KASPERSKY lab

Kaspersky Security Solutions for Enterprise 2018

#TrueCybersecurity

Kaspersky
Security Solutions for Enterprise
2018

Enterprise Security in an Era of Digital Transformation

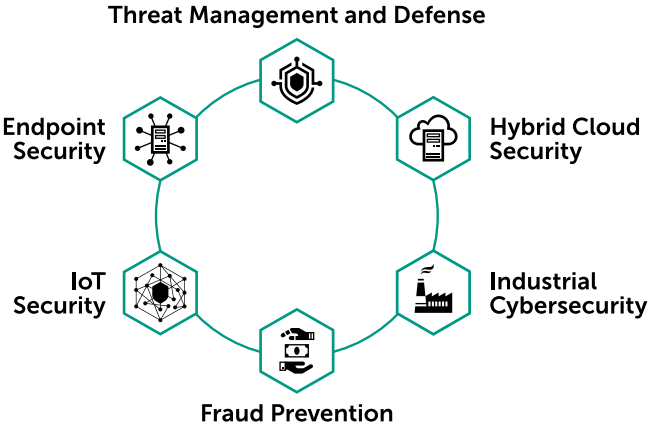
The number of cyberattacks continues to rise dramatically, with attacks to corporate infrastructure becoming increasingly professional and highly tailored. It's no longer a question of whether you will be attacked, but when, and how quickly and completely you can recover.

Meanwhile, corporate IT infrastructure has become ever more complex, as it extends beyond the organizational perimeter onto mobile devices and into public clouds and third party providers. While digital transformation brings massive benefits in terms of business efficiency and agility, it also brings new security challenges. Ensuring business continuity, protecting financial performance and safeguarding corporate and customer data all makes considerable demands on your IT security team, and on your budget.

Kaspersky Lab's new Enterprise Portfolio reflects the security demands of today's enterprise businesses, creating a complete cybersecurity platform that combines fully scalable protection capabilities for physical, virtual and cloud-based systems including static and mobile endpoints, servers, networks and specialized hardware and software.

A unique combination of leading technologies and services enables your security team to prevent most attacks, detect new and predict future threats, and respond to emerging incidents, helping to ensure operational continuity and regulatory compliance.

Our portfolio consists of the following solutions, all complemented with wide-ranging expert services, security training and professional support:



These solutions and their component technologies intermesh to create an adaptive security framework. This enables the prediction, prevention, detection and remediation of the most advanced cybersecurity threats and targeted attacks, promoting business continuity and resilience, with minimum impact on performance.

True cybersecurity, assisted by a combination of machine learning and human expertise and backed by industry-leading threat intelligence, delivers top performance protection together with unified visibility and manageability, and full support for your digital transformation.

Fighting for Your Digital Freedom

Your data and privacy are under attack by cybercriminals and agents of espionage, so you need a partner who is not afraid of standing beside you in the fight to defend your corporate assets. For 20 years, Kaspersky Lab has been uncovering and defeating all kinds of cyberthreats, no matter whether they come from script kiddies, cybercriminals or governments, or from the north, south, east or west. We believe the online world should be free from attack and state-sponsored espionage, and will continue fighting for a truly free and safe digital world.

Proven

Kaspersky Lab routinely scores the highest marks in independent ratings and surveys.

- Measured alongside **80 well-known vendors** in the industry
- **72 first places** in 86 tests and reviews in 2017
- **Top 3 ranking*** in over 90% of all product tests
- In 2017, Kaspersky Lab received **Platinum Status** for Gartner's Peer Insight** Customer Choice Awards, in the Endpoint Protection Platforms market

Our Global Research and Analysis Team has been actively involved in the discovery and disclosure of some of the most prominent malware attacks linked to governments and state organizations.

Transparent

We are totally transparent and are making it even easier to understand what we do:

- Independent review of the company's source code, software updates and threat detection rules
- Independent review of internal processes
- Three transparency centers by 2020
- Increased bug bounty rewards with up to $100K per discovered vulnerability

Independent

As a private company, we are independent from short term business considerations and institutional influence.

We share our expertise, knowledge and technical findings with the world's security community, IT security vendors, international organizations, and law enforcement agencies.

Our research team is spread across the world and includes some of the most renowned security experts globally. We detect and neutralize all forms of advanced APTs, regardless of their origin or purpose.

* www.kaspersky.com/top3
** https://www.gartner.com/reviews/customerchoice-awards/endpoint-protection-platforms

Endpoint Security

The leading multi-layered endpoint protection platform, based on Next Gen cybersecurity technologies

The threat environment is advancing exponentially, putting critical business processes, confidential data and financial resources at ever-increasing risk from zero-day attacks. To mitigate the risk to your organization, you need to be smarter, better equipped and better informed than the cyber-professionals targeting you. But one simple fact is true – the majority of enterprise cyber-attacks are initiated through the endpoint. If you can effectively secure every corporate endpoint, static and mobile, you have a strong foundation for your overall security strategy.

In the 2017 Gartner Peer Insights Customer Choice Awards for Endpoint Protection Platforms, **we were the only vendor to achieve a Platinum Award***.

*The Gartner Peer Insights Customer Choice Logo 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 Customer Choice Awards (https://www.gartner.com/reviews/customer-choice-awards/endpointprotection-platforms) are determined by the subjective opinions of individual end-user customers based on their own experiences, the number of published reviews on Gartner Peer Insights and overall ratings for a given vendor in the market, as further described here – http://www.gartner.com/reviews-pages/peer-insights-customer-choice-awards/ and are not intended in any way to represent the views of Gartner or its affiliates.

Digital Transformation Brings Additional Risks

The growing complexity of most corporate IT networks can create 'visibility gaps' where threats can hide.

On average, a Targeted Attack can continue to lurk within the target systems – totally undetected – for 214 days.

During this period, the threat could be continuing to perform a range of malicious activities. So it's vitally important to use efficient tools that can rapidly detect, remove and remediate.

Sadly, despite some vendors' grandiose claims, there's no single Silver Bullet security product that can guarantee 100% protection against all types of risk. Similarly, there's no 'one-time fix'. IT security is a constant process of evaluating how the dangers are evolving, then:

- Adapting & updating security policies and
- Rolling out new security technologies

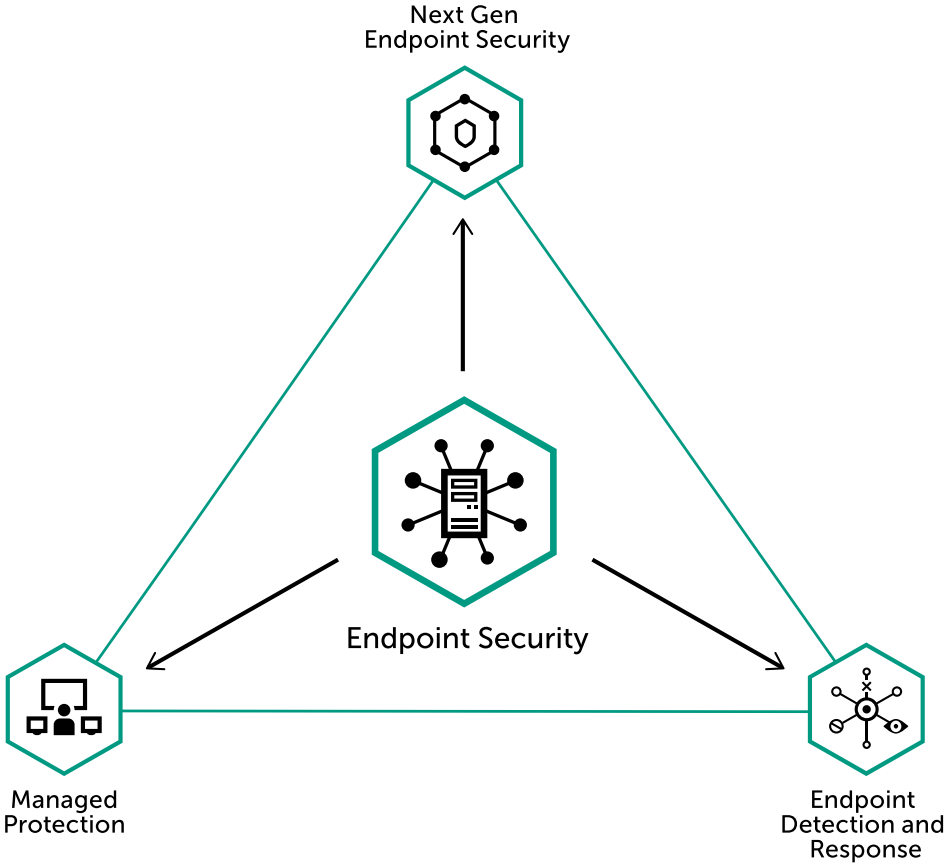
... to deal with new risks.

Kaspersky Endpoint Security addresses these needs through a reliable, proven multi-layered security platform that also protects your bottom line. This tightly integrated solution combines outstanding protection, detection and incident response capabilities, based on unequalled global security intelligence and Next Generation machine learning, to automatically enrich your SOC and enhance your risk mitigation capabilities. Protection for every physical, virtual and cloud-based endpoint is managed together through one console, improving efficiency and reducing your TCO.

This platform includes:

- **Next Gen Endpoint Security**
  Fully scalable protection, based on our award-winning threat intelligence engine and incorporating granular controls, anti-ransomware and exploit prevention technologies.
- **Endpoint Detection and Response**
  Proactively hunting out adversaries and halting threats before they can cause expensive damage, and responding rapidly and effectively to incidents and data breaches.
- **Managed Protection**
  A round-the-clock monitoring and incident response service, from the recognized world leader in investigating APTs, dedicated to hunting down cyberthreats to your organization.

Endpoint Security Solution



How attacks strike

The majority of attacks have four distinct stages:

- **Discovery** – identifying appropriate entry points for the attack
- **Intrusion** – into an endpoint on the corporate network
- **Infection** – often spreading to many locations on the corporate network
- **Implementation** – of the cybercriminal's malicious actions

Stage-by-stage defense

One of the keys to dealing with an attack is to have defenses that are capable of providing protection at each of the four stages of the attack.

Discovery Exposure Prevention
To block access to potential entry points

Intrusion Pre-Execution Protection
To detect threats before they can cause infections

Infection Post-Execution Processes
To detect suspicious behavior – and help prevent the infection performing malicious actions

Implementation Automated Response
To help the victim business to recover systems and data – plus identify how to avoid similar attacks in the future

Multi-layered protection... from a single vendor

We provide defenses for every stage of an attack – and at each stage, we don't just deliver one layer of defense, we provide multiple defense techniques. So our customers benefit from multi-layered protection at every stage of an attack.

Defense Stage 1 – Exposure Prevention
We help to block attacks at potential entry points.

Our protection layers include:

- Network filtering
- Cloud-enabled content filtering
- Port controls

Defense Stage 2 – Pre-Execution Security
We help to stop the 'intruder' from launching.

Our protection layers & services include:

- Endpoint hardening
- Reputation services
- Pre-execution detection – based on machine learning

Defense Stage 3 – Runtime Control
We proactively look out for suspicious behavior on any devices attached to your corporate network, including your employees' own mobile devices.

Our protection layers include:

- Behavioral analysis – based on machine learning – including:
  - Exploit prevention
  - Ransomware protection
- Execution privilege control

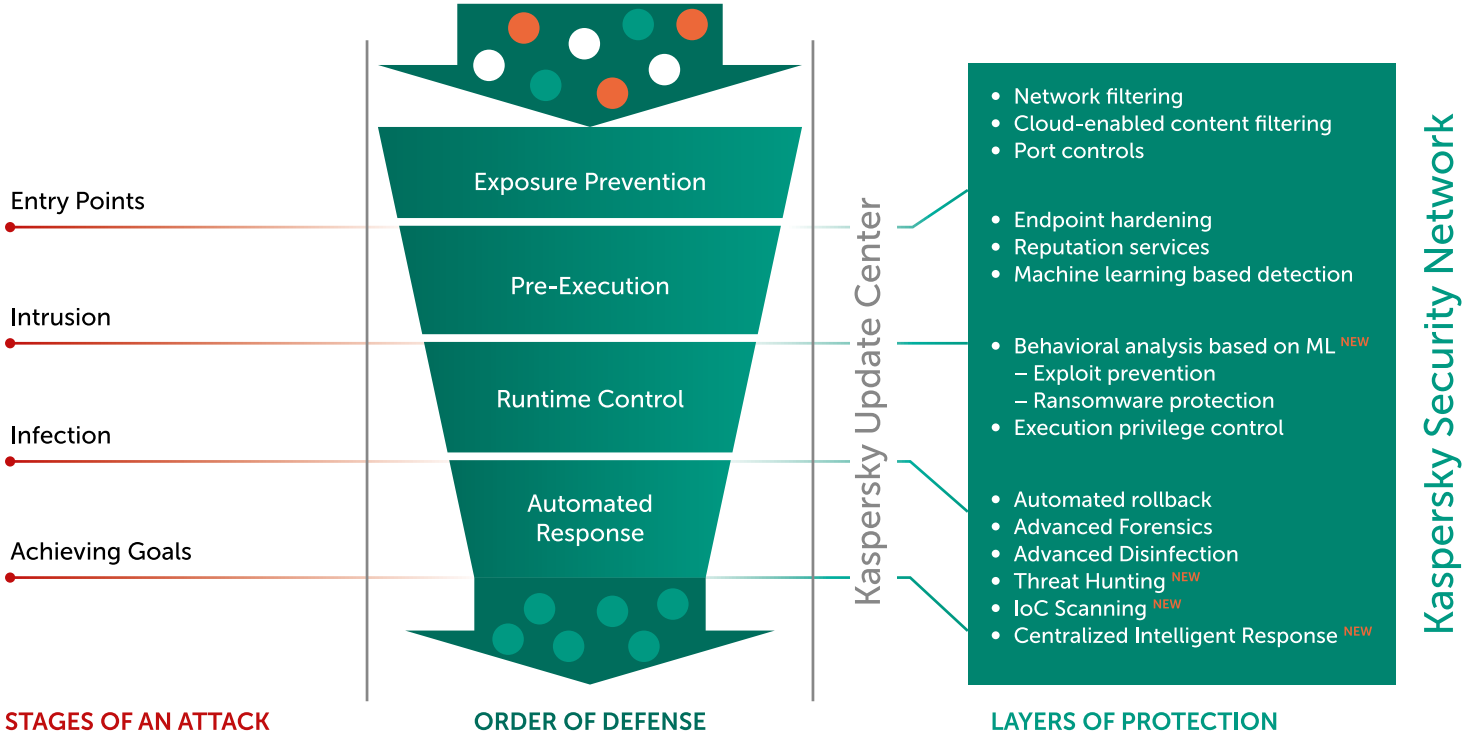
Defense Stage 4 – Automated Response
If your business has suffered an attack, we help you to deal with the aftermath more rapidly.

Our technologies and services include:

- Automatic rollback – to help restore systems to their pre-attack state
- Advanced forensics
- Advanced disinfection
- Threat hunting
- Indicator of Compromise (IoC) scanning
- Centralized intelligent response

Our Meta-Layer helps enterprises do more to protect against dangerous Targeted Attacks and APTs by correlating the findings of individual defense layers – identifying threats that may be capable of slipping through individual defenses.

Attack Chain



Mobile Security

Integrated security and management supporting your mobile security strategy

Based on our 2017 survey, 38% of enterprise businesses experienced exploits or loss through mobile devices as the main attack vector.

$1,700,000

The average Enterprise cost of a security incident involving exploits or data loss through mobile devices

Malicious software, websites and phishing attacks aimed at mobile devices continue to proliferate, while mobile device capabilities are still developing. As an important productivity tool at home and at work, mobile devices are tempting targets for cybercriminals. The rising use of personal devices for business purposes (BYOD) expands the range of device types and platforms within the corporate network and creates additional challenges for IT administrators trying to manage and control their IT infrastructures.

Employees' Personal Devices Are An Enterprise Risk

Employees using their mobile devices for work as well as for personal use increase the chances of your IT security being breached. Once hackers access unsecured personal information on a mobile device, gaining access to users' corporate systems and business data is simple.

No Platform Is Safe

Cybercriminals use a variety of methods to gain unauthorized access to mobile devices, including infected applications, public Wi-Fi networks with low security levels, phishing attacks and infected text messages. When a user inadvertently visits a malicious website – or even a legitimate website infected with malicious code – it puts the security of their device and the data stored on it at risk. Even connecting an iPhone to a Mac to charge its battery can result in malicious threats passing from Mac to iPhone (These threats are relevant to all common mobile platforms: Android, iOS and Windows Phone.)

The Solution: Kaspersky Security for Mobile

Kaspersky Security for Mobile solves these issues by providing multi-layered Mobile Threat Defense (MTD) and mobile management functions. These combined capabilities enable security teams to take a proactive approach to mobile threat management.

All functionality for both endpoints and mobile devices can be managed from the same console, effectively combating corporate cybercrime.

The combination of functional encryption and protection against malware enables Kaspersky Security for Mobile to proactively protect mobile devices rather than merely isolating a device and its data.

Advanced Protection for Mobile Devices

Anti-malware combines with cloud-assisted threat intelligence and machine learning to guard against advanced mobile threats.

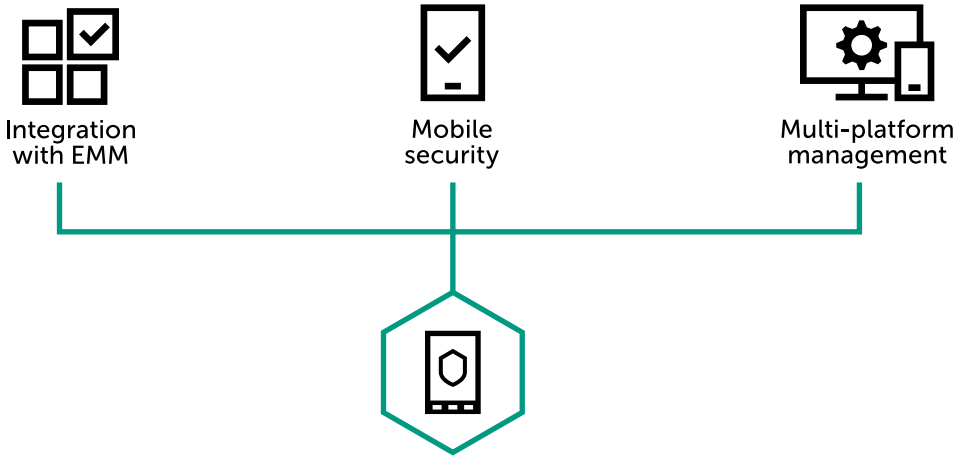
Web Control, Anti-Phishing and Anti-Spam

Powerful web control, anti-phishing and anti-spam technologies protect against phishing attacks and unwanted websites, calls and texts.

Integration with EMM Platforms

Implement and manage mobile security entirely through your EMM console (VMware AirWatch, Citrix XenMobile)

Advanced Protection for Mobile Devices



Hybrid Cloud Security

Borderless security engineered for multi-cloud environments

Our Hybrid Cloud Security solution provides unified, multi-layered protection for cloud-based environments. Wherever you process and store critical business data - in a private or public cloud, or both – we deliver a perfectly balanced combination of agile, continuous security and superior efficiency, protecting your data against the most advanced current and future threats without compromising on systems performance.

Simplified provisioning is achieved through native API integration, while the smallest possible resource footprint is ensured and precise capabilities delivered to defend multi-cloud environments against all forms of cyberthreat. All under unified security orchestration and management.

Next Generation Cybersecurity for Any Cloud

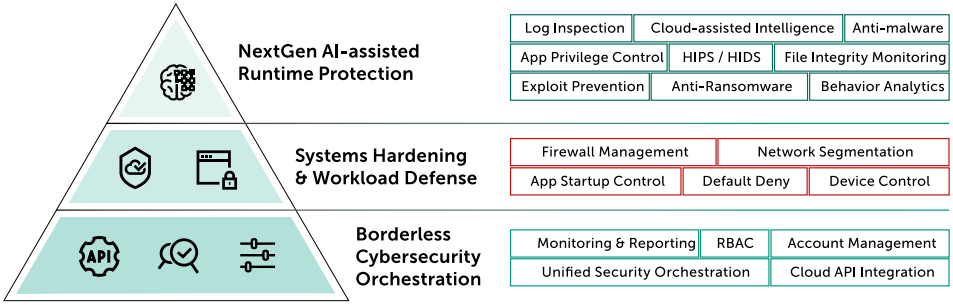
Addressing the need to protect what you deploy in public clouds as part of your shared security responsibility. Integration with cloud APIs enables us to deliver award-winning cybersecurity technologies to every cloud workload.

Unified Orchestration & Transparency

Borderless manageability, flexibility and visibility is delivered via an enterprise-level security orchestration console. Outstanding transparency means you know exactly what's happening right across the security layer of your entire hybrid cloud environment. This visibility, together with the fully automated provisioning of cybersecurity capabilities, enables the seamless orchestration of better and faster security across your cloud estate.

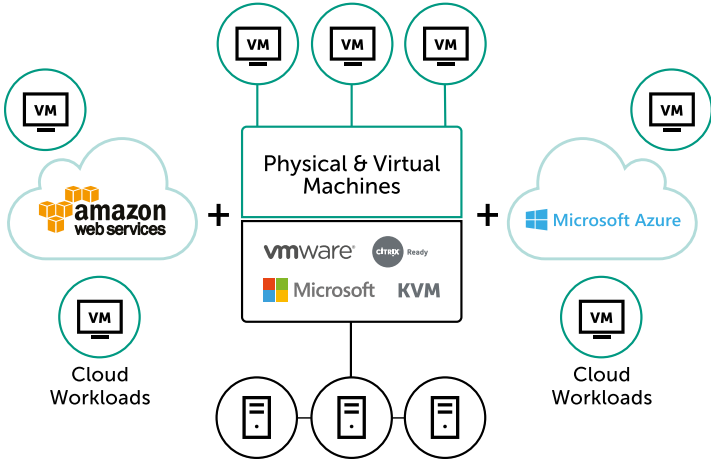
For Elastic and Secure Cloud Environments

Proven security for virtual and physical servers, VDI deployment, storage systems and even data channels. Patented architecture and integration capabilities help build cybersecurity into the core of your IT environment, while maintaining the operational efficiency of business critical systems.



Kaspersky Hybrid Cloud Security

Kaspersky Hybrid Cloud Security gives you everything required to build a perfectly orchestrated and adaptive cybersecurity ecosystem, delivering the precise capabilities your multi-cloud workloads require, while resource efficiency and seamless orchestration remain paramount. Kaspersky Hybrid Cloud Security has been engineered to protect applications and data on your physical, virtual and cloud workloads, ensuring business sustainability and accelerating compliance across your entire hybrid cloud environment.



In your Private Data Center, where corporate workloads are running on physical or virtual servers or even in VDI environments, a number of considerations need to be addressed as part of a successful digital transformation strategy:

- **Secure data access and processing** regardless of which virtualization platform or physical environment your workloads are running on
- **Interoperability between IT and Security layers** using native APIs to ensure near-zero response times to advanced threats
- **Resource-efficient operation** enhancing IT performance and maintaining business-critical systems productivity

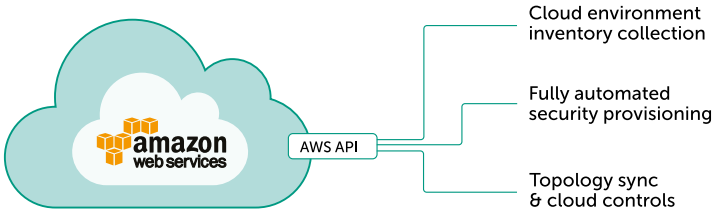
Kaspersky Hybrid Cloud Security offers proven excellence in protecting software-defined data centers built on VMware NSX, Citrix XenServer and XenDesktop, MS Hyper-V, and KVM virtualization platforms, eliminating complexity in managing enterprise-scale environments. Integration with core IT via native APIs helps address security needs with near-zero impact on precious systems performance.

- Integrated agentless security for VMware NSX for vSphere, allowing security and IT layers to interoperate for increased protection.
- Patented Light Agent protection for virtual servers and VDI platforms with resource-efficient and fault-tolerant operation.
- Traditional multi-layered security for physical servers, incorporating anti-ransomware, exploit prevention and behavior detection technologies.

Automated Cybersecurity for Public Clouds

The growing adoption of a cloud services model, where private data center resources expand instantaneously on demand and as needed into external clouds, delivers unprecedented flexibility, agility and clear economic benefits. However, the Shared Security Responsibility Model dictates the need for additional capabilities, enabling an elastic cybersecurity layer that covers your entire cloud environment and protects your Amazon Web Services (AWS) or Microsoft Azure workloads.

Integrates with Amazon Web Services (AWS)



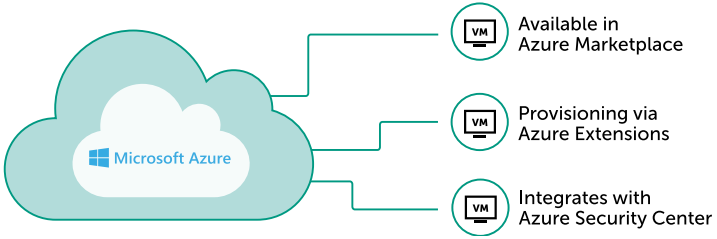
Kaspersky Hybrid Cloud Security helps to defend cloud assets, addressing the need to protect whatever's deployed in the public cloud as a part of your shared security responsibility. Kaspersky Hybrid Cloud Security provides multi-layered protection that integrates with cloud API and is available through MarketPlaces to deliver award-winning cybersecurity techniques to all cloud workloads with greater agility and borderless manageability, for a superior multi-cloud cybersecurity orchestration experience.

- Industry-leading cybersecurity protecting your workloads in public clouds, leveraging native integration via cloud API with Amazon Web Services (AWS) and Microsoft Azure Extensions.
- Complements cloud-native security capabilities and helps protect applications, OSs, data and users in the cloud, supporting GDPR compliance.
- Smart architecture and API integration minimizes cloud resource impact, automating inventory and security provisioning.

Gives Even More Protection

We complement cloud-native tools with proactive cybersecurity, exploit prevention, integrity monitoring, log inspection, apps controls, and even AI-assisted runtime protection and anti-ransomware capabilities. One product to fight every form of cyberthreat.

Engineered for Microsoft Azure



Unstoppable Security for Any Cloud

Cloud adoption has never been so seamless and yet secure. With Kaspersky Hybrid Cloud Security, integration via native APIs allows for easier public cloud infrastructure inventory and automated security provisioning on all your instances in AWS and Microsoft Azure.

Kaspersky Hybrid Cloud Security delivers multiple industry-recognized security technologies to support and simplify your IT environment transformation, securing your migration from physical to virtual, and to the cloud, while visibility and transparency guarantee a flawless security orchestration experience.

Kaspersky Security for Storage

Kaspersky Security for Storage provides robust, high-performance, scalable protection for valuable and sensitive data residing on corporate Network Attached Storages (NAS) and File Servers.

Smooth integration through fast protocols, including ICAP and RPC, preserves storage systems efficiency to maintain reliable, resource-efficient protection and an optimized end-user experience. Reliable, real-time protection for storages includes self-defensive capabilities for optimum continuity.

Reliable and Transparent Data Protection

- Native integration results in flexibility, scalability and outstanding operational efficiency, with no adverse impact on data storage systems' performance and productivity.
- Innovative technologies deliver the most advanced protection capabilities, exceptional fault-tolerance, and can even protect from ransomware attacks.

Secures Your Data Wherever It's Stored

- Natively integrates with the latest NAS and operates on corporate file servers
- All files on data storages are safe, with no need to check anti-malware on endpoints or mobile devices
- Flexible and granular configuration for on-access and on-demand anti-malware scan tasks
- Self-defensive capabilities for optimum operational continuity

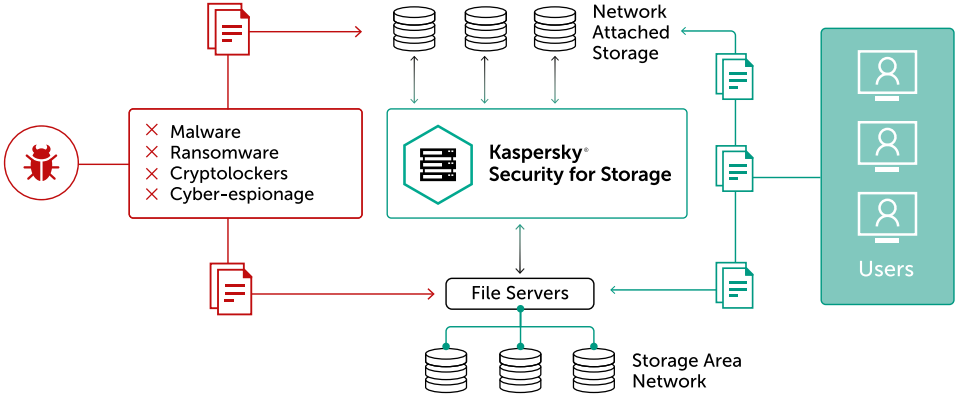
Fights Malware & Ransomware

- Our award-winning anti-malware scanning engine defending all files against the most advanced attacks
- Real-time anti-ransomware protection for NetApp NAS devices via FPolicy (pioneered by Kaspersky Lab)
- Support for a wide range of storage devices, thanks to integration via multiple protocols

Delivers Lightweight yet Reliable Security

- Integration via native API means greater security with less impact on end-user productivity
- Load balancing and fault-tolerance ensure uninterruptable protection
- Full visibility of datafile cybersecurity enabled across your entire storage infrastructure

Kaspersky Security for Storage can be combined with Kaspersky Hybrid Cloud Security, applying best of class protection over both the physical and virtualized components of your corporate data center.



Kaspersky DDoS Protection

The financial impact of a single DDoS attack can be between US$106,000 and US$1,600,000, depending on the size of the business. The cost of organizing a DDoS attack? Around US$20...

As the cost of launching a Distributed Denial of Service (DDoS) attack has decreased, the number of attacks has increased. Attacks have become more sophisticated and difficult to guard against. The changing nature of these forms of attack calls for more rigorous protection.

Unlike malware attacks that tend to propagate automatically, DDoS attacks rely on human expertise and insight. The attacker will research the business they are targeting – assessing vulnerabilities, and carefully choosing the most appropriate attack tools to achieve their objectives. Then, working in real time during the attack, the cybercriminals constantly adjust their tactics and select different tools to maximize the damage they inflict.

To defend against DDoS attacks, enterprises need a solution that detects attacks as quickly as possible.

The Solution: Kaspersky DDoS Protection

Kaspersky DDoS Protection is a total DDoS attack protection and mitigation solution that takes care of every stage of defending your business against all forms of DDoS attack. Three deployment options - Connect, Connect+ and Control – are available.

The instant a possible attack scenario is identified, Kaspersky Lab's Security Operations Center (SOC) is alerted. In Kaspersky DDoS Protection Connect and Connect+ deployment scenarios, mitigation is automatically initiated while our engineers immediately run detailed checks to optimize mitigation depending on the size, type and sophistication of the DDoS attack. With Kaspersky DDoS Protection Control, you decide when we should start mitigation in line with your cyber-security policy, business objectives and infrastructure environment.

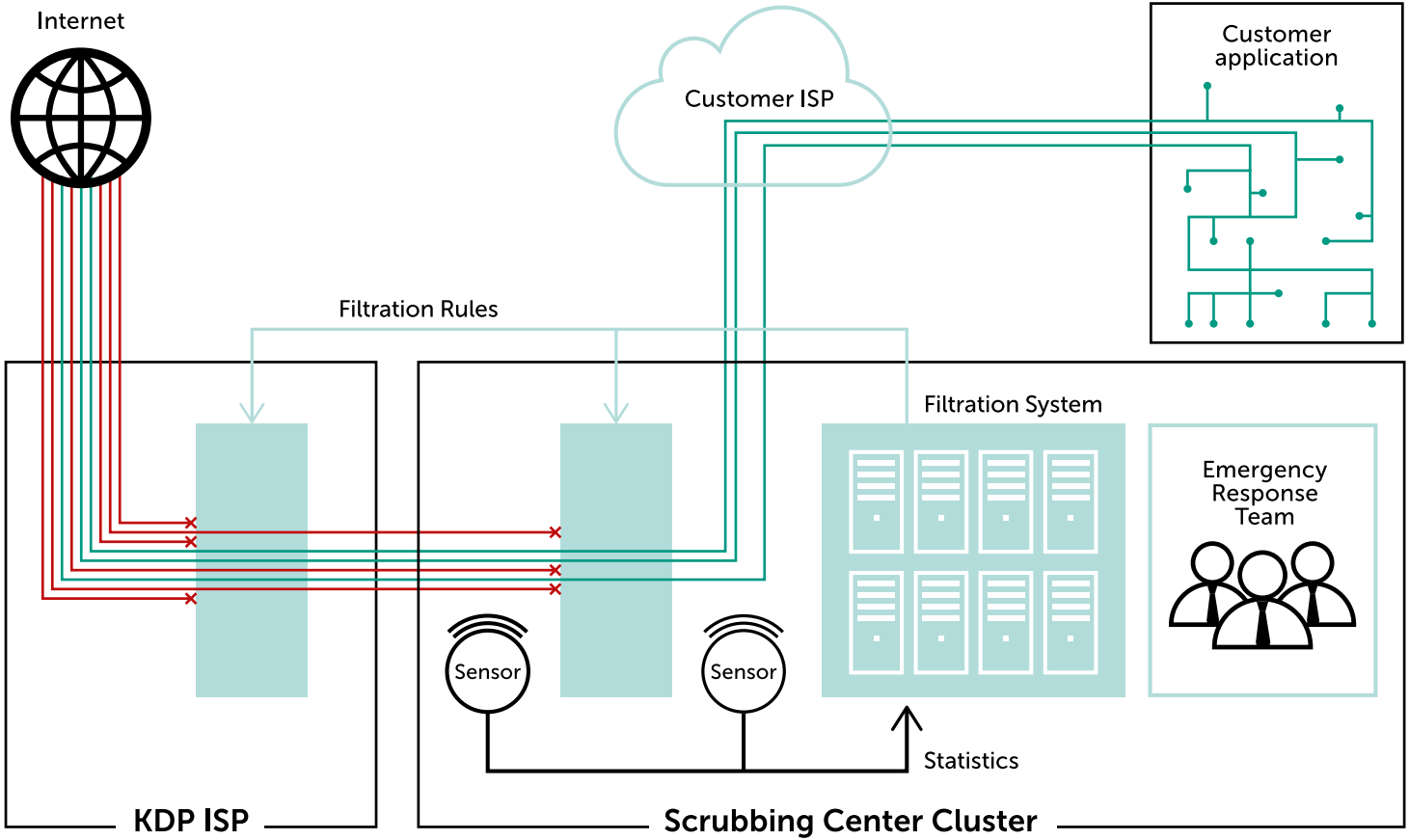
With the flexibility to address different configurations, we can ensure that we fully meet the needs of your business and its online assets.

Kaspersky DDoS Protection Architecture

This total defense solution provides:

- Comprehensive protection for business-critical online resources and network infrastructures
- Flexible deployment options – Kaspersky DDoS Protection Connect, Connect+ and Control
- Highly scalable cleaning centers throughout Europe
- Real-time global DDoS intelligence based on big data security analysis
- Rapid 24/7 protection and support from Emergency Response Teams.

Kaspersky DDos Protection



Threat Management and Defense

Advanced protection and threat intelligence

The protection of highly digitized infrastructures offers significant new enterprise challenges:

- High volume of manual tasks required for incident response
- IT Security team under-staffing, and a lack of high-level expertise
- Too many security events to process, analyze, triage, and respond to effectively within a limited timeframe
- Trust and data sharing compliance issues as the digital infrastructure broadens in scope.
- Lack of visibility, and evidence collection challenges for post-breach analysis

Business value of investing in Threat Management and Defense:

- Reduced financial and operational damage caused by cybercrime
- Reduced complexity through a simple, business-oriented management interface
- Reduced administrative costs though task automation and simplified security compliance processes
- Increased ROI through seamless workflow automation with no disruption to business processes
- Mitigated risk of advanced threats through rapid detection

Digital Transformation – a New Role for Cybersecurity

Digital transformation is a key factor in corporate growth and provides organizations with many new opportunities, but at the same time involves risks associated with ensuring the security of the IT infrastructure, along with compliance and safe data usage. Targeted attacks and complex threats, including Advanced Persistent Threats (APTs), are now amongst the most dangerous risks that enterprises have to deal with. A unified solution to help support accelerated innovation in digital transformation, **Kaspersky Threat Management and Defense** adapts to the specifics of the organization and its ongoing processes through a unique combination of leading security technologies and cybersecurity services, enabling you to build a unified methodology for complete corporate protection against advanced threats and unique targeted attacks.

Supporting the development or augmentation of the organization's threat management strategy, Kaspersky Threat Management and Defense enables the automated collection of information and digital evidence, simplifies manual detection and automates incident analysis, empowered with machine learning. The rich pool of data provided enables complex incident investigation and provides the support and expertise needed to counteract even the most sophisticated threats.

Kaspersky Threat Management and Defense delivers a unique combination of leading technologies and services, supporting the implementation of an Adaptive Security Strategy – helping to Prevent most attacks, Detect unique new threats rapidly, Respond to live incidents and Predict future threats. Kaspersky Threat Management and Defense includes the following components:

- **Kaspersky Anti Targeted Attack** based on leading security intelligence and advanced machine learning technologies combined with network and endpoint monitoring, advanced sandbox technology and threat intelligence-driven analysis. Kaspersky Anti Targeted Attack correlates different events and prioritizes incidents to help organizations to detect targeted attacks, advanced threats and already compromised systems.

- **Kaspersky Endpoint Detection and Response** helps gain endpoint threat visibility, automatically aggregating and centrally storing forensic data. Kaspersky Endpoint Detection and Response uses the same interface as Kaspersky Anti Targeted Attack and the same agent as Kaspersky Endpoint Security, providing a multi-faceted approach to revealing, recognizing and uncovering complex targeted attacks. There's a focus on detecting threats by using advanced technologies, responding in a timely way to attacks and preventing malicious actions by discovering threats on endpoints.

- **Kaspersky Cybersecurity Services** offer prompt and professional assistance during an ongoing incident – and afterwards, helping to reduce the risk of compromised data and minimizing possible financial and reputational damage. Our Cybersecurity Services portfolio includes a broad Security Training curriculum, up-to-the-minute Threat Intelligence, rapid Incident Response, proactive Security Assessments, fully outsourced Threat Hunting services and 24x7 Premium Support.

Depending on the customer's requirements for advanced prevention capabilities and the demands of their specific infrastructure, including the need for complete isolation of corporate data, we can further enrich our Threat Management and Defense solution with the following products, delivering a truly integrated, strategic approach to risk mitigation and the prevention of advanced threats and targeted attacks:

- **Kaspersky Endpoint Security** is a multi-layered endpoint protection platform, based on Next Gen cybersecurity technologies powered by HuMachine Intelligence, delivering flexible, automated defenses against the most advanced known and unknown threats, including fileless attacks and ransomware, through machine learning engines, suspicious behavior detection, controls, data protection and more.

- **Kaspersky Secure Mail Gateway** as functions part of a preventative approach to targeted attacks, providing automated email threat prevention and delivering outstanding protection for traffic running through mail servers against spam, phishing and generic and advanced malware threats. Kaspersky Secure Mail Gateway operates effectively even in the most complex heterogeneous infrastructures, and regardless of which mail delivery model is used: cloud, on-premise, encrypted.

- **Kaspersky Private Security Network** delivers a comprehensive threat intelligence database for isolated networks and environments with stringent data-sharing restrictions, allowing enterprises to take advantage of most of the benefits of cloud-assisted security without releasing any data whatsoever outside the controlled perimeter. It's an enterprise's personal, local and completely private version of Kaspersky Security Network. Kaspersky Private Security Network addresses critical enterprise cybersecurity concerns without a single piece of data leaving the local network.

Kaspersky Anti Targeted Attack

By correlating events from multiple layers – including network, endpoints and the global threat landscape – the Kaspersky Anti Targeted Attack delivers the near real-time detection of complex threats, as well as generating critical forensic data to empower the investigation process.

Kaspersky Anti Targeted Attack provides organizations with:

- Integral business continuity, achieved through building security and compliance into new processes right from inception
- Visibility over shadow IT and hidden threats
- Maximum flexibility, enabling deployment across both physical and virtual environments, wherever visibility and control is needed
- The automation of investigation and response tasks, optimizing the cost-effectiveness of your security, incident response and SOC teams
- Tight, straightforward integration with existing security products, enhancing overall security levels and protecting legacy security investment

Kaspersky Endpoint Detection and Response

Traditional endpoint security products (for example, Kaspersky Endpoint Security) perform a vital role in protecting against a wide range of threats, including ransomware, malware, botnets etc. However, to protect against an even wider range of advanced cyberattacks and intelligent adversaries, enterprises now need to implement additional levels of protection at endpoint level, including endpoint detection and response.

Kaspersky Endpoint Detection and Response helps organizations with:

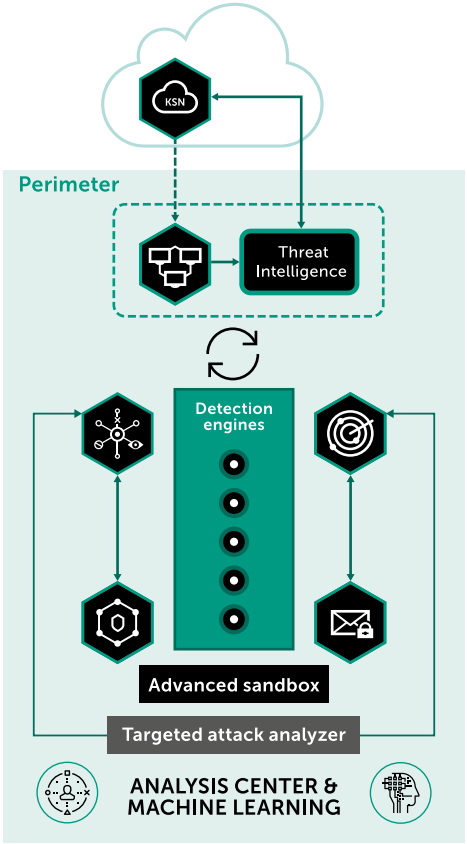
- Automating threat identification & response without business disruption
- Improving endpoint visibility & threat detection via advanced technologies, including machine learning, sandboxing, IoC scanning & threat intelligence
- Enhancing cybersecurity with an easy-to-use, enterprise solution for Incident Response
- Establishing unified and effective Threat Hunting, Incident Management and Response processes.

Kaspersky Secure Mail Gateway

Kaspersky Secure Mail Gateway is an automated email threat prevention solution delivering advanced technologies to protect mail traffic of any kind, as part of single approach to the detection and prevention of targeted attacks. Kaspersky Secure Mail Gateway provides innovative cloud-assisted antispam, anti-phishing and advanced multilayered anti-malware protection with zero-day and anti-exploit capabilities, powered by threat intelligence, machine learning and advanced sandboxing to provide a multi-layered automated approach to email security.

Kaspersky Secure Mail Gateway provides to organizations:

- Automated prevention of known, unknown and future threats
- Signature-based, cloud-assisted file analysis
- File analysis using machine learning methods
- Rapid incident notification
- Seamless improvement of enterprise cybersecurity



Kaspersky Private Security Network

Kaspersky Private Security Network is a local and completely private version of Kaspersky Security Network (KSN), allowing organizations who do not wish to release any data whatsoever outside their controlled perimeter to take advantage of most of the benefits of global cloud-based threat intelligence.

Kaspersky Private Security Network, as a patented technology:

- Provides access to global statistics of URLs and Files
- Categorizes URLs and files with specific verdicts for malicious and whitelisted objects
- Minimizes the damage caused by cybersecurity incidents through real-time threat awareness
- Allows the addition of unique customer -specific and third party threat source verdicts (file hashes)
- Complies with strict regulatory, security and privacy standards.

Cybersecurity Services

Intelligence and expertise, providing a new level of cyber-immunity

Threat Intelligence Portal

By sharing our up-to-the-minute intelligence with customers, Kaspersky Lab provides enterprises with a 360-degree view of the methods, tactics and tools used by threat actors, helping them to guard against modern cyberthreats. Our broad range of threat intelligence services helps ensure your Security Operations Center and/or IT security team is fully equipped to counteract even the most sophisticated attacks.

- **Threat Data Feeds.** Enhance your security controls (SIEM, IDS, firewalls etc.) and improve forensic capabilities with our up-to-the-minute cyberthreat data, shared in a wide range of formats and delivery methods
- **APT Intelligence Reporting** delivers exclusive, proactive access to descriptions of high-profile cyber-espionage campaigns, including Indicators of Compromise (IOCs) and YARA rules.
- **Financial Threat Intelligence Reporting** is focused on threats aimed specifically at financial institutions, including targeted attacks, attacks on specific infrastructure (e.g. ATM/POS) and tools developed or sold by cybercriminals to attack banks, payment processing companies, ATMs and POS systems.
- **Tailored Threat Reporting.** Threat intelligence tailored to your specific organization or country, derived from proprietary and open sources including both deep and dark web.
- **Threat Lookup.** A web portal giving you complete access to all the knowledge acquired by us at Kaspersky Lab about threat indicators and their relationships.
- **Cloud Sandbox** allows you to submit suspicious files to Kaspersky Lab, obtain a detailed description of the file's behavior with the help of our world-leading technology, and run comprehensive and deep investigations based on tight integration with Kaspersky Threat Lookup.
- **Phishing Tracking.** Real-time notifications about ongoing phishing attacks targeting you or your customers.
- **Botnet Tracking.** Real-time notifications about ongoing botnet attacks threatening your customers and your reputation.

Security Assessment

Kaspersky Security Assessment Services – expert-level security analysis and cutting-edge research, brought together to test information systems of any level of complexity in real-world environments.

Penetration Testing
Threat Intelligence-driven adversary simulation, demonstrating potential attack vectors and providing an overview of your corporate security posture from the standpoint of an attacker.

Application Security Assessment
An in-depth search, hunting out business logic flaws and implementation vulnerabilities in applications of any kind, from large cloud-based solutions to embedded and mobile applications.

Payment Systems Security Assessment
Comprehensive analysis of the hardware and software components of payment systems, aimed at revealing potential fraud scenarios and vulnerabilities leading to financial transaction manipulations.

ICS Security Assessment
Case-specific threat modelling and vulnerability assessment of Industrial Control Systems and their components, providing insights into your current attack surface and the potential business impact of an attack.

Transportation Systems Security Assessment
Specialized research focused on identifying security problems relating to mission-critical components of modern transportation infrastructures, from Automotive to Aerospace.

Smart Technologies and IoT Security Assessment
A detailed evaluation of today's highly-interconnected devices and their back-end infrastructure, revealing vulnerabilities in firmware, network, and application layers.

Threat Hunting

Proactive threat hunting techniques carried out by highly qualified and experienced security professionals, helping to uncover advanced threats hiding within the organization.

- **Kaspersky Managed Protection**
  Round-the-clock monitoring and continuous analysis of your cyberthreat data by Kaspersky Lab experts.

- **Targeted Attack Discovery**
  A comprehensive offering, enabling the proactive identification of any current or historical signs of compromise, and response to attacks previously missed.

Incident Response

Kaspersky Lab's Incident Response Services are carried out by highly experienced cyber-intrusion analysts and investigators. The full weight of our global expertise can be brought to bear on the resolution of your security incident.

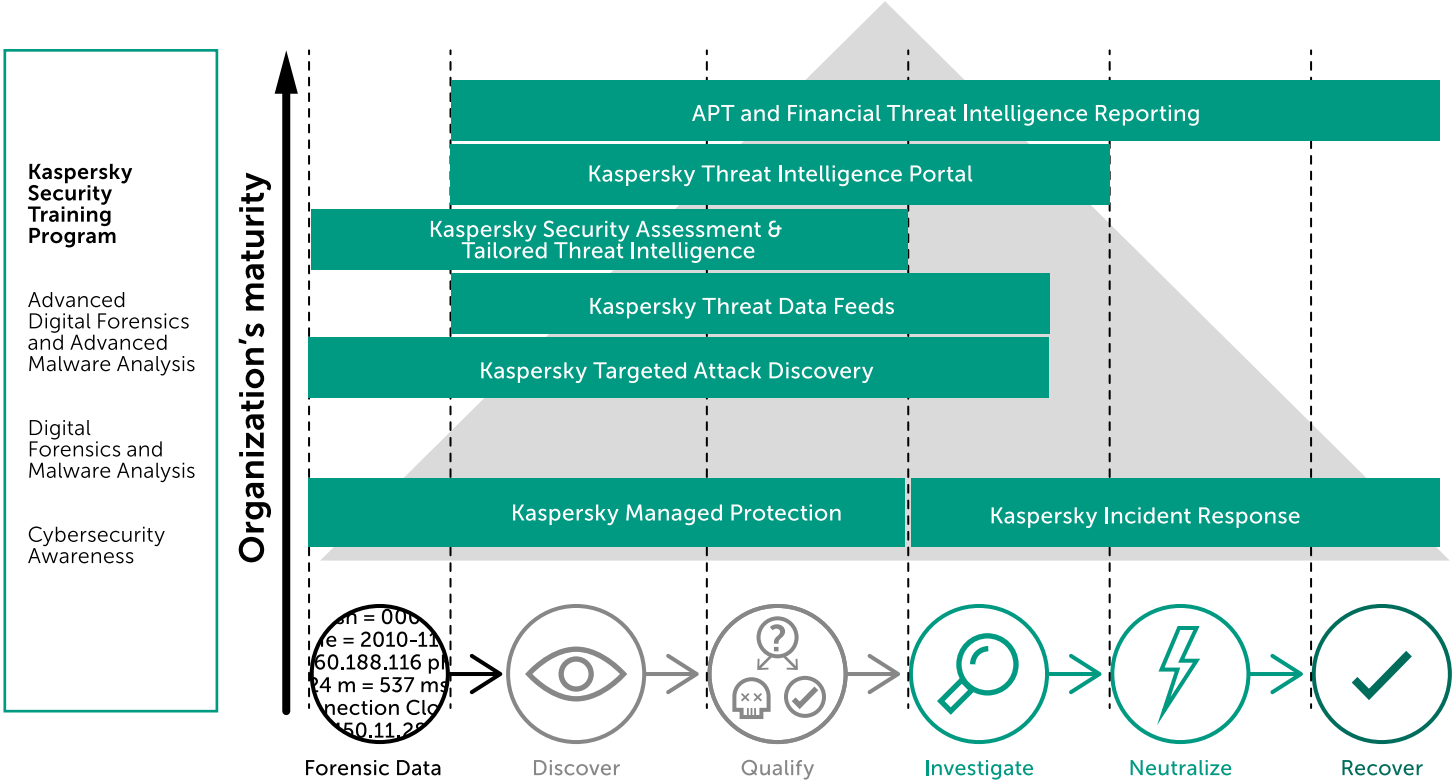
- **Incident Response.** Covering the entire incident investigation cycle to completely eliminate the threat to your organization.
- **Digital Forensics.** Analysis of the digital evidence relating to a cybercrime, leading to the creation of a comprehensive report detailing all relevant findings.
- **Malware Analysis.** Providing you with a complete picture of the behavior and functionality of specific malware files.

Security Training

We offer a portfolio of courses covering everything from fundamentals to advanced techniques and tools used for digital forensics, malware analysis and incident response, enabling organizations to improve their cybersecurity knowledge pool in these areas.

- **Digital Forensics:** Courses are designed to fill experience gaps – developing and enhancing practical skills in searching for digital cybercrime traces and in analyzing different types of data for restoring attack timelines and sources.
- **Malware Analysis and Reverse Engineering:** Courses provide the knowledge needed to analyze malicious software, to collect IoCs (Indicators of Compromise), to write signatures for detecting malware on infected machines, and to restore infected/encrypted files and documents.
- **Incident Response:** Courses will guide your in-house team through all stages of the incident response process, equipping them with the comprehensive knowledge needed for successful incident remediation.
- **Efficient Threat Detection with YARA:** Participants will learn how to write the most effective YARA rules, how to test them and how to improve them to the point where they uncover threats that are undiscoverable through other methods.

Kaspersky Cybersecurity Services



Cybersecurity Awareness

Building a safe corporate cyber-environment with gamified training

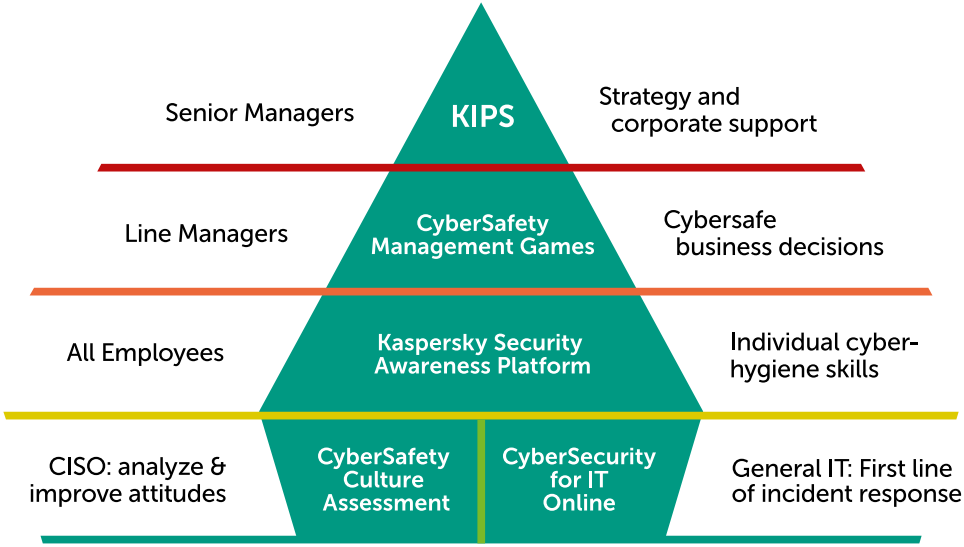
On average, enterprises must pay around $1,155,000 to recover from attacks caused by careless/uninformed employees, while SMBs spend $83,000. More than 80% of all cyber-incidents are caused by human error. Phishing attacks alone cost up to $400 per employee per year.

Enterprises lose millions recovering from staff-related incidents – but the effectiveness of traditional training programs intended to prevent these problems is limited, and they usually fail to engender the desired behavior and motivation.

Kaspersky Lab offers a family of computer-based training products that leverage modern learning techniques and address all levels of the organizational structure. Our training program has already proved its effectiveness – both for our customers and for our Kaspersky Lab partners:

- Up to 90% decrease in the number of incidents
- 50-60% reduction in potential monetary losses associated with cyber-risks
- Up to 93% probability of knowledge being used in daily life
- 86% of participants would recommend their course to colleagues.

Kaspersky Security Awareness Training Products



Winning Approach

- **Building behavior, not just delivering knowledge**: the learning approach involves gamification, learning-by-doing, group dynamics, simulated attacks, learning paths, automated reinforcement of skills, etc. This results in strong behavioral patterns and produces long-lasting cybersecurity improvements;
- **Serious, practical content** (based on the power of Kaspersky Lab R&D) delivered as a series of interactive exercises fine-tuned to meet the business needs and time/format preferences of different organizational levels: senior managers, line managers, average employees;
- **Real-time measurement, painless program management**: purpose-built training software delivers automated training assignments, skills assessments, and reinforcement through repeated simulated phishing attacks and auto-enrolment in training modules. Courses can be managed and delivered by Kaspersky Lab partners or by the customer's own T&D teams (Train-the-Trainer programs and support are provided by Kaspersky Lab).

How It Works

- The training covers a wide range of security issues – from data leakage and ransomware to internet-based malware attacks, safe social networking and mobile security.
- The continuous learning methodology fuels a constant reinforcement of skills and drives motivation deep into the organization.
- Training courses which address different organizational levels and functions together create a collaborative CyberSafety culture, shared by everyone and driven from the top.
- Training features analytical and reporting tools that measure employee skills and learning progress, as well as program effectiveness on a corporate level.
- Educational plans and best practices provided by Kaspersky Lab facilitate program implementation and help the customer's IT Security and T&D teams get the most out of Security Awareness initiatives.

Industrial Cybersecurity

Specialized protection for industrial control systems

Although air gaps between industrial floors and the outside world used to be sufficient to offer a good level of protection, that's no longer the case. In the era of Industry 4.0, most non-critical industrial networks are accessible via the internet, whether or not by choice.

Malicious attacks on industrial environments have increased significantly in recent years. Risk to supply chains and interruptions to business operations have ranked as the number one business risk concern globally for the past three years; cyber-incident risk is the number one emerging concern. For businesses operating industrial or critical infrastructure systems, the risks have never been greater.

Industrial security has consequences that reach far beyond business and reputational protection. In many instances, there are significant ecological, social and macro-economic considerations when it comes to protecting industrial systems from cyberthreats. Every critical infrastructure needs the highest possible levels of protection against a growing range of threats.

At the same time, industrial environments need an integrated solution that maintains the availability of industrial processes by detecting and preventing actions (intentional or accidental) that could disrupt or halt vital services.

The Solution: Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity is a portfolio of technologies and services designed to secure every industrial layer, including SCADA servers, HMI, engineering workstations, PLCs, network connections and people – without impacting on operational continuity and the consistency of the industrial process. Flexible, versatile settings mean the solution can be configured to meet the unique needs and requirements of individual industrial facilities.

The solution has been developed to protect critical infrastructures, built on a number of different industrial control systems. The flexibility and scope of Kaspersky Industrial CyberSecurity allow organizations to configure their solution in strict accordance with the requirements of their specific ICS environment. The optimal configuration of security technologies and services is established through a full infrastructure audit carried out by Kaspersky Lab experts.

Kaspersky Lab's approach to protecting industrial systems is based on more than a decade's expertise in discovering and analyzing some of the world's most sophisticated industrial threats. Our deep knowledge and understanding of the nature of system vulnerabilities, coupled with our close collaboration with the world's leading law enforcement, government and industrial agencies, including Interpol, Industrial Internet Consortium, various ICS vendors and regulators has enabled us to take a leadership role in addressing the unique requirements of industrial cybersecurity.

This highly specialized solution:

- Provides a holistic cybersecurity approach for industrial environments
- Offers the full cycle of security services, from cybersecurity assessment to incident response
- Supplies unique security technologies that were developed specifically for industrial systems
- Minimizes downtime and industrial process delays.

Kaspersky Industrial CyberSecurity

Technologies

Anomaly Detection (DPI)

Integration with other systems

Anti-Malware

Integrity Control

Centralized Management

Incident Investigation

Intrusion Detection System

Services

Education and Intelligence

- Cybersecurity training
- Awareness programs
- Threat Intelligence

Expert Services

- Cybersecurity assessment
- Solution integration
- Maintenance
- Incident response

Fraud Prevention

The advanced solution for a seamless user experience and proactive prevention of fraud in real-rime

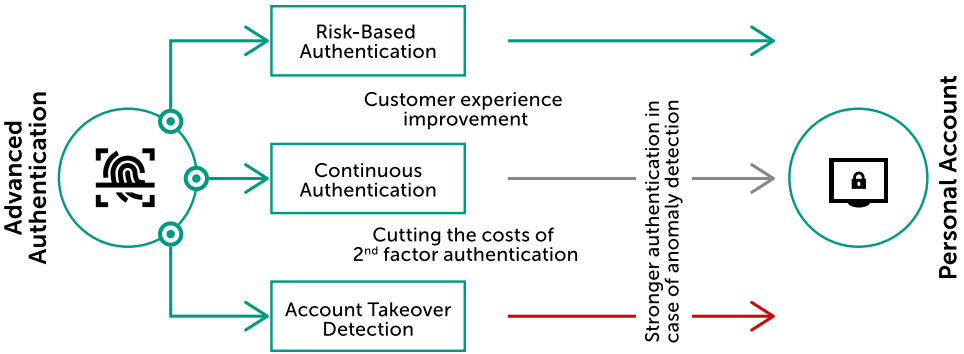
Going digital isn't just a trend: it's a necessity. As most customers now use online and mobile channels for their daily needs, businesses must deliver high-level services with maximum functionality. Simultaneously, they must juggle online security with a frictionless customer experience. Which is where Kaspersky Fraud Prevention comes in - letting you grow and develop your online and mobile channels without the added stress of security concerns and online usability issues.

Kaspersky Fraud Prevention is powered by a complex range of advanced technologies including behavioral analysis and biometrics, device and environment analysis brought together in the Kaspersky Fraud Prevention Cloud. Machine learning is applied for the proactive detection of sophisticated fraud schemes across web and mobile channels. This empowers fraud monitoring systems to benefit from additional context for more accurate, proactive decision-making, as well as for the intelligent and adaptive use of step-up authentication.

The solution consists of two full-featured products which can either be used separately, solving relevant business issues, or together, significantly improving security levels and protection from fraud as well as enhancing user experience.

Advanced Authentication has been developed to improve the user experience, cut the cost of second factor authentication and continuously detect suspicious activity, leading to business growth and higher levels of security.

Right from the moment of initial login, Advanced Authentication continuously analyzes events, enabling risk levels to be calculated and appropriate recommendations made.



Automated Fraud Analytics uses a perfectly balanced combination of cutting-edge technologies with global threat intelligence and human expertise. This capability helps identify and alert the organization to possible fraudulent activity in advance, analyzing crucial data to enable accurate and timely decisions to be made and complicated fraud cases to be uncovered.

Events during user sessions which affect users, their devices and their environments feed fraud management systems with the data necessary for timely and accurate decision-making. Ready-to-use incidents generated within Kaspersky Fraud Prevention Cloud provide insights into real fraud cases, getting right to the root of the problem.

Along with advanced technologies and expertise, Kaspersky Fraud Prevention offers:

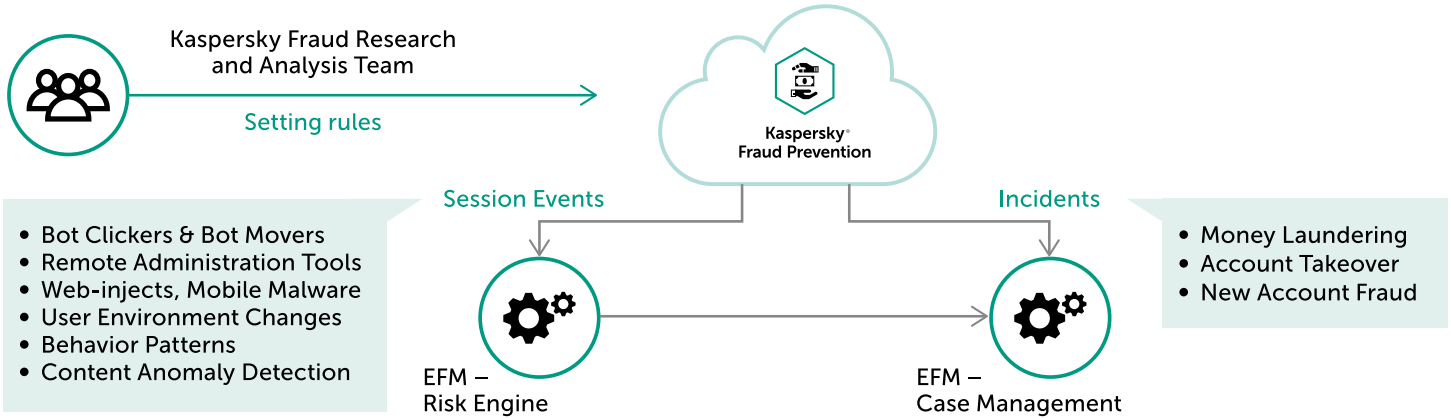
Maintenance Service Agreement - superior support for all your security needs, protecting your business with world-class assistance from our local teams of certified engineers.

Implementation services – dedicated implementation engineers interconnecting our product line with existing security and fraud prevention solutions.

Fraud Prevention consulting - business consultancy to help build the right fraud prevention strategy, from a team of professionals with a range of expert skillsets and multi-industrial expertise.

Key benefits of Kaspersky Fraud Prevention:

- Growth of online and mobile channels without the added stress of security concerns and usability issues
- Control of fraud prevention costs and cutting fraud losses
- Real-time detection of advanced fraud before any transaction has occurred
- Enriching Enterprise Fraud Monitoring solutions with extra data



IoT Security

Justifying your customers' trust through securing their privacy

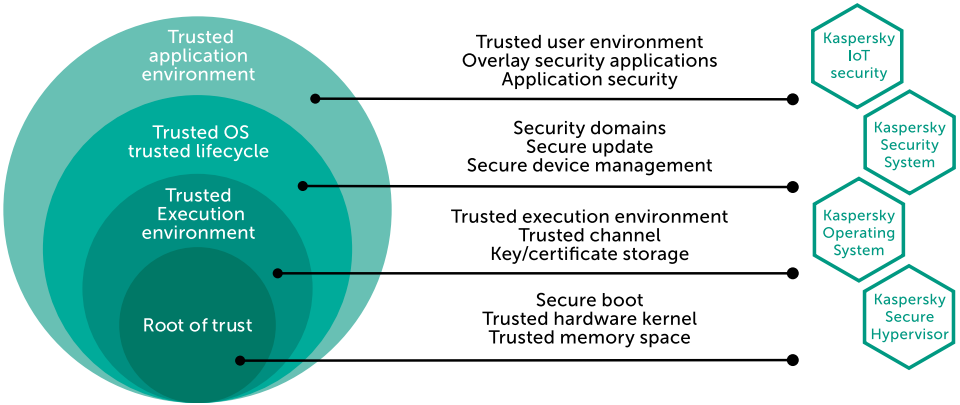
The Internet of Things (IoT) is a new paradigm that's changing the world. It could make our world safer, improve our health, save us time and money, reduce waste and add a new dimension to production control and life in general.

Cybersecurity has traditionally been associated with the security of personal data. In the IoT era, however, this has transformed into the security of privacy. Violations of user privacy such as remote surveillance via smart home cameras, multimedia or baby monitors; interference in the functioning of household devices; unexpected shutdowns and the failure of everyday services – all of this is unacceptable to the end user.

At the same time, the Internet of Things provides tremendous opportunities for device manufacturers (including hardware components and software), telecom service providers and the systems integration market. A lack of trust in IoT solutions among end-users could block or significantly slow down realization of these potential opportunities. That's why end-to-end security of IoT solutions is a top priority for all those involved.

As things stand, IOT edge devices and telecoms equipment provided to customers can easily incorporate cybersecurity violations. Hardware may fail to control the integrity of the firmware, and devices are sometimes shipped with preinstalled passwords, including administrator passwords. Weak network security settings or the use of old and vulnerable software can also be issues. Add to that a lack of software update processes, meaning that vulnerable devices can work for years without updates, and it's clearly just a matter of time before the device is successfully attacked.

Guarantees of trust at device level



The principle of a chain of trust forms the basis for guaranteeing the secure functioning of an IoT device. Including edge devices and infrastructure elements (gateways). This principle begins with the use of a root of trust at hardware level.

This technology carries out a trusted boot of an operating system, including the integrity of OS image checking, applying cryptography and mechanisms of hardware-assisted secure storage for key information. Trusted boot is crucial for key IoT infrastructure devices such as gateways, ensuring the operating system is booted from predefined media and only after the equipment has successfully passed specific integrity checks.

The next important element in the chain of trust is a secure operating system capable of ensuring the proper execution of software that is not considered to be trusted. Recent developments in computer technology make it possible to implement an environment at OS level that restricts the behavior of applications that cannot be considered trusted.

The IoT concept encompasses a huge variety of appliances, gadgets, technologies, software and communication protocols. But this heterogeneous environment generates many security risks that could seriously hamper any aspect of our IoT-connected lives. Kaspersky lab has engineered a number of products which help minimize the associated risks:

- **Embedded Systems Security**
  Harden and protect your Microsoft Windows based embedded devices and computers with a solution created to optimize security for low-end systems with limited memory capacity, which doesn't require ongoing maintenance or internet connectivity.

- **KasperskyOS**
  The KasperskyOS operating system is designed to protect diverse and complex embedded systems from the consequences of malicious code, viruses and hacker attacks, through strong separation and policy enforcement. KasperskyOS creates an environment where a vulnerability or bad code is no longer a big deal. The Kaspersky Security System protection component controls interactions across the whole system, rendering the exploitation of vulnerabilities useless.

- **Kaspersky Security System**
  Kaspersky Security System is a security policy verdict computation engine capable of working simultaneously with different types of security policies (role-based and mandatory access control, temporal logic, control flow, type enforcement, etc.) and can be customized to meet a client's needs. The more precise the policies, the more control and security afforded the entire system.

  Kaspersky Security System can be used together with KasperskyOS (the most secure configuration) as well as in a Linux-based solution (secure actions in an insecure system).

- **Kaspersky Secure Hypervisor**
  Kaspersky Secure Hypervisor (KSH) runs on the KasperskyOS microkernel. With KSH, potentially untrusted virtualized guest operating systems can be separated from each other and all communications between them can be controlled and trusted, even though they are physically running on the same hardware platform. An additional benefit of KSH is its ability to reduce hardware maintenance costs.

- **Kaspersky Transportation Security Service**
  Built-in 'Security for Safety' based on KasperskyOS technology – a single secure gateway into Electronic Control Units (ECUs), and a spectrum of security assessment services addressing the needs of current and future connected vehicles.

- **Secure Communication Unit**
  The Secure Communication Unit (SCU) is a communication gateway control unit, connected to several subnets and/or gateway controllers to those subnets within the car network. Thus, the SCU is a single gateway to external communications, whereas internal devices can communicate within a domain or even between domains without using SCU services. The SCU is powered by KasperskyOS and hardened by Kaspersky Security System. KasperskyOS controls all interactions within the SCU at the lowest level, and enforces Kaspersky Security System's policy verdicts. Only explicitly permitted interactions are possible.

Embedded Systems Security

All-in-one security specifically designed for Embedded systems

Operating as they do with real money and credit card credentials, Embedded systems are targets of choice for cybercriminals, so require the highest levels of focused, intelligent protection. Now is the time to apply well-proven technologies like Device Control and Default Deny as a first line of defense.

Today we see embedded systems everywhere: in ticketing machines, ATMs, kiosks, Point of Sale systems, medical equipment... the list goes on.

Embedded systems are a particular security concern as they tend to be geographically scattered, challenging to manage and rarely updated. But systems working with cash and customer credentials have to be fault-tolerant and resistant. Embedded devices must not just be protected against threats in themselves, but must be inaccessible by cybercriminals or by an inside attacker as an entry point into the corporate network.

Standard security regulations for embedded devices tend to cover only antivirus based security or system hardening, which is not enough. A purely antivirus approach is of limited effectiveness against current embedded systems threats, as has been amply demonstrated in recent attacks.

Default Deny for Applications, Drivers and Libraries, boosted by Device Control functionality, is the only approach which can ensure the safety of obsolete critical systems still in use.

The Solution: Kaspersky Embedded Systems Security

Kaspersky Lab has created a security solution specifically for organizations operating embedded systems, reflecting their unique functionality and OS, channel and hardware requirements, while focusing on the specific threat environment faced by these systems and fully supporting the Windows XP family.

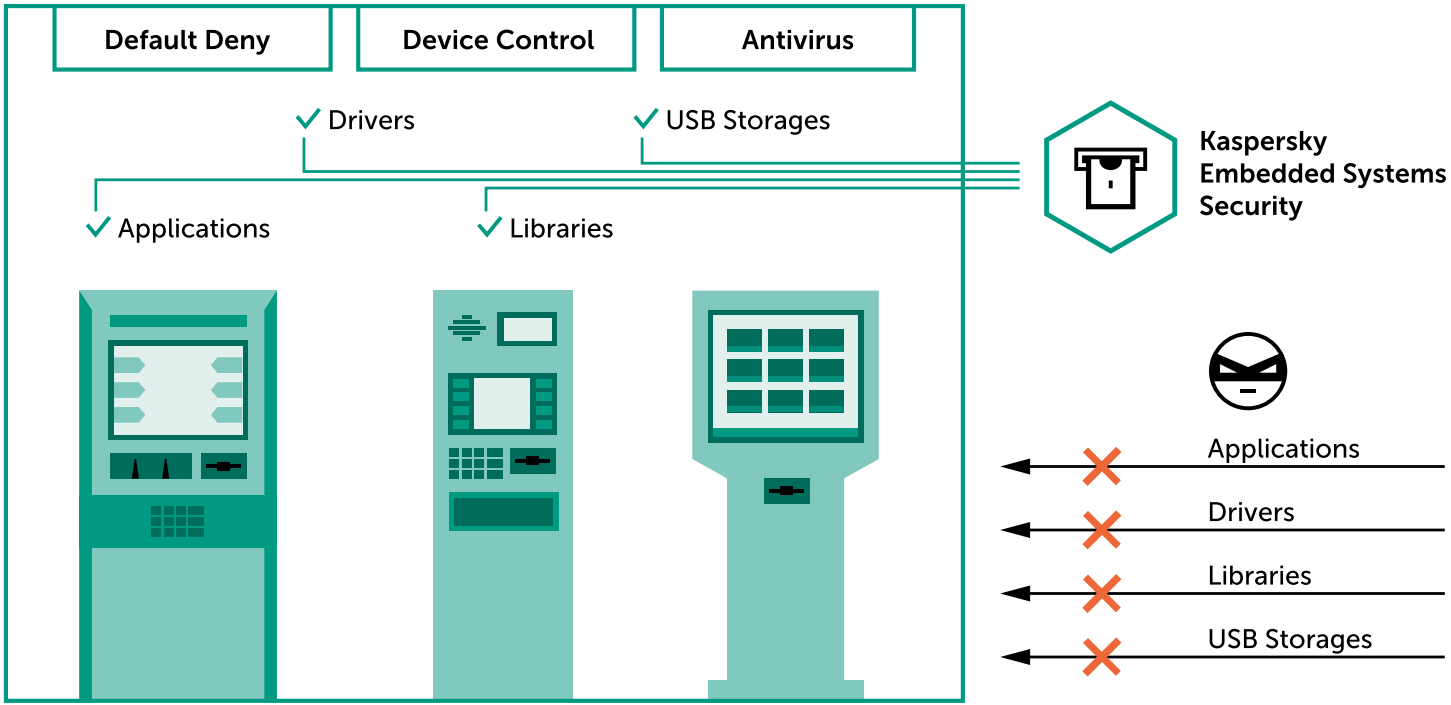
Kaspersky Embedded Systems Security offers a 'Default Deny only' operational mode, where system requirements start from 256Mb of RAM and 50Mb HDD space for Windows XP for low-end hardware systems.

There's also an on-demand scan mode supplied by an optional Antivirus module, including firewall management. This module is powered by the Kaspersky Security Network, with patch management facilities if required.

So this single solution meets three key objectives:

- Efficient security for 'difficult to manage' systems
- Compliance with PCI DSS requirements 5.1, 5.1.1, 5.2, 5.3 and 6.2
- A soft timeline for obsolete systems and hardware replacement

The solution has been designed specifically to mitigate cybersecurity risks to systems based on Embedded operating systems, protecting the attack surfaces unique to these architectures while respecting related hardware and efficiency considerations. A single intuitive console gives you the control and visibility you need to manage effective multi-layered security for your endpoints, your critical systems and your whole IT infrastructure



Premium Support And Professional Services

A choice of services to ensure that enterprises extract maximum benefit from Kaspersky Lab products

Premium Support

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 hundreds of thousands of dollars. Our premium support plans focus on achieving precisely 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.

Kaspersky Lab offers a choice of premium support programs that treat your IT security issues as high priority at all times, helping to keep your business running smoothly, focusing the full force of our expertise directly on finding the fastest, most effective route to getting you safely back to full performance.

Our premuim support plans include:

- Dedicated Technical Account Manager
- 24/7 support via dedicated phone line
- Incident response SLAs
- Proactive alerts to new threats

Professional Services

Cybersecurity is a big investment. Get the most out of it by engaging with experts who understand exactly how you can optimize your investment to meet the unique requirements of your company.

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 Lab products across your enterprise IT infrastructure.

Kaspersky Lab Professional Services ensure that your response to change or transition is smooth, effective and doesn't cause undue interruption to business operations.

Kaspersky Professional Services comprises:

- Implementation and Upgrade
- Configuration
- Health-Check
- Product Training

About Kaspersky Lab

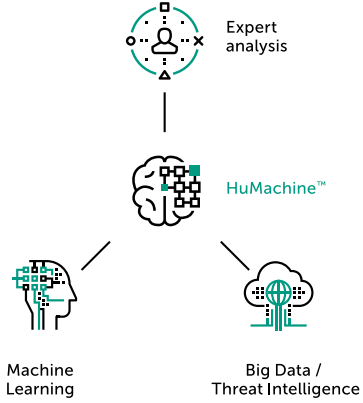
Kaspersky Lab is one of the world's fastest-growing cybersecurity companies and the largest one that is privately owned.

Our independence allows us to be more agile; to think differently and act faster. We are constantly innovating, delivering protection that's effective, usable and accessible. We pride ourselves on developing world-leading security that keeps us – and every one of our 400 million users and 270,000 corporate clients – a step ahead of potential threats.

Our commitment to people as well as advanced technology also keeps us ahead of the competition.

Visit kaspersky.com/enterprise to find out more about Kaspersky Lab's unique expertise and our Security Solutions for Enterprise.

For Notes



Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com