Cybersecurity portfolio for business

kaspersky

Kaspersky Security for Small and Medium Businesses

Security challenges SMBs face

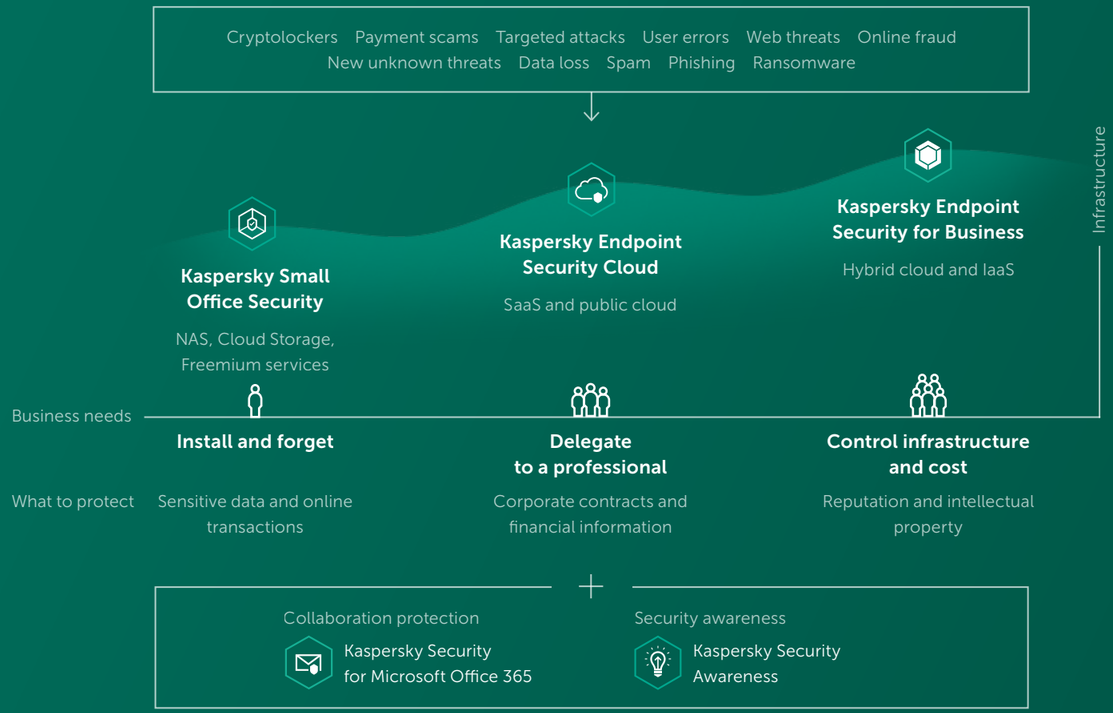
Cyberthreats

One size doesn't fit all. Smaller businesses face many of the same cyberthreats as large enterprises. But they 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 are running a small or medium sized business, the chances are that resources are continuously 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.

Effortless protection which evolves as your business matures



Choose your strategy

Advantages of cloud-based endpoint protection management

Quick-start endpoint protection with a Security-as-a-Service solution that makes minimal demands on your budget, time and energies.

- No extra server or software deployment costs
- Protection for any endpoint – with free mobile device security
- Instant protection with predefined security policies
- Always the latest, most up-to-date software

Advantages of on-premises endpoint protection management

Future-proof security that enables business transformation by fully protecting against even the most advanced threats and separating responsibilities, giving you more time to focus on business needs.

- Scales easily, securing diverse environments and platforms
- Flexible policies, with the freedom to choose when to migrate to new versions
- Powerful security and control for any static or mobile device

Kaspersky Small Office Security

cloud-based

Kaspersky Small Office Security is designed specifically for very small businesses without IT specialists. It's easy to install, even easier to manage, and provides the world's most tested, most awarded security to computers, file servers, laptops and mobile devices, while protecting your business from online attacks, financial fraud, ransomware and data loss.

Ideal for organizations looking for hassle-free 'install and forget' protection

Business benefits

- Installs in under 10 minutes
- Out-of-the-box security that's easy to use – simply set and forget
- Secures sensitive data and protects your business from data breaches, fines and lost business

Use cases

- Multiple layers of protection in one easy-to-use package
- No experience needed to get maximum security across your business with minimum fuss

Kaspersky Endpoint Security Cloud

cloud-based

Kaspersky Endpoint Security Cloud offers small and medium sized businesses effortless yet complete cloud-based protection against known and unknown threats – including cryptors, ransomware and other attacks. We do this without making demands on your time or budget, because we know just how over-stretched business resources can be.

Ideal for businesses looking for instant and easy-to-use cloud-based protection

Business benefits

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

Use cases

- Simply protect your business, without sacrificing IT resources, time, or budget.
- Automated solution to reduce IT costs and free up resources

Kaspersky Security for SMB

Kaspersky Endpoint Security for Business

on-premises

Kaspersky Endpoint Security for Business is designed for mixed IT environments, and incorporates a flexible web console together with a full stack of proven technologies. As well as securing all your endpoints and servers, it delivers adaptive security layers to protect

Ideal for organizations with more sophisticated IT security needs

Business benefits

- Scales easily, without limits
- Policies are granular for businesses of any size
- Works natively with your systems
- All settings are under your control
- Freedom to choose when to upgrade

Use cases

- Fully protects against even the most advanced threats
- Adaptable to your unique business needs
- Supports compliance initiatives
- Streamlines and automates routine IT tasks, freeing up your time tasks

1 Skills required

5 Customization and scalability

2 Cost

Kaspersky Security for Microsoft Office 365

cloud-based

Kaspersky Security for Microsoft Office 365 is the number one choice when it comes to protecting your cloud-oriented business from known and unknown email-borne threats. It instantly halts the spread of phishing, ransomware, malicious attachments, spam and business email compromise (BEC) attacks, and requires no specialist IT skills to install and use.

Ideal for Microsoft Office 365 adopters looking for an additional layer of protection

Business benefits

- Advanced corporate mailbox protection you can rely on
- Doesn't affect user productivity — no email delay, no latency
- No missed emails
- Supports GDPR and data compliance

Use cases

Advanced Microsoft Office 365 protection even for non security-savvy users.

2 Skills required

2 Customization and scalability

1 Cost

Kaspersky Security Awareness cloud-based

Kaspersky ASAP changes employees' behavior, providing them with the skills to protect the business and help create a cybersafe environment for everyone. ASAP is built on the principle of interval learning with constant reinforcement to develop 'pattern perception': employees are able to recognize new dangers and behave safely, even when faced with unknown threats.

Ideal for all types of organizations, especially those interested in instant program set-up and hassle-free management

Business benefits

- Incremental learning with skill-based lessons: employees acquire a new skill every day
- Automated learning management saves hundreds of platform management hours each year
- All lessons are connected with employees' everyday working life
- Supports GDPR and data compliance

Use cases

Creates a 'human firewall' to protect your business from within

Kaspersky MSP Partner Program Kaspersky Managed Service Providers Program

Our security portfolio for MSPs includes flexible, powerful tools to secure, monitor and manage customer infrastructure — all from a single, easy-to-manage console. Deliver the next generation of cybersecurity solutions to your customers' physical and virtual infrastructure, on-premises or from the cloud.

Ideal for Managed Service Providers focused on offering high-quality IT security services

Business benefits

With easy multi-tenant capabilities, our light-yet-powerful tools enable you to deploy and manage security solutions for all your customers from a single console, with no need for additional hardware.

Integration

Our security solutions are integrated with the most popular RMM and PSA platforms:

- ConnectWise® Automate™
- ConnectWise® Manage™
- Autotask®
- Tigerpaw® One
- SolarWinds® N-central®

Supported products

Kaspersky Endpoint Security for Business Advanced

Kaspersky Endpoint Security for Business Select

Kaspersky Endpoint Security Cloud

Kaspersky Security for Microsoft Office 365

Kaspersky Hybrid Cloud Security

Kaspersky Automated Security Awareness Platform (ASAP)

Kaspersky Security for Enterpise

About the Kaspersky Enterpise Portfolio

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

Kaspersky's Enterprise Portfolio reflects the security demands of today's businesses, responding to the needs of organizations at different levels of maturity with a step-by-step approach. This approach combines different layers of protection against all types of cyberthreat to detect the most complex attacks, respond quickly and appropriately to any incident, and prevent future threats.

The role of endpoint security in long-term planning

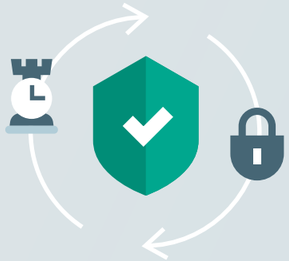
Traditional security evolution process

Decision-making:

- Market trends
- Siloed security solution
- ‘Firefighter’ approach
- Driven by compliance

Leveraging traditional products:

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

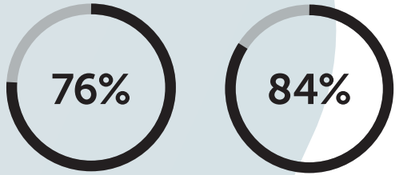


Attributes

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

Why traditional approaches fail

- Growing complexity of threats and the threat landscape
- Complexity of cybersecurity technologies
- Business requirements for a long-term cybersecurity strategy



Of all alerts are generated by endpoints

Of all endpoint breaches involve more than one endpoint

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 effective investigation of complex incidents.

3 steps towards advanced cybersecurity planning for enterprises

1 Security Foundations

Harden systems and block the maximum possible number of threats automatically.

Broader Threat Landscape

Endpoints	Network	Cloud	Support	Data	People
Kaspersky Endpoint Security for Business	Kaspersky Embedded Systems Security	Kaspersky Secure for Mail Server	Kaspersky Security for Internet Gateway	Kaspersky Hybrid Cloud Security	Kaspersky Premium Support and Professional Services	Kaspersky Security for Storage	Kaspersky Security Awareness

2 Advanced defense

Focus on advanced detection and a fast response to those complex threats missed by preventive protection.

Advanced threats and targeted attacks

Endpoints	Services	Network	Intelligence	People	Privacy
Kaspersky Endpoint Detection and Response	Kaspersky Targeted Attack Discovery Service	Kaspersky Anti Targeted Attack	Kaspersky Threat Intelligence	Kaspersky Cybersecurity Training	Kaspersky Private Secutity Network

3 Integrated cybersecurity approach

Readiness for APT-level attacks. High level of expertise, advanced threat intelligence capabilities and continuous threat hunting.

Targeted campaigns and cyber-weapons

Kaspersky Threat Management & Defense

4 business benefits of this approach

- Forms the basis for development of a long-term cybersecurity strategy, taking into account the specifics of the business and trends in the threat landscape.
- Optimized investment in security technology and reduced TCO.
- Reduced financial & operational damage caused by cybercrime.
- Increased ROI through seamless workflow automation and no disruption to business processes.

1 Security Foundations

Automated preventive technologies and security awareness

Blocking the maximum possible number of threats

Ideal for smaller enterprises that have no dedicated security team or very limited cybersecurity expertise

- Multi-vector automated prevention of a large number of possible incidents caused by commodity threats
- The fundamental step for mid-to-large enterprises in building an integrated defense strategy against complex threats

Endpoints

- Kaspersky Endpoint Security for Business
- Kaspersky Embedded Systems Security

Cloud

- Kaspersky Hybrid Cloud Security

Network

- Kaspersky Secure Mail Gateway
- Kaspersky Security for Internet Gateway

People

- Kaspersky Security Awareness

Data

- Kaspersky Security for Storage

Support

- Kaspersky Premium Support
- Kaspersky Professional Services

Kaspersky Endpoint Security for Business

The majority of cyberattacks against enterprises start at an endpoint. Limited prevention and automation capabilities result in specialists becoming overloaded with security incidents. Every endpoint has the potential to become a root cause of business disruption; Kaspersky Endpoint Security for Business prevents threats and hardens endpoints by combining adaptive security with extended control tools. Threats are blocked before they can damage data or undermine user productivity, even when the endpoint is not inside the corporate perimeter.

Ideal for

Organizations whose expectations of IT are growing and diversifying

Organizations wanting to reduce the opportunities for, and frequency of, user error leading to security breaches

1 Skills required

5 Customization and scalability

2 Cost

Business benefits

Prevents business interruption and human error

Supports digital transformation and secures mobile workforces

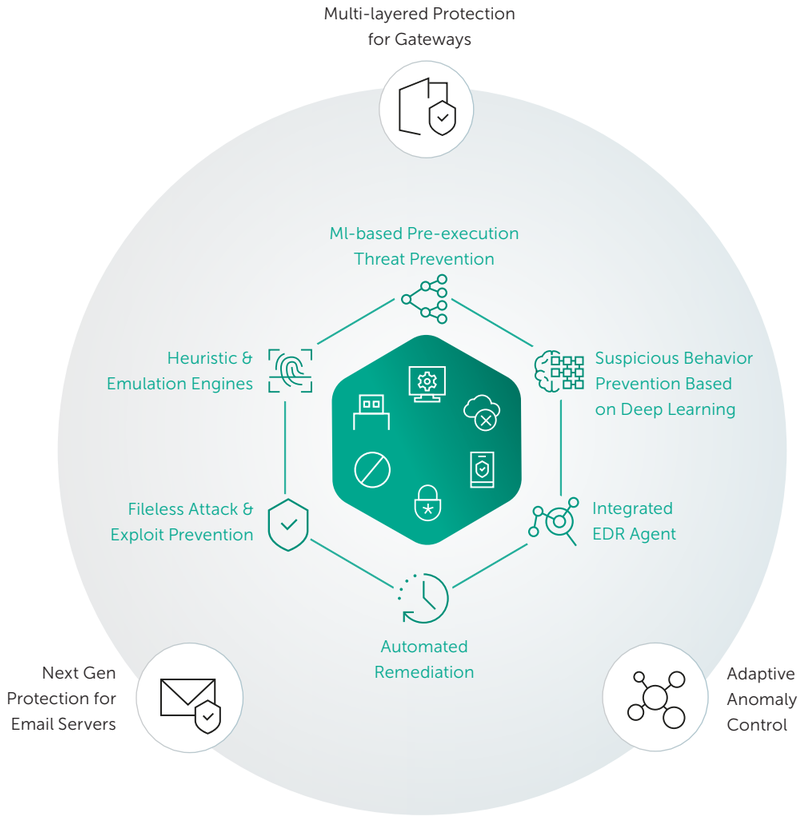
Improves audit-readiness – hunts and fixes vulnerabilities, 'configuration drift', and unencrypted devices

Maximizes ROI by reducing the attack surface and the number of incidents to manage

Enables control of every endpoint, thanks to an integrated console and unified agent

Use cases

- Reduces exposure to attack by applying adaptive hardening, protecting endpoints, email and file servers, and internet gateways
- Ensures endpoint compliance with regulatory requirements
- Automates detection, response and software deployment tasks, freeing up security specialists' time
- Streamlines the integration and adoption of other security technologies



Kaspersky Hybrid Cloud Security

Hybrid Cloud Security is a solution that simplifies and secures the digital transformation, as organizations virtualize or move workloads into the cloud. Patented Light Agent technology allows centralization and smart optimization of the security function, significantly lowering hypervisor resource use. Native integration with a wide range of virtualization, container and public cloud platforms provides consistent visibility and control throughout the whole infrastructure. A full stack of security technologies managed from the same console ensures streamlined risk management in diverse environments a day-to-day basis.

Ideal for

Enterprises that virtualize server and desktop workloads

Organizations that are moving or maintain infrastructures in, public clouds

Enterprises leveraging public clouds and containers for DevOps

Business benefits

Ensures consistent visibility and control across datacenter and cloud deployments

Reduces attack surface and dwell time, complicating lateral movement

Frees up to 30% of hypervisor resources, and cuts login time from minutes to seconds

Supports compliance

Ensures efficient collaboration between IT, Information Security and Development teams, reducing risk and security gaps

Use cases

- Resource-cautious protection for virtualized server infrastructures
- Security for VMWare and Citrix VDI
- Enables compliance by meeting core security requirements
- Cloud workload protection for AWS and Azure instances with automated deployment and consistent visibility through native API integration
- Security for DevOps with container protection and management API

Kaspersky Security for Mail Server

Kaspersky Security for Mail Server protects against mail-based threats, preventing them from reaching the endpoint where most social engineering and malware work. All kinds of malware - including ransomware and miners – are blocked, as well as phishing attempts, with special attention to the prevention of Business Email Compromise. The solution also blocks undesired mass mailing and prevents unwanted data transmissions.

Ideal for

Any business with well-developed IT and concerns about privacy and data safety

Any business relying heavily on email communications and requiring granular management

Enterprises wanting to enrich their APT detection data with email context, and block email-borne APT components

Business benefits

Increases productivity by blocking unwanted mass mails – including spam – and offering mail categories for more convenient communications management

Helps prevent business disruption by blocking email-based threats

Boosts data security by preventing the transfersof undesirable data types

Helps cut service overheads by reducing user-level incidents

Boosts the effectiveness of the existing mail gateway security by adding superior detection capabilities – without added false positives

Use cases

- Works with a broad range of external Mail Transfer Agents or as an all-in-one virtual appliance.
- Provides API-integrated mail security for Microsoft Exchange servers, operating at both gateway and mailbox levels
- Blocks he transfers of undesirable file types
- Integrates with Kaspersky Anti Targeted Attack to block email-borne APT components

Kaspersky Security for Internet Gateway

Kaspersky Security for Internet Gateway delivers protection against web-based threats at the level of the corporate defensive perimeter, preventing them from reaching the number one final target for all forms of attack — the endpoint. The solution helps prevent attacks based on social engineering, and blocks all kinds of malware — including ransomware and miners – as well as phishing attempts. Pair with your existing corporate proxy for enhanced performance, or deploy as a ready-to-use, all-in-one virtual appliance.

Ideal for

Any business with developed IT and concerns about privacy and data safety

MSPs and xSPs (including Telecom providers)

Business benefits

Prevents business disruption by blocking web-based threats before somebody clicks and lets them in

Boosts the effectiveness of existing web gateway security, adding superior detection capabilities without adding false positives

Helps cut service overheads by reducing the number of user-level incidents

Boosts productivity & reduces risk by governing internet usage and the transmission of specific file types

Use cases

- Blocks malicious and phishing web resources and downloaded malware
- Prevents the use of undesirable web resources
- Enables the management of separate workspaces with their own sets of rules
- Filters out undesired file types travelling both ways, based on multiple criteria
- Integrates with Kaspersky Anti Targeted Attack as a web sensor – and blocks targeted attacks components according to advanced detection results

Kaspersky Security for Storage

Easily accessible connected storage can readily become a source of infection across the entire infrastructure – and a target for threats like ransomware. Kaspersky Security for Storage safeguards corporate' data and prevents network contagion with a solid stack of protective technologies powered by global threat intelligence. Includes unique features such as Remote Anti-cryptor, enabled by integration with storage system APIs.

Ideal for

Any business with developed IT and privacy or data safety concerns

Businesses, such as banking, e-commerce and insurance, that work with large volumes of sensitive/private data

Business benefits

Protects data on connecting storages without intruding into the storage's software

Reduces administrative hassle and boosts security thanks to a single-point-of-view management console

Preserves business continuity by keeping stored data safe from remotely running ransomware and crypto-wipers

Supports compliance by offering security for a broad range of models that can then be used as Regulated Storage

Use cases

- Secures both network-connected storages and the server it runs on
- Whenever a new file appears in the secured storage, or an existing file is changed, it is checked for maliciousness. On demand scans are also possible
- When files start being encrypted from afar, the solution detects and blocks the source on the network, preventing further damage*

* Only with API integration available for some storages

Kaspersky Embedded Systems Security

Featuring powerful threat intelligence, real-time malware detection, comprehensive application and device controls and flexible management, Kaspersky Embedded Systems Security provides all-in-one security designed specifically for embedded systems.

Ideal for

Financial Services

Retail and Transport

ATM and POS service providers

Business benefits

Mitigates the risks associated with threats targeting specific financial infrastructures

Meets the compliance requirements of regulations such as PCI/DSS, SWIFT, etc.

Optimizes administrative costs through a single management console

Use cases

- Secures geographically scattered and rarely updated embedded systems that present specific and unique security concerns
- Protection for unsupported Windows XP, still widely used on low-end hardware
- Efficient design delivers powerful security with no risk of systems overload

2 Skills required

5 Customization and scalability

3 Cost

Kaspersky Premium Support (MSA) service

When a security incident occurs, the time taken to identify the cause and eliminate it is critical. Rapidly detecting and solving an issue can save businesses significant costs. Our Maintenance Service Agreement (MSA) plans are specifically designed to achieve this goal. Round-the-clock access to our experts, appropriate and informed issue prioritization with guaranteed response times and private patches - everything needed to ensure your issue is solved as soon as possible.

Ideal for any organization using Kaspersky products

Business benefits

Ensures business continuity with allocated experts on standby, tasked with taking ownership of your issue and achieving the swiftest possible resolution

Reduced cost of a security incident though access to a priority support line, guaranteed response times and private patches

A dedicated Technical Account Manager acts as your representative inside Kaspersky Lab with the authority to mobilize any expertise needed to quickly resolve the issue

Use cases

- Fast-track critical issues straight to those behind-the-scenes specialists at Kaspersky, headquarters who are best equipped to provide the right solution for you, at speed
- Proactive measures tailored to your system, including prioritized hot fixes and personalized patches, keep you fully protected
- Reduce the time spent on maintenance and troubleshooting by your valuable in-house resources

1 Skills required

5 Customization and scalability

3 Cost

Kaspersky Professional Services service

Cybersecurity is a big investment. Get the most out of yours by engaging with experts who understand exactly how you can optimize your security to meet the unique requirements of your organization. Working in accordance with our established best practices and methodologies, our security experts are available to assist with every aspect of deploying, configuring and upgrading Kaspersky products across your enterprise IT infrastructure.

Kaspersky Professional Services comprise:

- Implementation and Upgrade
- Configuration
- Product Training

Ideal for any organization using Kaspersky products

Business benefits

Maximizes your ROI on your security solutions by ensuring they perform at 100% capability

Reduces costs for internal IT staff

Minimizes the risks of downtime through periodic audits of product configurations, ensuring the most up-to-date defensive mechanisms are in place

Reduces the product adoption period, allowing all the benefits to be extracted faster from the product implemented

Use cases

- Reduces the risks of implementation that can diminish protection, adversely impact productivity and even lead to downtime
- Minimizes the impact of implementing your new security solution on everyday business operations and lowers overall implementation costs
- Prepares your staff to undertake ongoing product maintenance with our product training programs, helping to prevent mistakes, demonstrating product compatibilities and explaining operational principles

Kaspersky Security Awareness

Our computer-based training programs change habits and form the new behavior patterns that are the real goal of awareness training. The Kaspersky Security Awareness training portfolio includes: Automated Security Awareness Platform (ASAP) – awareness training for all employees that builds concrete cyber-hygiene skills day after day; Cybersecurity for IT Online (CITO) – training for generalist IT specialists that develops practical skills in how to recognize a possible attack scenario and to collect incident data; and Kaspersky Interactive Protection Simulation (KIPS) - cybersecurity gameplay for decision-makers.

Ideal for

Organizations whose expectations of IT are growing and diversifying

Organizations who want to reduce the opportunities for, and frequency of, user error leading to security breaches

Business benefits

Protects businesses from within

Maintains a high 'cybersafe mindset' throughout the corporate culture

Reduces human errors by up to 80%

Use cases

- Develops cybersafe behavior through typical scenarios and situations, cyberattack simulations, different tasks and explanations
- Builds an understanding of potential threats and provides the skills needed to deal with them
- Develops practical skills essential to recognizing a possible attack in an ostensibly benign PC incident, and collecting incident data for handover to IT Security
- Establishes a better security understanding among senior managers and decision-makers

2 Advanced defense

Advanced detection technology, and a centralized response

Maximum automation at the stage of detection and response to complex threats missed by preventive technologies

- Growing, increasingly complex IT environments with increased attack surface
- Runs a small security team with limited expertise
- Has basic incident response capabilities

Ideal for mid-enterprises:

Endpoint
Kaspersky Endpoint Detection and Response

People
Kaspersky Cybersecurity Training

Services
Kaspersky Targeted Attack Discovery

Network
Kaspersky Anti-Targeted Attack

Privacy
Kaspersky Private Security Network

Intelligence
Kaspersky Threat Intelligence

Kaspersky Endpoint Detection and Response

To defend yourself successfully against advanced threats at the earliest possible stage, it's essential to supplement preventive technologies with advanced endpoint detection and response capabilities. Kaspersky EDR is a specialized solution which addresses advanced threats to your endpoints, sharing a single agent with our world-leading Kaspersky Endpoint Security protection solution. Kaspersky EDR provides comprehensive visibility across all endpoints on the corporate network, enabling the automation of routine tasks in order to discover, prioritize, investigate and neutralize complex threats fast.

Ideal for

Enterprises

Organizations already using Kaspersky Endpoint Security

SOCs and incident response teams

4 Skills required

3 Customization and scalability

2 Cost

Business benefits

Mitigates the risks associated with advanced threats and targeted attacks

Optimizes administrative costs though task automation and a single, simplified, business-oriented interface

Increases the speed and effectiveness of incident processing, at no extra cost

Increases productivity, freeing up the time of your IT and security teams for other tasks

Supports compliance with internal security policies and regulatory requirements

Use cases

- Addresses the complete endpoint protection cycle, from automatic threat blocking to complex incident response against advanced threats, using a single agent
- Provides fast endpoint data access, even when compromised workstations are unavailable or data is encrypted
- Complements incident investigations with threat hunting, IoA analysis and MITRE ATT&CK mapping
- Enables an efficient response across distributed infrastructures, through wide-ranging automated actions

Kaspersky Anti Targeted Attack

The number and quality of targeted attacks is growing continuously. To counter these new emerging threats, it's necessary to constantly adapt your security systems. Kaspersky Anti Targeted Attack focuses on advanced threat detection at network level, with fully automated data collection, analysis and correlation, and provides a detailed understanding of the scope of the threat. The result is effective protection of your corporate infrastructure against complex threats and targeted attacks, without the need for additional resources.

Ideal for

Enterprises

SOC teams

MSSPs

Any organization under compliance

4 Skills required

3 Customization and scalability

5 Cost

Business benefits

Mitigates the risks associated with advanced threats and targeted attacks

Reduces financial and operational damage by introducing a single reliable system to protect against complex attacks

Optimizes administrative costs though task automation and a single simplified business-oriented interface

Streamlines tasks through seamless workflow automation, with no disruption to business processes

Use cases

- Rapid discovery of the actions of cybercriminals who bypass preventive technologies, through the centralized monitoring and control of potential entry points into the infrastructure
- The detection of threat signs and correlation of multi-vector events within an attack into a single picture, to enable more effective investigation
- Timely provision to the incident response team of all the necessary information about detected threats

Kaspersky Private Security Network

Kaspersky Private Security Network allows enterprises to take advantage of most of the benefits of global cloud-based threat intelligence, without releasing any data whatsoever outside their controlled perimeter. It's an organization's personal, local and completely private version of the Kaspersky Security Network.

Ideal for

Enterprises with strict data access control requirements

Critical Infrastructures with physically isolated networks

Telecom, managed security and other service providers

Business benefits

Empowers superior detection of the threats targeting your business

Ensures faster response times through real-time access to threat and reputation statistics

Increases operational efficiencies by minimizing false positives

Supports full compliance with regulatory requirements for the security of isolated systems and environments

Use cases

- All the benefits of cloud-assisted security – without the need to share information outside your controlled infrastructure
- Enables the building of customized protection by adding your own 'verdicts'
- Adapted for isolated critical networks

4 Skills required

4 Customization and scalability

5 Cost

Kaspersky Targeted Attack Discovery service

Kaspersky Targeted Attack Discovery is a comprehensive compromise assessment service that determines whether you are currently under attack, what's happening, and who the threat actor is. Our experts detect, identify and analyze ongoing incidents as well as those that occurred previously, and compile a list of systems affected by those attacks. We help you uncover malicious activities, identify the possible sources of an incident and plan the most effective remedial actions.

Ideal for

Enterprises with non-existent or immature security teams

Government institutions

Critical infrastructures

Business benefits

Prevents and minimizes the damage resulting from a systems compromise, significantly reducing the cost

Helps maintain the relationship of trust with your customers, partners, and investors, to further foster business opportunities

Ensures you avoid regulatory penalties and fines

Strengthen your defenses against future incidents through remedial recommendations

Use cases

- Gain an understanding your organization's digital footprint and the associated risks
- Helps assess the risk by conducting in-depth inspections of your IT infrastructure and data (such as log files) and analyzing your outgoing network connections
- Identify signs of ongoing or past intrusions within your networks
- Recognize how the attack is affecting your systems, and what you can do about it

1 Skills required

5 Customization and scalability

3 Cost

Kaspersky Threat Intelligence

Counteracting today's cyberthreats requires a 360-degree view of the tactics and tools used by threat actors. Generating this intelligence and identifying the most effective countermeasures requires constant vigilance and high levels of expertise. With petabytes of rich threat data to mine, advanced machine-learning technologies and a unique pool of world experts, Kaspersky Lab supports you with the latest threat intelligence from around the world, helping you maintain immunity to even previously unseen cyberattacks.

Ideal for

Enterprises

Government institutions

SOCs and incident response teams

MSSPs

Business benefits

Instant threat detection to prevent the disruption of business operations

Minimizes potential financial losses from incidents

Ensures cost-effective investments in certain technologies and staff the right based on timely information about threats targeting your enterprise

Prevents competitors from gaining an unfair competitive advantage through the exfiltration of intellectual property

Helps build a **proactive and adaptable defense**

Use cases

- Reinforce network security solutions with continuously updated **Threat Data Feeds**
- Effectively prioritize overwhelming amounts of security alerts, and immediately identify those which should be escalated to incident response teams with **Threat Data Feeds** and **CyberTrace**
- Gain real-time 'situational awareness' and leverage threat intelligence feeds more effectively with **CyberTrace**
- Identify your organization's digital footprint and mitigate the associated risks with **Tailored Threat Intelligence Reporting**

Kaspersky Cybersecurity Training: Incident Response service

Cybersecurity education is a critical for enterprises faced with the growing volume of constantly evolving threats. IT security staff must be skilled in the advanced techniques central to effective enterprise threat management and mitigation strategies. Kaspersky Cybersecurity Training helps to equip your in-house security team with all the necessary knowledge needed to deal with a continuously evolving threat environment.

Ideal for

Enterprises

Government institutions

SOCs and incident response teams

MSSPs

Business benefits

Mitigates the potential damage from security incident quickly and effectively, to significantly reduce the incident's cost

Ensures you avoid regulatory penalties and fines

Helps maintain the relationship of trust with your customers, partners, and investors, to further foster business opportunities

Strengthens your defenses against future incidents through the lessons learned

Use cases

- Differentiate APTs from other threats
- Understand various attacker techniques and the anatomy of targeted attacks
- Apply specific methods of monitoring and detection
- Create effective detection rules
- Reconstruct incident chronology and logic, and follow the incident response workflow

3 Integrated Cybersecurity Approach

Threat Management and Defense

Be ready for APT-level attacks

Ideal for enterprises with a high level of expertise, used to working with threat intelligence and undertaking threat hunting

- Complex and distributed environments
- In-house security team or SOC
- Higher costs of incidents and data breaches
- Subject to compliance

Services

- **Kaspersky Managed Protection**
- **Kaspersky Incident Response**

People

- **Kaspersky Cybersecurity Training**

Intelligence

- **Kaspersky Threat Intelligence**

Kaspersky Threat Management and Defense

Kaspersky Threat Management and Defense is a specialized solution providing a comprehensive framework for rapid threat discovery, incident investigation, response and remediation. It consists of global threat intelligence, advanced threat detection and response technologies, a range of cybersecurity training, continuous threat hunting and response to threats circumventing existing security barriers. The solution can be integrated into your current organizational strategy to counter complex threats, complementing existing protection technologies, and supporting you with leading expertise when needed.

Ideal for

Enterprises

Government institutions

SOCs and incident response teams

MSSPs

5 Skills required

5 Customization and scalability

5 Cost

Business benefits

Minimizes the financial and operational damage caused by cybercrime and helps maintain business stability

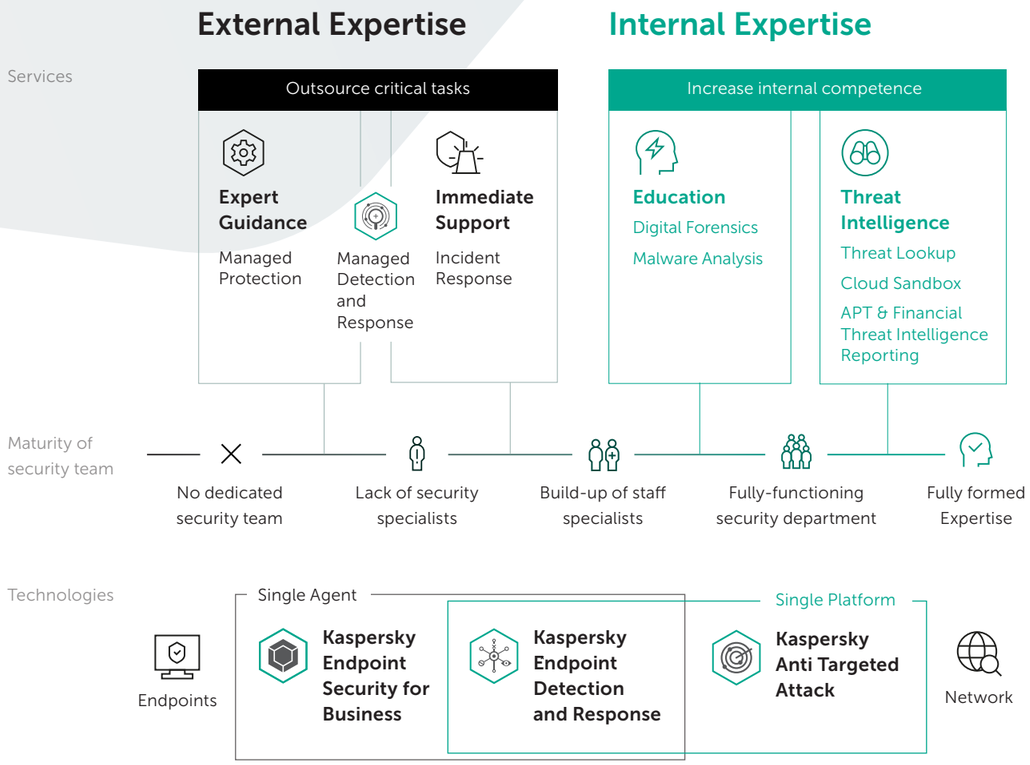
Increases ROI through automation and the avoidance of disruption to business processes

Reduces staff turnover rates and increases operational efficiencies by growing in-house expertise

Deploys fully informed and cost-effective information security strategies based on tailored threat models

Use cases

- The all-in-one technological platform automates time-consuming evidence collection and routine manual tasks
- Proactive threat intelligence provides the context needed to promptly detect, prioritize, investigate and respond to threats
- Enterprise threat management strategy through the provision of advanced skills
- Threat hunting enables detection of unknown and advanced threats designed to circumvent preventive technologies
- Access to third-party expertise supports effective investigation and response to complex incidents



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, businesses 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

An 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.

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.

Kaspersky Security for Enterprise

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

One of the most highly recommended

Kaspersky has once again been named a Gartner Peer Insights Customers' Choice for Endpoint Protection Platforms, having received a high customer satisfaction rating of 4.6 out of 5 as of May 28, 2019.*

Most transparent

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

*Gartner Peer Insights Customers' Choice constitute the subjective opinions of individual end-user reviews, ratings, and data applied against a documented methodology; they neither represent the views of, nor constitute an endorsement by, Gartner or its affiliates. Read on website

Contact us

Find a partner near you: www.kaspersky.com/buyoffline
Kaspersky for Business: www.kaspersky.com/business
Enterprise Cybersecurity: www.kaspersky.com/enterprise
IT Security News: business.kaspersky.com/
Our unique approach: www.kaspersky.com/true-cybersecurity

#bringonthefuture

www.kaspersky.com

kaspersky

Bring on the future

www.kaspersky.com