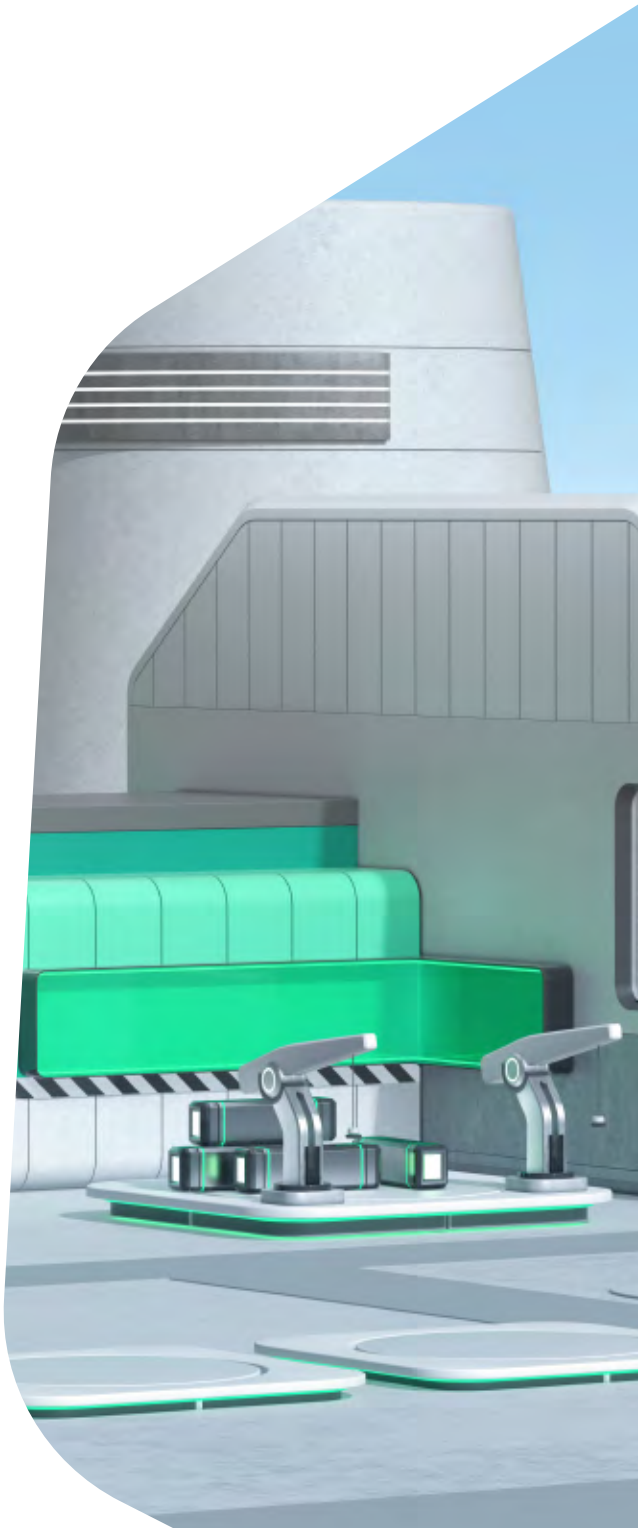
kaspersky

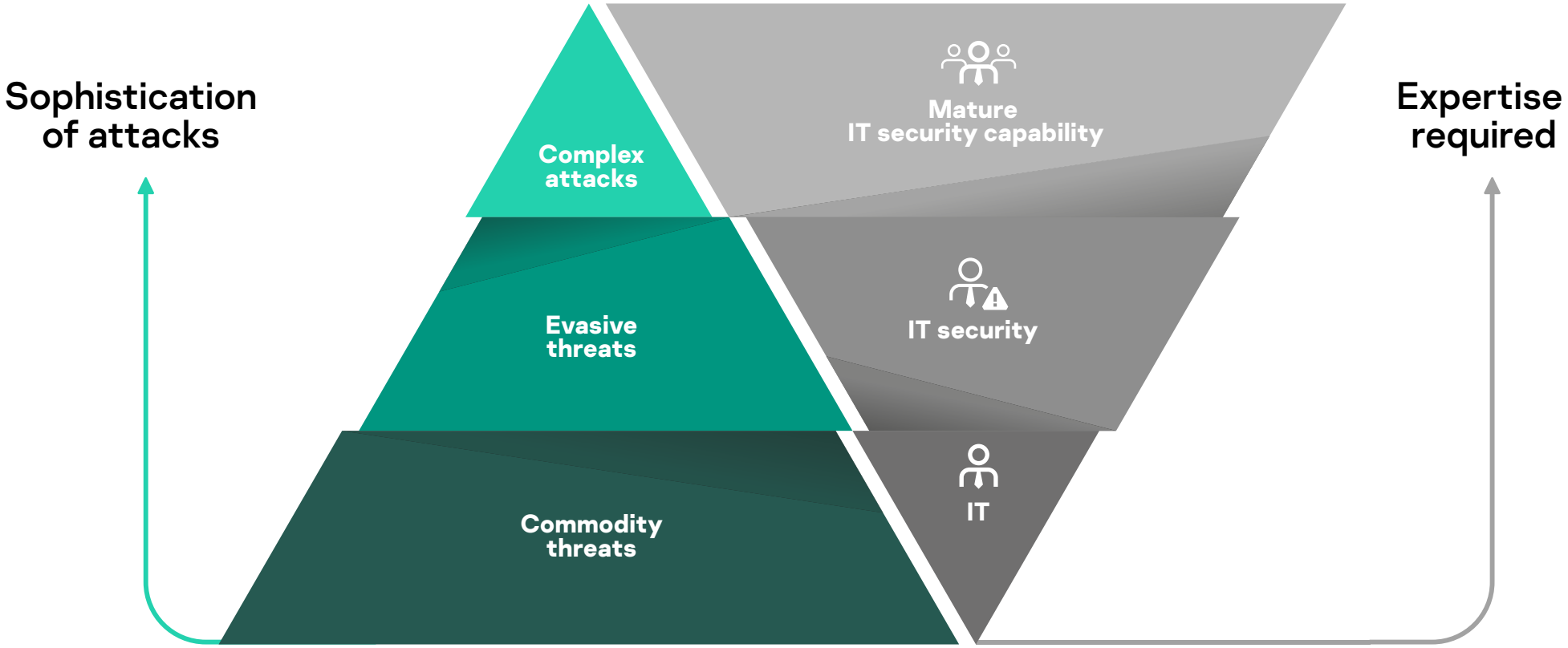
Kaspersky Security for Enterprise

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



Threat types and the expertise required to counteract them



Short-term vs. long-term security planning

Traditional security evolution process

Decision making:

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

Leveraging traditional products:

- Endpoint Protection Platforms (EPP)
- Firewalls / Next Generation Firewalls (NGFW)
- Web Application Firewalls (WAF)
- Data Loss Prevention (DLP)
- Security Information and Event Management Systems (SIEM)
- And others

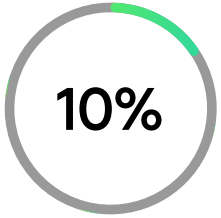
Attributes

- 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 cybersecurity technologies
- Successful digital transformation of the business requires a long-term cybersecurity strategy

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.

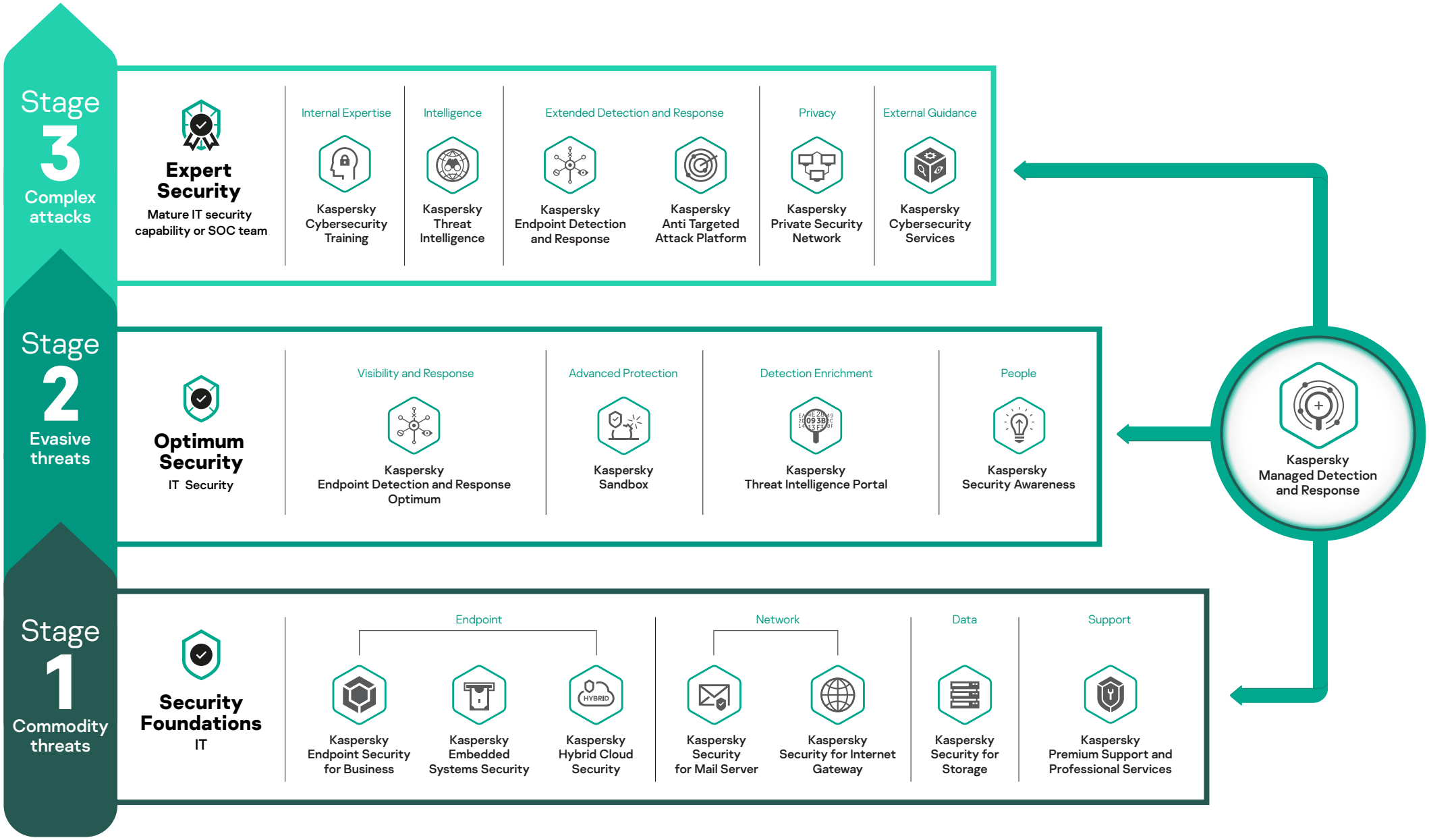


of businesses
detect attacks
almost instantly

is the additional
cost of a data breach
if detected after seven days

Source: IT Security Economics 2020 report by Kaspersky

Kaspersky's stage-by-stage cybersecurity approach



Stage 1
Security Foundations

Automatically block the maximum possible number of threats

- The fundamental stage for organizations of any size and infrastructure complexity in building an integrated defense strategy against complex threats
- Usually sufficient for smaller enterprises with IT teams only and not deploying IT security specialists

Kaspersky Endpoint Security for Business

The reputation of your business must be defended at all costs, which is why we do more than 'just' protect and control all your endpoints. Kaspersky Endpoint Security for Business secures your organization against the full range of threats, from BIOS-related to fileless threats, while server hardening boosts your high-performance server defenses with specific controls that prevent the loss of personal and financial information. Delivered from the cloud or on-premises for flexible security and management.

Ideal if you're aiming to:

- Prevent employees from exposing your business, and themselves, to an attack
- Reduce the number of endpoint incidents that have to be processed manually
- Secure diverse environments with flexible and proven defenses

2 Skills required

5 Customization and scalability

2 Level of investment

Business benefits

- Decreases your TCO by automating your defenses against different threats in an all-in-one product
- Ensures business continuity by protecting any device, anywhere
- Helps meet compliance requirements while providing the flexibility to outsource IT security management

Practical Applications

- Reduce your risk of falling victim to an attack, with the most awarded endpoint protection technology
- Ensure your IT estate is patched, with management from the cloud or the on-premises console
- Migrate from third-party solutions easily and fast
- Organically add new technologies, including EDR and other capabilities, without reinstalling on endpoints
- Protect your data while meeting compliance goals through built-in encryption management, including remote wipe and device control for various OS

Kaspersky Hybrid Cloud Security

Kaspersky Hybrid Cloud Security simplifies and secures your digital transformation, as your organization virtualizes or moves workloads into the cloud. Patented Light Agent technology significantly lowers hypervisor resource use. Native integration with a wide range of virtualization, containerization and public cloud platforms provides consistent visibility and control throughout your whole infrastructure. A full stack of security technologies managed from the same console ensures streamlined risk management in diverse environments on a day-to-day basis.

Ideal if you're aiming to:

- Virtualize your server and desktop workloads
- Move or maintain infrastructures in public clouds (IaaS)
- Integrate security steps into your DevOps pipelines
- Securely leverage containerization

Business benefits

- Minimizes financial and reputational damage by reducing your attack surface and your attacker's dwell time
- Optimizes IT costs by freeing up to 30% of hypervisor resources
- Supports compliance by meeting core security requirements
- Ensures efficient collaboration between IT, Information Security and Development (DevOps) teams, reducing risk and security gaps

Practical Applications

- Ensure consistent visibility and control across your datacenter and cloud deployments
- Enable security for VMWare and Citrix VDI
- Protect your cloud workloads in AWS, Azure and Google Cloud instances, with automated deployment and consistent visibility through native API integration
- Enable security for DevOps with container protection, pipeline integration interfaces and management API

Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security is a specialized multi-layered solution designed to protect your Windows-based embedded devices – and older endpoints running unsupported OSs that you can't currently upgrade. Application Control combines with optional anti-malware including exploit prevention plus network threat protection, integrity monitoring and other security layers for optimum protection tailored to your processes and device capabilities.

Ideal if you're aiming to:

- Protect ATMs, PoS systems, healthcare equipment or any other non-industrial-grade embedded systems
- Optimize the security of systems running obsolete hardware and OS – including old endpoints
- Integrate your embedded infrastructure's security into your Kaspersky-based security ecosystem

Business benefits

- Ensures continuous, disruption-free business processes in areas where the financial, legal and reputational impact of an attack could be devastating
- Helps to avoid being forced to upgrade - continue safely using old and as yet irreplaceable, scenario-specific endpoints for as long as you wish
- Enables full compliance through reliable protection mechanisms – including those specifically recommended by regulators

Practical Applications

- Configure the most effective security scenario for your system, according to its usage and power level, from a choice of security layers and scenarios
- Ensure durable and hassle-free protection where frequent maintenance operations are impossible
- Thwart insider attacks – a major risk for embedded devices which can't be attacked via email or the web.
- Protect devices with poor internet connectivity

Kaspersky Security for Mail Server

Kaspersky Security for Mail Server prevents email-based threats, including crimeware, ransomware, phishing and spam, from reaching your endpoints, where most malware and socially-engineered scams operate. Cloud-based AI implementation and on-premises machine learning-based models ensure high detection rates with exceptionally low false positives, addressing sophisticated mail-based threats, including Business Email Compromise (BEC). Resource-wasting spam is blocked efficiently before it can gain momentum.

Ideal if you're aiming to:

- Strengthen your capabilities against both mass-delivered and highly targeted attacks using email as a delivery method
- Cover a breadth of email security scenarios involving different platforms and deployment schemes

Business benefits

- Reduces the disruptive effects of email-borne malware- and social engineering-based attacks
- Boosts staff productivity by negating spam-induced distractions
- Reduces IT/IT security workloads and optimizes your operational costs
- Minimizes your legal and reputational risk by controlling emailed content transfer

Practical Applications

- Critically reinforce your infrastructure defenses at mail server level, blocking threats before they reach their targets – your users and endpoints
- Boost existing gateway security without adding false positives
- Empower your Kaspersky-based advanced threat detection facilities with added context and automated gateway-level response capabilities

Kaspersky Security for Internet Gateway

Kaspersky Security for Internet Gateway, with its core application Kaspersky Web Traffic Security, offers solid gateway-level protection against web-based cyberthreats, including malware, ransomware, miners, online phishing and malicious web resources. It also allows you to control use of the World Wide Web, restricting access to specific web resources in alignment with corporate policies, and limiting the transfer of certain file types.

Ideal if you're aiming to:

- Prevent web-based threats from affecting your endpoints
- Reduce the risk of infection and boost overall productivity by applying controls to internet usage
- Reduce the workload on your IT/IT security teams, by automatically blocking web-based threats at the point of entry

Business benefits

- Minimizes business disruption and the impact of intra-network security disturbances
- Increases IT/IT security efficiency and optimizes your operational costs
- Secures your organization against online social engineering based threats
- Promotes increased employee productivity, by controlling online access to specific web resources

Practical Applications

- Reinforce your endpoint-based defenses at gateway level
- Complement and strengthen your existing web gateway security, without adding false positives
- Protect devices which can't otherwise be fully secured at endpoint level for business or usage reasons
- Empower your Kaspersky-based advanced threat detection facilities by adding context and providing the means for an automated gateway-level response

Kaspersky Security for Storage

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

Ideal if you're aiming to:

- Safeguard connected storages against external attacks and spreading infection
- Protect valuable data on connected storages against ransomware attacks
- Manage your data storage security alongside endpoints and servers protected by Kaspersky solutions

Business benefits

- Upholds business continuity by preventing malware outbreaks using storages as spreading-points
- Helps uphold compliance, offering reliable means of protection for your regulated data storage
- Reduces operational hassle, through a unified management experience with other Kaspersky endpoint and server protection solutions

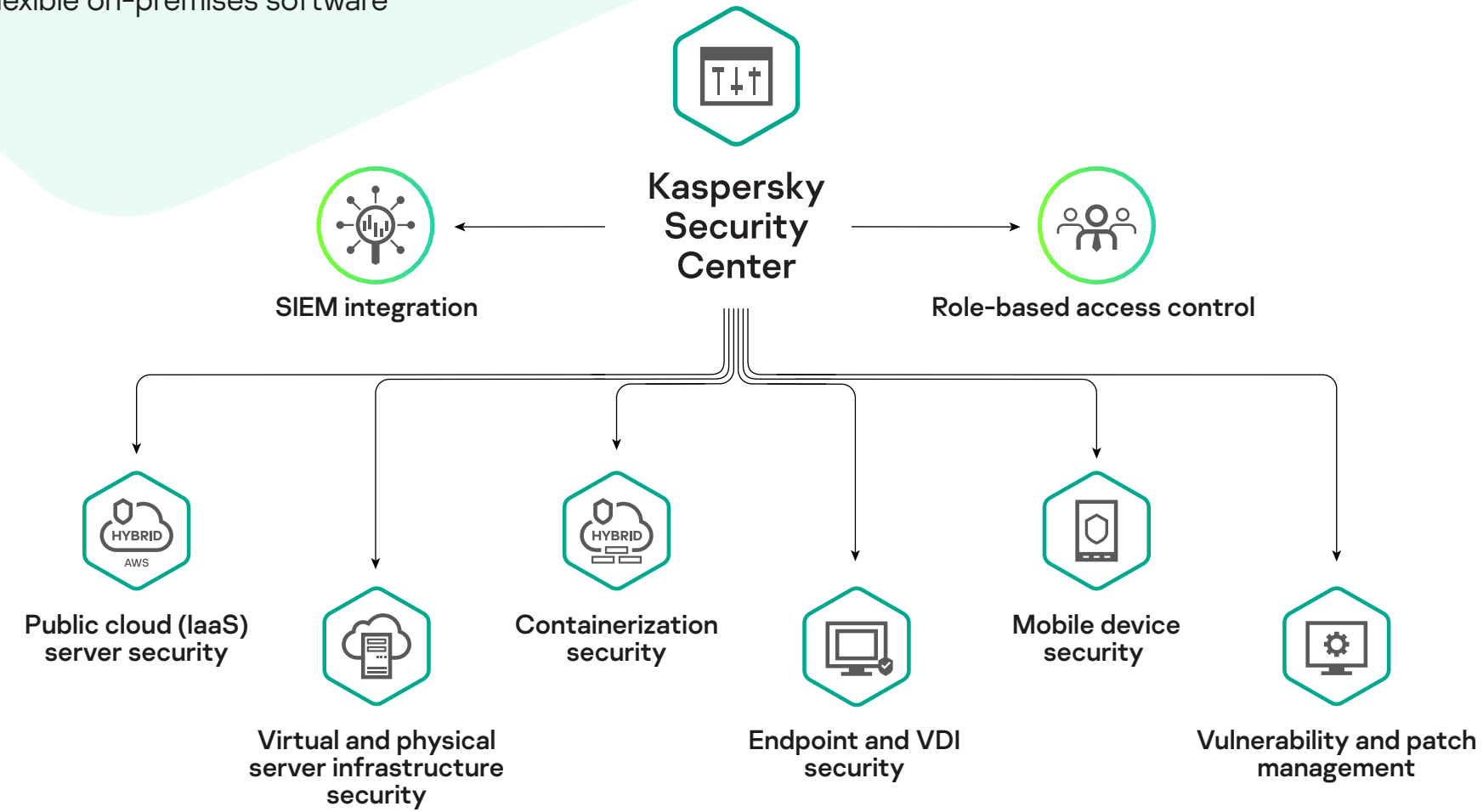
Practical Applications

- Protect NAS, DAS or SAN, or any combination of these used in your infrastructure
- Protect both storages and the server used to host the security solution – all in one product
- Prevent data loss caused by remotely running cryptors

Single pane of glass security management

Kaspersky Security Center for multiple workloads management and policy-based control, delivered as:

- Scalable SaaS offering
- Flexible on-premises software



Kaspersky Premium Support (MSA)

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 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 if you're aiming to:

- Enjoy the assurance of knowing that your IT systems are protected, not just by industry-leading security technologies, but by the skills and dedication of Kaspersky's world-class experts

Business benefits

- Ensures business continuity, with allocated experts on standby, tasked with taking ownership of your issue and achieving the swiftest possible resolution
- Reduces the cost of a security incident through access to a priority support line, guaranteed response times and private patches
- A dedicated Technical Account Manager acts as your representative inside Kaspersky, with the authority to mobilize any expertise needed in order to quickly resolve the issue

Practical Applications

- Fast-track critical issues straight to the specialists best equipped to provide the right solution for you, at speed
- Keep fully protected with proactive measures tailored to your system
- Reduce the time spent by your valuable in-house resources on maintenance and troubleshooting

Kaspersky Professional Services

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.

Ideal if you're aiming to:

- Accelerate, optimize and customize your Kaspersky solution to meet best cybersecurity practices

Business benefits

- Maximizes the ROI on your security solutions by ensuring they perform at 100% capability
- Reduces costs for internal IT staff
- Minimizes the impact to everyday business operations of implementing any new security solution, and reduces overall implementation costs
- Helps to ensure that any critical issue arising is dealt with fast and effectively

Practical Applications

- Reduce the risk of implementation issues that can diminish your protection, impact productivity and lead to downtime
- Minimize the risks of downtime, through periodic audits of product configurations which ensure the most up-to-date defensive mechanisms are in place
- Reduce the product adoption period, allowing the full benefits to be extracted right away

Stage 2
Optimum Security

Advanced detection and a centralized response

Enables smaller cybersecurity teams to tackle even threats that bypass automatic prevention – with a resource-conscious solution building up organically from Security Foundations.

Kaspersky Endpoint Detection and Response Optimum

Kaspersky Endpoint Detection and Response (EDR) Optimum helps organizations with basic cybersecurity expertise to address a number of evasive threats. It includes the protection capabilities of Kaspersky Endpoint Security for Business Advanced and is managed from Kaspersky Security Center. The product provides an easy-to-use toolkit based on simplified root cause analysis, IoC (Indicator of Compromise) scanning, and automated or 'single-click' response options.

Ideal if you're aiming to:

- Increase threat visibility across all your endpoints
- Decrease your mean-time-to-respond
- Optimize your IT security resources and raise efficiency

Business benefits

- Minimizes financial, reputational and other risks associated with threats that evade preventive protection
- Helps to optimize staff workloads and resource usage through streamlined workflow and a set of automation capabilities
- Boosts efficiency with a cost-conscious, accessible tool which doesn't require deep expertise, and a lot of time to master

Practical Applications

- Enjoy granular visibility of endpoint security alerts
- Analyze the threat detected on the host further, to reveal its scale and root cause
- Learn if you're under attack by searching for IoCs imported from third party sources
- Respond to threats automatically on discovery or during your investigation – in just a few clicks

3 Skills required

4 Customization and scalability

3 Level of investment

Kaspersky Managed Detection and Response Optimum

Kaspersky Managed Detection and Response Optimum gives you an instantly matured IT security function, through fast and scalable turnkey deployment with no need to invest in additional staff or expertise. Patented machine-learning models, unique ongoing threat intelligence and automated threat hunting using proprietary Indicators of Attack (IoAs) ensure your organization is continuously defended against complex threats leveraging known tactics, techniques and procedures.

Ideal if you're aiming to:

- Establish and improve early, effective threat detection and response, through 24/7 continuous-monitoring coverage
- Rapidly decrease your company's susceptibility to advanced threats - without your own IT security team spending much time on increasing their skills and mastering new solutions

Business benefits

- Delivers the reassurance of knowing that you're continuously protected against even the most innovative threats
- Reduces overall security costs without the need to employ and train a range of in-house security specialists to cover all eventualities

Practical Applications

- Enable a systemic approach to protection by automatically preventing, detecting, hunting and responding to threats targeting your networks
- Ensure a swift reaction to incidents while keeping all response actions within your full control
- Gain complete real-time visibility into all detections, the assets covered, and their current protection status

Kaspersky Sandbox

Kaspersky Sandbox automatically protects you from new and unknown threats designed to bypass endpoint protection. It complements Kaspersky Endpoint Security for Business and helps organizations to significantly increase their levels of endpoint and server protection against threats such as previously unknown malware, new viruses and ransomware, zero-day exploits, and others – without the need to hire new security personnel.

Ideal if you're aiming to:

- Boost you defenses against evasive threats
- Automate advanced detection
- Optimize your staff workload and expertise requirements

Business benefits

- Reduces IT security risk and ensures business continuity
- Protects against new and unknown threats without affecting endpoint performance or user productivity
- Minimizes labor costs through automating manual operations
- Optimizes costs for the advanced threat protection of remote offices

Practical Applications

- Facilitate the in-depth dynamic analysis and detection of unknown and evasive threats
- Deliver an automated response across all protected endpoints
- Avoid impacting productivity and boost the security of highly loaded endpoints by offloading resource-intensive behavior analysis to the sandbox
- Integrate with third-party solutions through an API
- Save man-hours thanks to simple installation and fully automatic functioning of your sandbox, with no advanced IT or cybersecurity staff skills needed

Kaspersky Threat Intelligence Portal

The Kaspersky Threat Intelligence Portal brings together all the knowledge we've acquired about cyberthreats into a single, powerful web service. It allows you to check suspicious threat indicators, whether it's a file, file hash, IP address or URL. The Portal analyzes objects with a set of advanced threat detection technologies such as reputational detection via Kaspersky Security Network, structural machine learning models and advanced dynamic detection by means of Kaspersky Cloud Sandbox, revealing whether an object is in the 'Good', 'Bad', or 'Not Categorized' zone. The contextual data provided helps you prioritize and respond to threats more effectively.

Ideal if you're aiming to:

- Gain free access to a trusted threat intelligence source
- Prioritize incidents more effectively
- Expedite investigation and threat discovery

Business benefits

- Circumvents a high cost-barrier to commercial threat intelligence adoption
- Helps maintain the effective protection of your networks by giving you timely access to 100%-vetted data

Practical Applications

- Validate and prioritize alerts or incidents posing a real threat, based on impact and risk levels
- Immediately identify alerts that should be escalated to your incident response team
- Separate real threats from noise, and determine where to focus your limited incident response resources
- Eliminate the need to perform complicated searches through different databases to find details of a particular observation or attack
- Discover previously undetected threats

3 Skills required

4 Customization and scalability

0 Level of investment

Kaspersky Security Awareness

Kaspersky Security Awareness is a collection of computer-based gamified training products that shapes your employees' cyber-hygiene skills and motivates them to maintain safe practices, addressing all levels of the organizational structure. It consists of:

- Kaspersky Interactive Protection Simulation & CyberSafety Management Games – for engagement and motivation
- Gamified Assessment Tool – to define the right starting point
- Online Learning Platform & Cybersecurity for IT Online – to gain practical skills
- [Dis]connected – a casual educational game that reinforces newly learnt skills.

Ideal if you're aiming to:

- Reduce the number of incidents caused by employee ignorance or negligence
- Develop the right understanding of cybersecurity measures for staff at every level
- Instill a strong cybersecurity culture within your organization with ready-to-use solutions

2 Skills required

4 Customization and scalability

3 Level of investment

Business benefits

- Helps reduce the number of human-related security incidents, ensuring business continuity and minimizing the impact of an incident
- Engages and motivates people to learn, and turns management into supporters of cybersecurity measures and initiatives
- Improves the cybersecurity culture throughout your organization

Practical Applications

- Equip your employees with the skills and knowledge needed to adopt and maintain safe behavior
- Foster a healthy corporate attitude to cybersecurity issues
- Empower employees to achieve better results in their day-to-day responsibilities without exposing your business to cyber risks

Stage 3
Expert Security

Readiness for complex and APT-like attacks

Focus on extended defenses powered by threat intelligence, expert guidance and knowledge transfer, empowering mature IT-security teams to face down complex threats and targeted attacks.

Kaspersky Endpoint Detection and Response

A powerful feature-rich EDR tool for IT security experts, enabling complete visibility, premium threat detection and efficient analysis, with fast access to the collected data. Your investigation process is powered by retrospective analysis, proprietary Indicators of Attack (IoAs) and MITRE ATT&CK mapping, as well as proactive threat hunting and access to Kaspersky Threat Intelligence. Reveal the entire sequence of intrusion, understand multi-staged complex attacks targeting endpoints and respond appropriately and fast!

Ideal if you're aiming to:

- Strengthen your endpoint protection
- Further improve in-house incident response capabilities continuously decreasing your mean-time-to-detect/respond
- Boost your proactive threat hunting operations

Business benefits

- Helps to keep watch on your most valuable assets
- Mitigates cyber risk and reduces financial and operational damage caused by endpoint incidents
- Reduces your IT security operational costs by simplifying endpoint-related incident analysis and response
- Helps ensure compliance with regulatory requirements

Practical Applications

- Effectively detect (with capabilities proven through MITRE evaluation) and rapidly respond to advanced attacks at the endpoint level
- Conduct retrospective analysis and effective investigations across centrally aggregated data
- Centralize incident management with guided investigation and response
- Hunt out hidden threats with automated and proactive threat hunting capabilities
- Kaspersky EDR forms part of the Kaspersky Anti Targeted Attack Platform, creating an Extended Detection and Response solution

Kaspersky Anti Targeted Attack Platform

Kaspersky Anti Targeted Attack Platform combines network-level advanced threat discovery and EDR capabilities, acting as an Extended Detection and Response solution to deliver all-in-one APT protection powered by our Threat Intelligence and the MITRE ATT&CK framework. Your IT security specialists have all the tools they need to handle superior multi-dimensional threat discovery, undertake effective investigations, proactively hunt for threats and deliver a rapid, centralized response — through a single solution.

Ideal if you're aiming to:

- Build effective extended defenses against most sophisticated attacks with a single, powerful system
- Obtain complete enterprise-wide visibility
- Decrease your mean-time-to-detect/respond
- Power your Security Operations Center
- Enhance your security posture while safeguarding your privacy

5 Skills required

3 Customization and scalability

5 Level of investment

Business benefits

- Mitigates cyber-risk and reduces the financial, reputational and operational damage caused by complex targeted attacks
- Reduces IT security operational costs by streamlining and automating incident management processes
- Helps ensure compliance with regulatory requirements

Practical Applications

- Secure multiple potential threat entry-points at both network and endpoint levels
- Rapidly discover advanced threats that bypass your existing preventive technologies
- Hunt out hidden threats, with automated and proactive threat hunting capabilities
- Provide your IT security team with timely information about detected threats for deeper investigation
- Enable a centralized response to complex incidents through wide-ranging automated scenarios

Managed Detection and Response Expert

Offload your time- and resource-consuming incident triage and investigation processes to us at Kaspersky. All the features and functionality of Kaspersky Managed Detection and Response Optimum combined with managed hunting for threats leveraging unknown tactics, techniques and procedures (TTPs), direct call-in access to Kaspersky's SOC analysts, up to 3 months of raw data retention, privileged access to Kaspersky Threat Intelligence, and an API enabling integration with third-party ticketing systems, significantly cutting the time you need to spend on workflow administration.

Ideal if you're aiming to:

- Free up more of your mature in-house IT security team's limited time, so they can focus on critical incidents that really require their involvement
- Further enhance your security team's efficiency by augmenting your in-house best practices with Kaspersky's seasoned expertise

Business benefits

- Provides the major benefits of having a Security Operations Center, without the need to establish your own
- Maximizes the value from your Kaspersky security solutions
- Helps reduce overall security costs, and the need for additional future investment in this area by instantly raising the IT security capability without the need to employ and train a range of in-house security specialists

Practical Applications

- Gain an individually tailored ongoing detection, prioritization, investigation and response function
- Consult with our experts and gain additional supporting context on threats observed in your networks
- Enable retrospective hunting for threats using newly acquired threat intelligence
- Boost incident investigation by querying Kaspersky's complete knowledge base on threats and their relationships

Kaspersky Threat Intelligence

Kaspersky Threat Intelligence provides rich and meaningful context throughout the incident management cycle. Our unique and immediately actionable insights can be delivered in different forms and formats, supporting smooth integration with your existing security workflows. The portfolio comprises threat intelligence feeds, industry and threat-specific human-readable reports and a searchable repository with petabytes of data on threats, legitimate objects and their various relationships.

Ideal if you're aiming to:

- Optimize your prevention and detection capabilities
- Move from a reactive to a proactive security posture
- Enhance your threat intelligence program
- Enable better-informed strategic security decision-making

Business benefits

- Helps reduce IT security staff turnover by preventing analyst burnout
- Increases security operational efficiencies, minimizing business disruption and incident impact
- Helps optimize your ROI by aligning your IT security investment with your specific threat landscape

Practical Applications

- Reinforce security solutions with continuously updated, machine-readable cyberthreat data
- Improve alert prioritization by determining critical alerts requiring escalation to incident response teams
- Boost human-driven investigations by revealing relationships between detected threats
- Justify your IT security budget by presenting clear and relevant risk scenarios

Kaspersky Cybersecurity Training

Skills development is critical for enterprises in the face of a 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, such as reverse engineering, YARA rules creation and working with digital evidence. Kaspersky Cybersecurity Training helps to equip your in-house security team with all the expertise needed to deal with a continuously evolving threat environment.

Ideal if you're aiming to:

- Raise your levels of in-house IT security expertise
- Strengthen your Security Operations Center practices
- Build up internal threat research capabilities

Business benefits

- Up-skills your SOC team to mitigate potential damage from security incidents faster and more effectively
- Saves your time and money on trying to recruit hard-to-find ready-skilled staff and then waiting until they learn all your company's specifics
- Helps retain and motivate in-house staff through promoting skills-based career development.

Practical Applications

- Boost your incident response with malware analysis, for a full understanding of the threat and the most effective response plan development
- Maintain a trail of evidence on host or network systems to reveal the root cause of an incident, prevent similar incidents in the future and avoid legal action
- Enable scalable, rapid and effective incident response processes to ensure successful recovery from a wide range of threats within enterprise networks

Kaspersky Cybersecurity Services

Kaspersky Cybersecurity Services provide access to the full weight of Kaspersky's expertise in responding to information security incidents, revealing past and ongoing compromise attempts as well as conducting enterprise-wide and industry-specific security assessments to close security gaps before their exploitation, and to prevent future attacks. Collaborating with Kaspersky's experts allows your internal IT security teams to achieve greater efficiency in fighting increasingly sophisticated threats.

Ideal if you're aiming to:

- Have an expert partner covering your back in case of an incident
- Understand whether your existing detection and prevention systems are sufficient
- Ensure you're taking a proactive security approach

Business benefits

- Ensures damage from incidents, however complex, is minimized, through continuous access to proven IT security expertise
- Significantly reduces potential downtime expenses and avoids negative publicity
- Supports full regulatory compliance, helping avoid penalties and fines

Practical Applications

- Get your systems and business operations back on track faster
- Detect compromise attempts and mitigate incident impact before it becomes apparent
- Improve the security of industry-specific infrastructures
- Evaluate your defensive capabilities and identify weak points that need addressing

3 Skills required

5 Customization and scalability

4 Level of investment

Kaspersky Private Security Network

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

Ideal if you're aiming to:

- Protect a privacy-sensitive company with strict policies against any data leaving the confines of its IT infrastructure
- Satisfy strictest data protection regulations
- Facilitate threat intelligence circulation within your organization to bolster protection and speed up response times

Business benefits

- Upholds business continuity through efficient detection & response, supported by internal information-sharing
- Increases operational efficiency by helping keep false positives at bay
- Supports compliance with regulatory requirements for the security of isolated systems and environments

Practical Applications

- Protect your isolated, even air-gapped, infrastructure without compromising on threat detection effectiveness
- Organize a national threat data exchange facility
- Integrate your existing Kaspersky advanced threat detection solutions with any other Kaspersky B2B solutions through your own internal threat intelligence network

5 Skills required

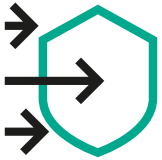
5 Customization and scalability

5 Level of investment

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.

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®

The GARTNER PEER INSIGHTS CUSTOMERS' CHOICE badge is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. 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.

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 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.

kaspersky