
A broad range of devices and IT network functions must be united to function as a single – and secure – whole.

Getting all this under control is a constant struggle.

What's holding you back?

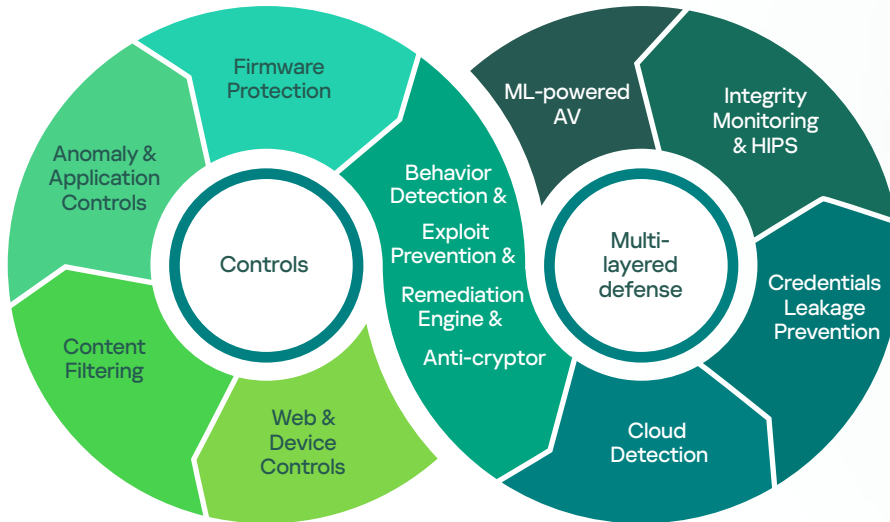
- The inability to ensure protection of corporate and customer data from exposure and loss
- A poor end-user security culture
- Severe budgeting and resource constraints
- Loss of IT visibility and control
- Old systems and patchy protection, leaving crucial parts of the infrastructure exposed

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 and limit or block the activities of apps capable of threatening 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

[Read more](#)



Kaspersky
Hybrid Cloud
Security

[Read more](#)



Kaspersky
Security for
Mail Server

[Read more](#)



Kaspersky
Security for Internet
Gateway

[Read more](#)



Kaspersky
Embedded System
Security

[Read more](#)

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, maximizing 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
[Read more](#)

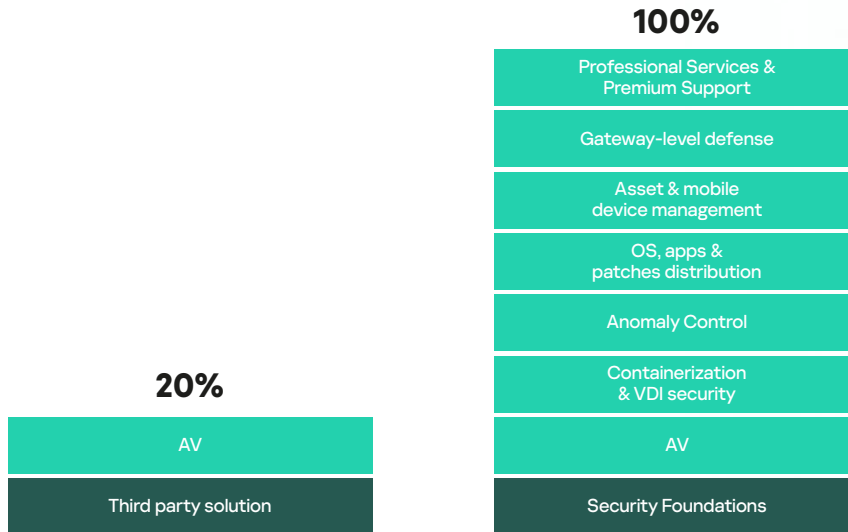
 Kaspersky Hybrid Cloud Security
[Read more](#)

 Kaspersky Security for Mail Server
[Read more](#)

 Kaspersky Security for Internet Gateway
[Read more](#)

Optimized range of technologies that maximizes 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
[Read more](#)



Kaspersky
Hybrid Cloud
Security
[Read more](#)



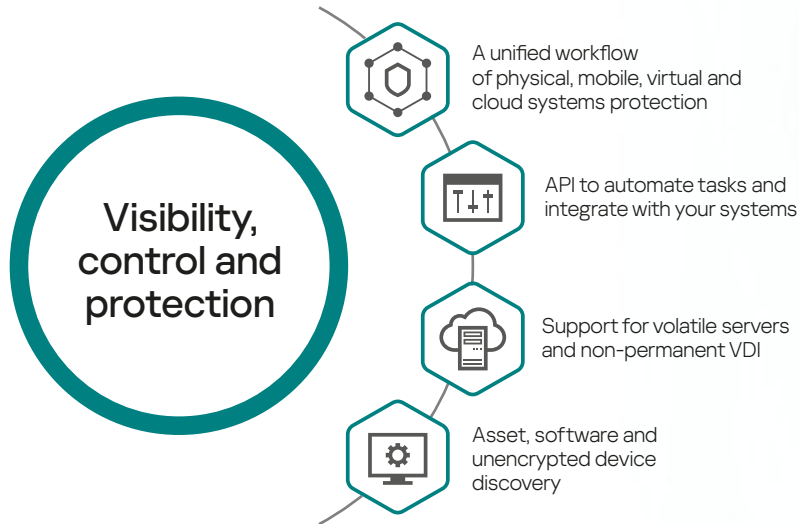
Kaspersky
Security for
Mail Server
[Read more](#)



Kaspersky
Security for Internet
Gateway
[Read more](#)

Visibility, control and protection of 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

[Read more](#)



Kaspersky Hybrid Cloud Security

[Read more](#)



Kaspersky Security for Mail Server

[Read more](#)



Kaspersky Security for Internet Gateway

[Read more](#)

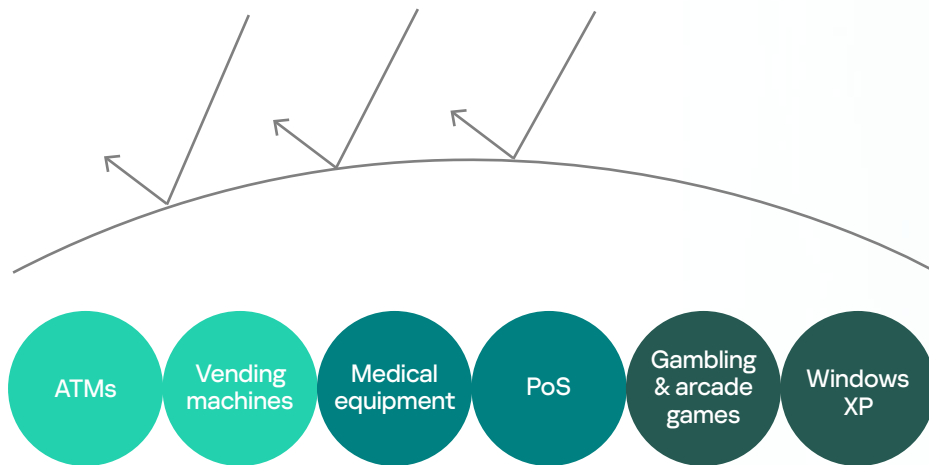


Kaspersky Embedded System Security

[Read more](#)

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

[Read more](#)

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.

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.

Unified management of whole IT estate

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

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 Industrial CyberSecurity

[Back to contents](#)

How we protect industrial enterprises



Visibility

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



Risk management

We help to enforce policies, assign controls and stop threats without compromising processes



Centralization

We help to quickly respond to incidents, easily replicate successful deployments and manage complex distributed infrastructure

Solution for industrial enterprises



Kaspersky Single Management Platform

A platform of natively integrated technologies, training and expert services

Platform



Kaspersky Industrial CyberSecurity



for Nodes

Endpoint Protection, Detection and Response



for Networks

Network Traffic Analysis, Detection and Response

Services

Training and Awareness



Kaspersky Security Awareness



Kaspersky Cybersecurity Training



Kaspersky Threat Intelligence



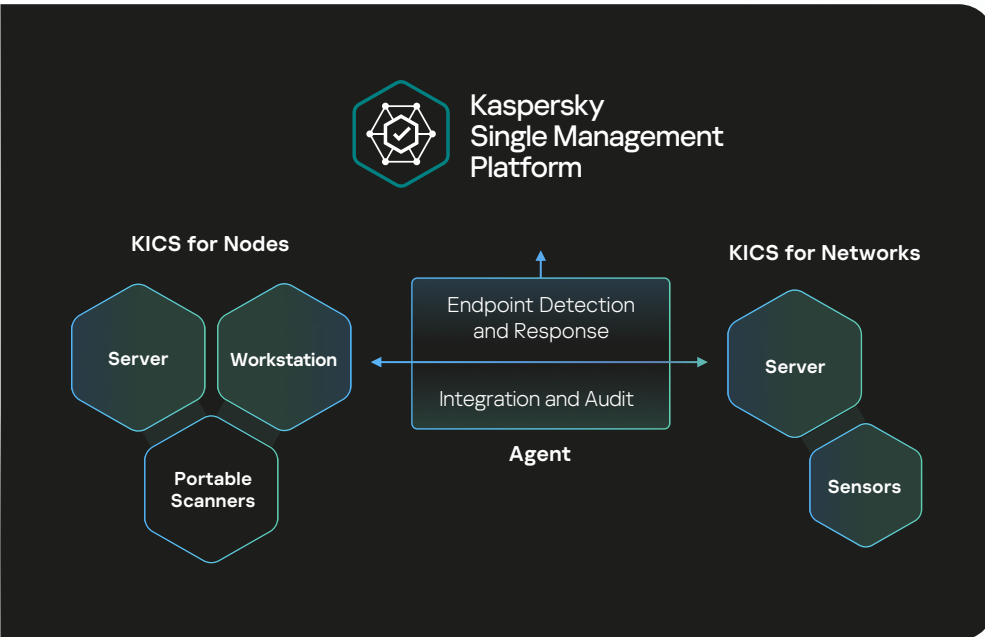
Kaspersky Security Assessment



Kaspersky Incident Response

Expert Services and Intelligence

Platform architecture and main function



Network detection and response

Network traffic analysis and endpoint sensors to detect intrusions on the lowest level (ICS Protocols DPI and IDS signatures)

Risk and asset management

Passive detection of OT components and vulnerabilities. Optional active polling, risk-oriented situational awareness and reporting

Endpoint detection, response and audit

Anti malware, software & device whitelisting and more. ICS EDR enables root cause analysis of incidents in OT

Kaspersky Industrial CyberSecurity's holistic approach



Training and Awareness

- Professional education in incident response and investigation in OT
- Basic trainings for OT specialists



Assessment and other Security Services

- Penetration testing
- Cybersecurity assessments
- APT reports
- Managed detection and response service
- ICS-CERT consulting



Threat Intelligence

- Vulnerability research and malware database



Incident Response

- IR and forensics service (remote and onsite)
- Handbook preparation and simulation

Key differentiators

Certified

Industrial vendors confirmed that over 150 of their automation systems are compatible with the Kaspersky Industrial CyberSecurity platform.

Compliant

Designed and tested to be compliant with various critical national infrastructure requirements, best practices and international standards.

Efficient

We protect industrial enterprises. From one site to global operations, our solution guarantees performance, efficacy and great scalability.

Future-proof

An open platform, ecosystem of products, great integration capabilities and 25+ years of success make Kaspersky a reliable supplier for more than 600 industrial enterprises worldwide.



Kaspersky SASE

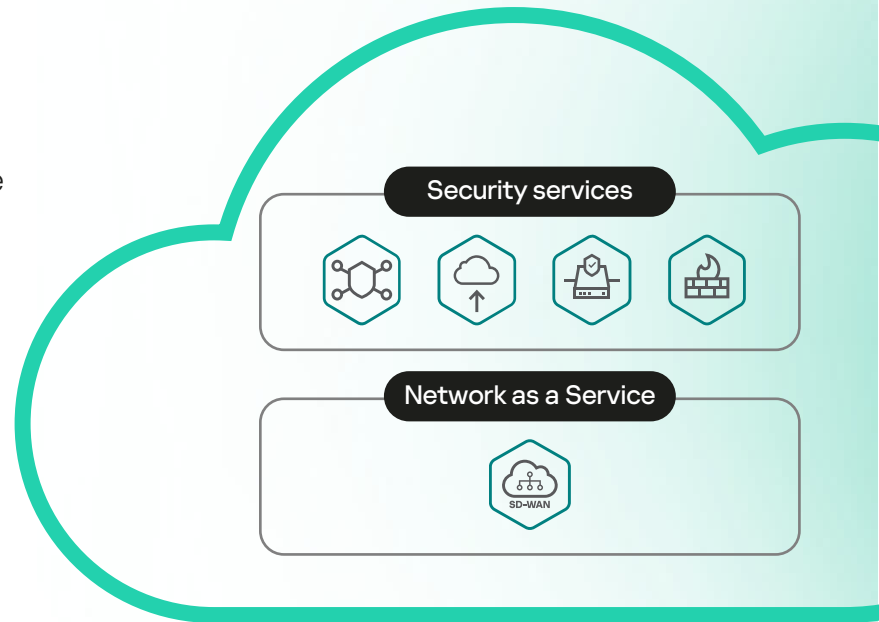
[Back to contents](#)

SASE – Secure Access Service Edge

SASE refers to network and security services synergy, which aims to provide agile and reliable networks, while shifting from different security solutions to unified security available from a private or public cloud.

With SASE, the whole company network is secured, regardless of where your users are or how they connect to it.

SD-WAN technology is an essential step in building unified security on top of a reliable distributed network.





Reliable network and security capabilities rolled into one



Easy scalability

Connect new locations with a zero-touch experience to meet constantly changing business demands



Convenient management

Manage your entire network from a single console, modifying security policies and traffic filtering rules



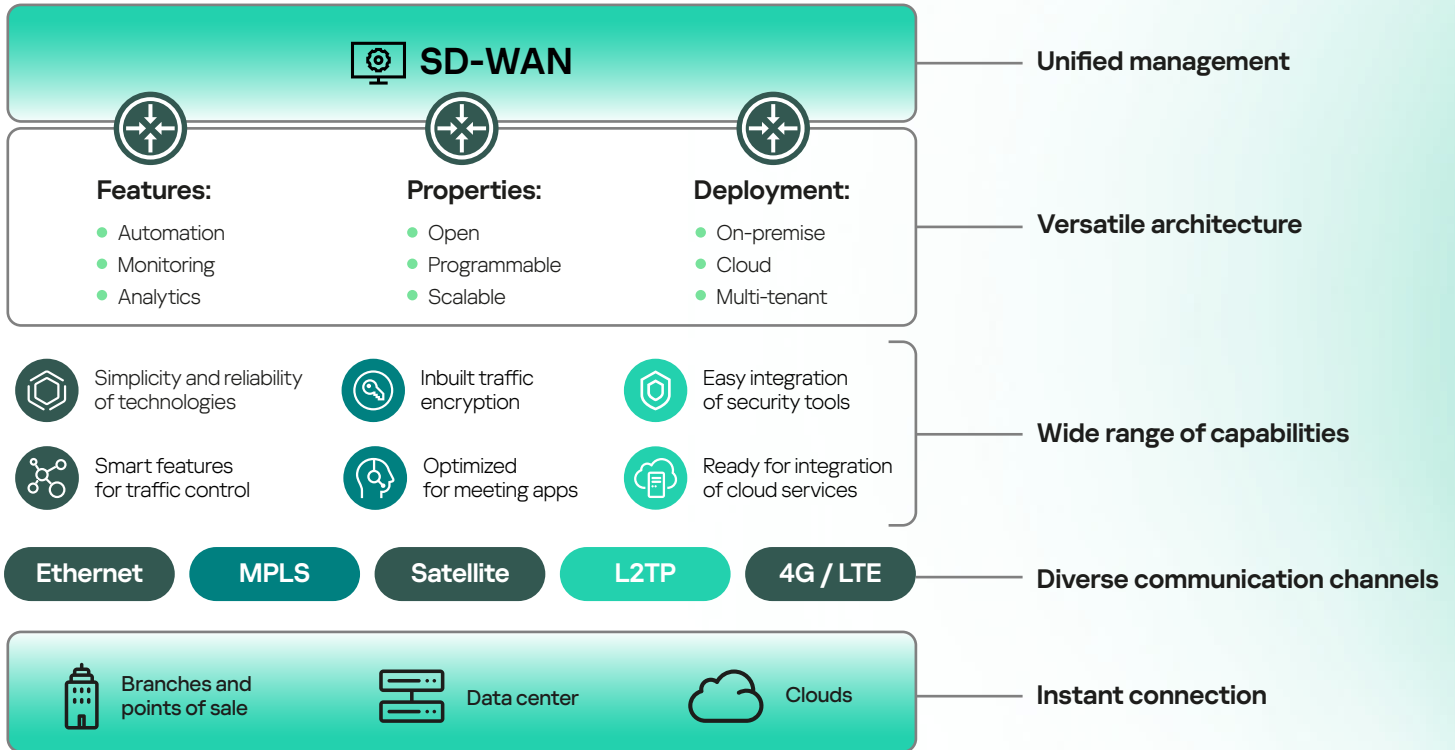
Cost optimization

Reduce infrastructure costs, converging separate communication channels and network functions

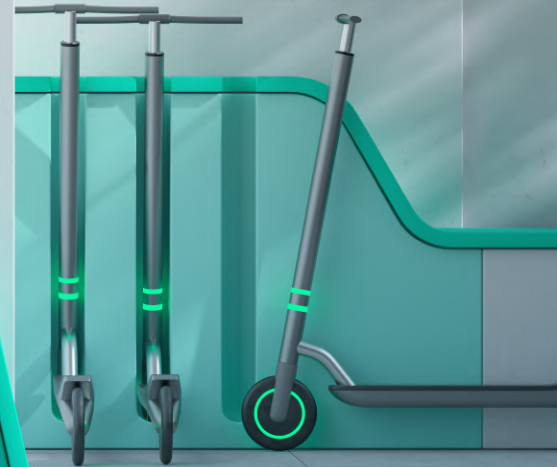


Centralized security

Automatically deploy virtualized traffic control and security tools through the VNF manager



Kaspersky Security for Small and Medium-sized Businesses



[Back to contents](#)

Security challenges faced by SMBs

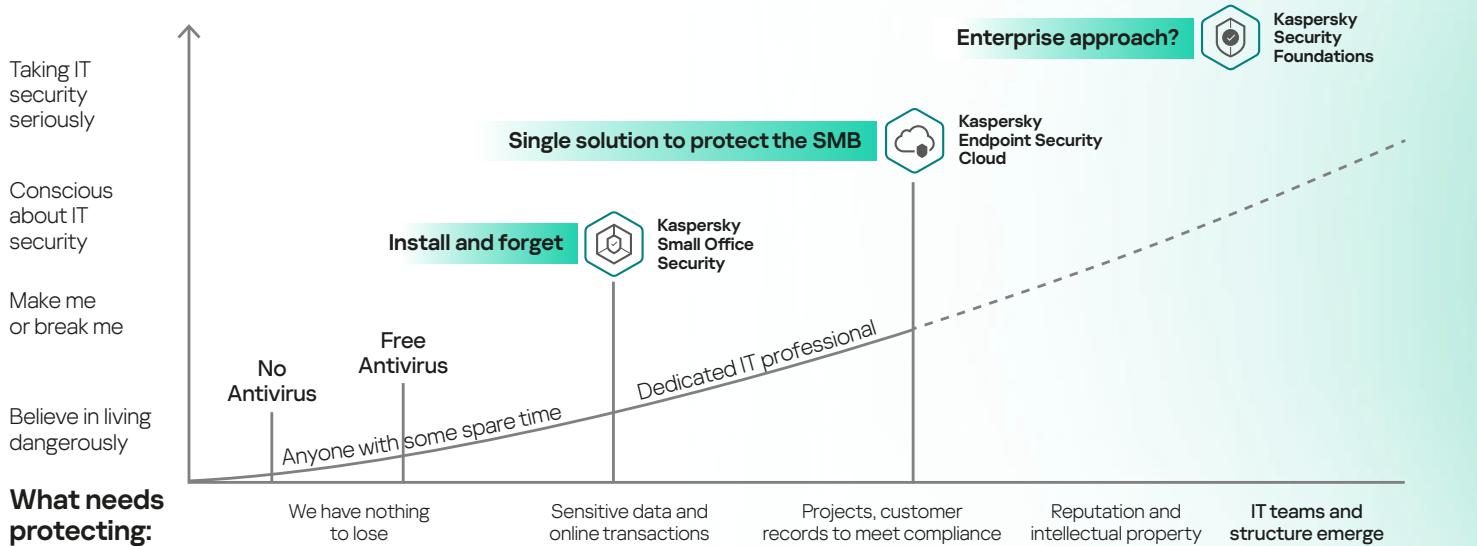
Cyberthreats

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.

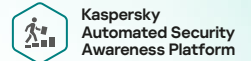
Overstretched resources

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 stretched. 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



Improve cybersecurity awareness





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, 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

[Read more](#)



Kaspersky Endpoint Security Cloud

Kaspersky Endpoint Security Cloud provides a single solution for all your organization's IT security needs. You can ensure 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 responsible for all IT tasks; and 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 25 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 doesn't require dedicated resources or any special cybersecurity knowledge to launch and manage

[Read more](#)

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 pressure 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, as it plays 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



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

www.kaspersky.com