Kaspersky Enterprise Cybersecurity

# Kaspersky Security Solutions for Enterprise 2017

#TrueCybersecurity

# Kaspersky Enterprise Security Solutions

## Technological

### Anti Targeted Attack

Comprehensive multi-vector discovery and risk mitigation of advanced threats and targeted attacks

### Endpoint Security

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

### Cloud Security

Borderless security engineered for your hybrid cloud

### Cybersecurity Services

Leveraging Threat Intelligence, Security Training, Incident Response and Assessment from the world leader

### Security Operations Center

Empowering your SOC with the tools and information to efficiently detect and remediate threats

### Fraud Prevention

Proactive detection of cross-channel fraud in Real Time

## By Industries

### Financial Services Cybersecurity

Providing Financial Services with the tools to raise security levels, prevent and predict cyber-incidents and respond efficiently

### Telecom Cybersecurity

Efficient protection for telecoms infrastructure and information systems against the most advanced cyberthreats

### Healthcare Cybersecurity

Protecting healthcare infrastructures and sensitive clinical data in a ruthless cyberthreat landscape

### Data Center Security

Empowering your data center to detect and respond to the most advanced cyberthreats

### Government Cybersecurity

Security controls and services geared to the demands of government organizations and related public bodies

### Industrial Cybersecurity

Specialized protection for industrial control systems

# Securing the Enterprise

Kaspersky Lab is a global cybersecurity company celebrating its 20 year anniversary in 2017. Kaspersky Lab's deep threat intelligence and security expertise is constantly transforming into security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats.

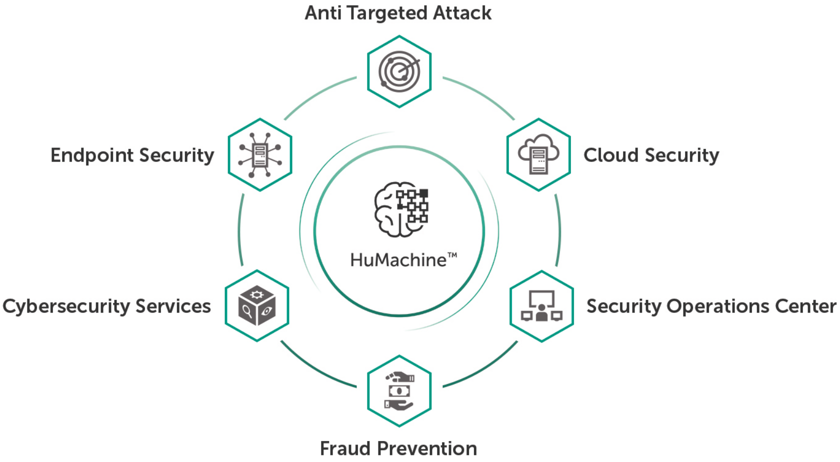
## Taking enterprise security seriously

The costs of a security breach are substantial: In Kaspersky Lab's 2016 Global IT Security Risks Survey, we found that the average direct recovery cost to an enterprise is US$861,000. To avoid these costs and the disruption associated with them, enterprises must strengthen the type and level of protection within their IT infrastructure.

Based on the security intelligence which is fundamental to all our products and services, Kaspersky Lab solutions provide prediction, prevention, detection and response capabilities across a variety of enterprise infrastructure segments and emerging technologies: endpoints, online and mobile, virtual infrastructure, data centers, industrial control systems, and more.

Kaspersky Lab is a pioneer in helping businesses to upgrade their security strategies to better defend against the latest advanced threats and targeted attacks. We offer a unique combination of technologies and services – all underpinned by world-leading security intelligence – to help businesses detect targeted attacks and mitigate the risk at an earlier stage, before severe damage is caused.

By addressing every possible stage of IT incidents, Kaspersky Lab solutions deliver a holistic, adaptive and strategic approach to enterprise security. Our philosophy is straightforward: the best intelligence combined with the best technologies delivers the best protection.



# Anti Targeted Attack

## Comprehensive multi-vector discovery and risk mitigation of advanced threats and targeted attacks

Targeted attacks are long-term processes that compromise security and give the attacker control over the victim's IT, while evading detection through traditional security technologies.

While some attackers use Advanced Persistent Threats (APTs), which can be very effective but expensive to implement, other 'targeted attacks' are much cheaper to mount and can be just as devastating. These targeted attacks, using basic techniques – social engineering, stolen employee credentials, legitimate software or even malware covered by a stolen certificate – may not make the headlines, but they're everywhere.

Most enterprises have already made a major investment in traditional IT security solutions, located primarily at gateway level. However, while these preventative security technologies can be very effective in protecting against common threats – including malware, data leakage, network attacks and more – they are clearly not enough: the overall number of business security incidents and breaches has not decreased one iota.

Today even with innovative technologies like Sandbox, EDR and other 'next gen' solutions, the challenge stays the same - how to choose the right incident and which incident relates to the most critical threats. Specialized discovery solutions play a core role in identifying those incidents that most warrant further investigation and response.

Advanced, targeted threats can typically remain undetected for 200 days or more, while cybercriminals silently gather valuable information and / or impact vital business processes.

According to Kaspersky Lab statistics, even a single targeted attack incident can cost an enterprise more than $2.5 million,compared to a starting point of $80k for the average small to medium business.

- Left unchecked, a targeted attack is likely to cause severe damage to the business, including:
- Substantial financial losses
- Loss of critical data
- Remote control by the attacker of apparently 'authorized' business processes
- Stealth manipulation of data

**In a survey of Enterprise organizations conducted by Kaspersky Lab in 2015, 1 in 4 organizations (23%) confirmed that they had already been subjected to at least one targeted attack.**

## The Solution: Kaspersky Anti Targeted Attack

The Kaspersky Anti Targeted Attack Platform is part of an adaptive, integrated approach to enterprise security. Monitoring network traffic, combined with object sandboxing and endpoint behavior analysis, delivers detailed insights into precisely what's happening right across a business's IT infrastructure. This adaptive security approach protects businesses against the most sophisticated threats, targeted attacks, new malware – including ransomware and crimeware – and of course APTs.

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

Our industry-leading Global Security Intelligence is one reason why we can deliver this superior detection performance. No other security vendor can match the quality and breadth of our security intelligence, enabling us to protect businesses from an ever-widening range of threats.

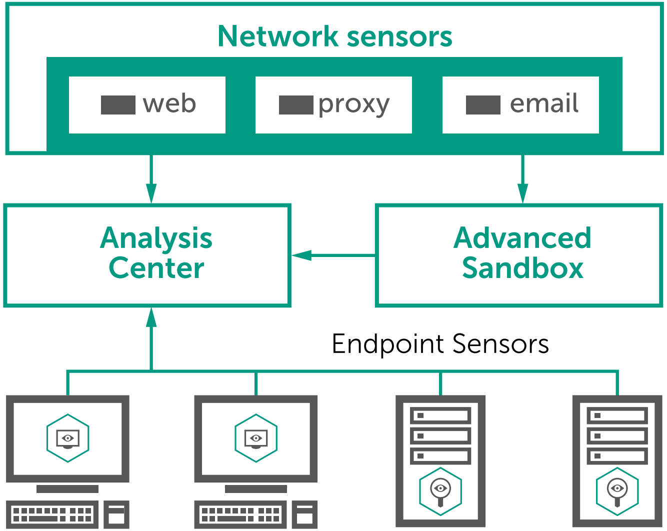
But Global Security Intelligence is just the beginning – the Kaspersky Anti Targeted Attack Platform also incorporates powerful detection and analysis technologies, including:

- **Multi-layered sensor architecture** – for 'all-round' visibility. Through a combination of Network Sensors, Web and Email Sensors and Endpoint Sensors, the Kaspersky Anti Targeted Attack Platform provides advanced detection capabilities at every level of your corporate IT infrastructure.

- **Advanced Sandbox** – to assess new threats. The result of over 10 years of continuous development, our Advanced Sandbox offers an isolated, virtualized environment, where suspicious objects can be safely executed and their behavior observed.

- **Powerful analysis engines** – for rapid verdicts and fewer false positives. Our Targeted Attack Analyzer assesses data from network and endpoint sensors, rapidly generating threat detection verdicts for your security team.

Kaspersky Anti Targeted Attack Platform



# Kaspersky Private Security Network

## The  comprehensive threat intelligence database for isolated networks and stringent data-sharing restrictions

It takes up to four hours for standard security solutions to receive the information needed to detect and block the almost 310,000 new malicious programs discovered by Kaspersky Lab every day. Threat intelligence sharing via Kaspersky Private Security Network provides this information in 30-40 seconds.

Cybercrime is growing not just in volume, but in sophistication, too: while 70% of threats faced by enterprises every day are known, 30% are unknown, advanced threats that traditional, signature-based security alone can't tackle.

Kaspersky Security Network delivers Kaspersky Lab's security intelligence to every system connected to the internet, ensuring the quickest reaction times and lowest false positive rates, and maintaining the highest level of protection – even against unknown, advanced threats.

While all information processed by Kaspersky Security Network is completely anonymized and disassociated from source, we recognize that some enterprises require absolute data lock-down. Traditionally this has meant that such enterprises haven't been able to avail themselves of cloud-based security solutions.

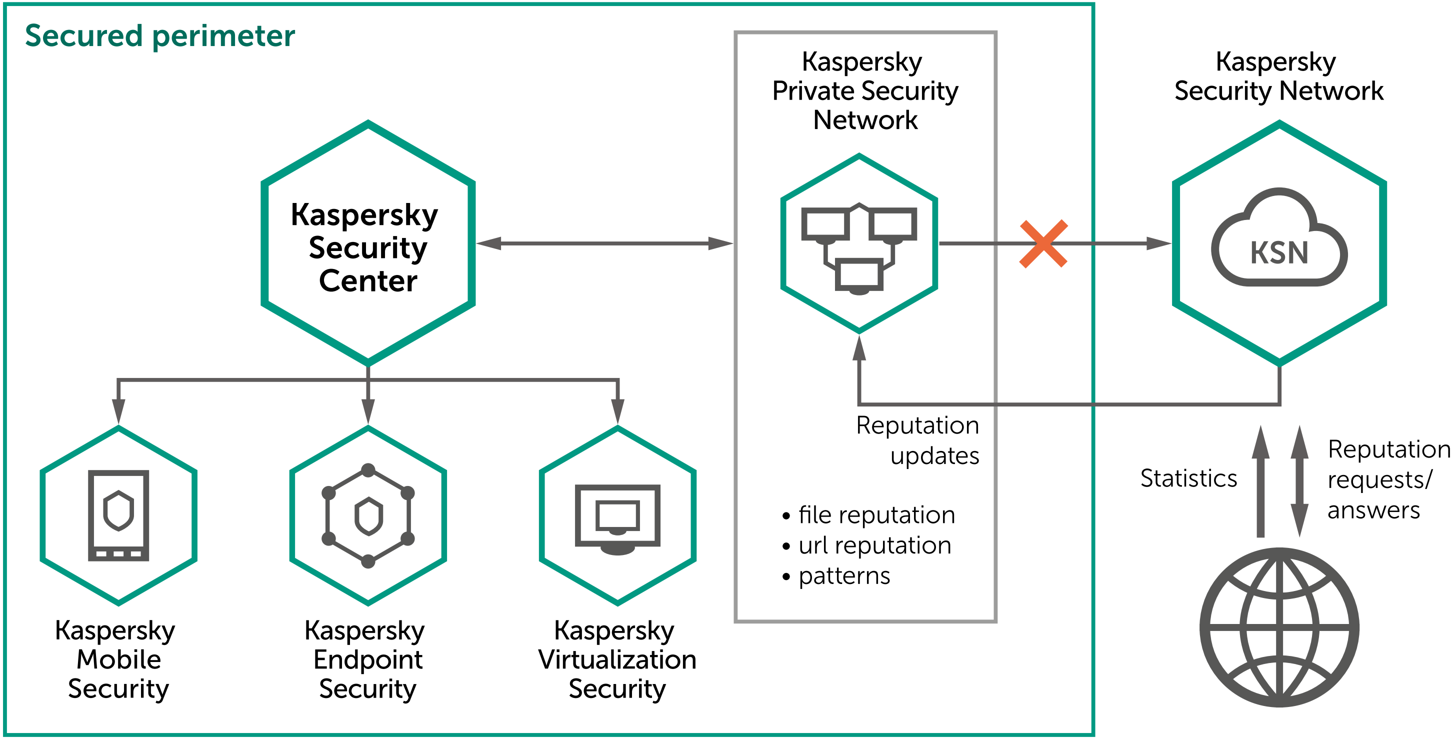
### The Solution: Kaspersky Private Security Network

For customers with these specialized needs, Kaspersky Lab has developed Kaspersky Private Security Network, allowing enterprises to take advantage of most of the benefits of cloud-assisted security without releasing any data whatsoever outside their 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 Private Security Network:

- 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 3rd party threat source verdicts (file hashes)
- Reduces false positives
- Complies with strict regulatory, security and privacy standards.

Kaspersky Private Security Network applies our unique threat intelligence and information not just to Kaspersky Lab security solutions but to other solutions the enterprise may be running: including SIEM, risk management and compliance. All these capabilities can be integrated through SDK, direct calls and the API of Kaspersky Private Security Network, delivering a unique insight into your organization's security and threat readiness.


Secured perimeter
Kaspersky Security Center
Kaspersky Private Security Network
Kaspersky Security Network
KSN
Reputation updates
• file reputation
• url reputation
• patterns
Statistics
Reputation requests/ answers
Kaspersky Mobile Security
Kaspersky Endpoint Security
Kaspersky Virtualization Security

# Endpoint Security

## The leading multi-layered endpoint protection platform, based on true 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.

With the growth of digital business, enterprise IT environments have become ever more complex. Meanwhile, cybercriminals are adopting increasingly sophisticated methods of attack, creating new ways to infiltrate corporate infrastructure.

The majority of enterprise cyber-attacks are initiated through the endpoint. Without effective Global Threat Intelligence and Machine Learning, traditional security technologies can't protect from highly sophisticated threats.

We deliver zero-second protection against unknown and advanced threats and targeted attacks through our Advanced Detection technologies, drawing on a combination of machine learning and threat intelligence.

Protection against advanced threats is further enhanced by powerful control and data protection tools including Integrated Encryption, Automated Patching and Mobile Endpoint Protection – all managed together through Kaspersky Security Center.

All components are developed in-house and form a common platform which can be easily adapted to meet the changing needs of the organization.

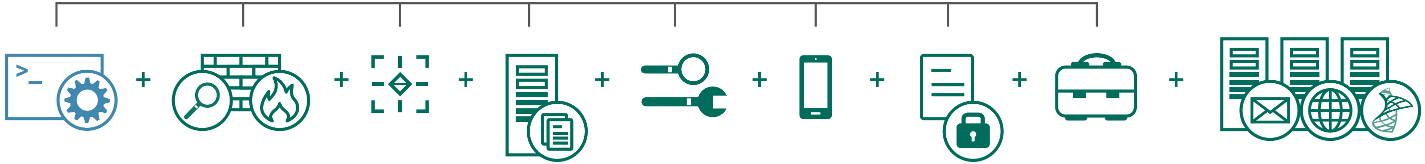
### The Solution: Kaspersky Endpoint Security

Fully securing every endpoint against every form of advanced cyber-threat is critical. Traditional antivirus protection is nowhere near enough. Only through employing a cutting-edge security platform including machine learning for dynamic and static detection, while adopting a multi-layered approach, can you hope to fully protect every single endpoint within and beyond your perimeter.

Based on unequalled sources of real-time threat intelligence, our technologies continually evolve to protect your business from even the latest, most sophisticated threats, including zero-day exploits. By aligning your security strategy with the world leaders in advanced threat discovery, you are choosing to adopt best of breed endpoint protection, now and in future.

There is no better security posture for your organization.

## Kaspersky Endpoint Security



Centralized Security Management + Advanced Malware Protection using Machine Learning + Automatic Exploit Prevention + Server Protection + Web, Application and Device Controls + Enterprise Mobility Management + Data Encryption + Automated Patch Management + Protection for Collaboration Servers, Mail Servers and Internet Gateways

**Unprecedented proven protection for all forms of endpoint**
Our advanced protection technologies secure enterprise organizations and their IT infrastructures, however complex, including every endpoint, from physical and virtual desktops and servers to mobile devices.

**Behavior analysis using Machine Learning to protect your business**
Our solution uses Machine Learning based on both static and dynamic data technologies. This is how we protect you even from future threats.

**Powerful Global Threat Intelligence**
All our technologies are powered by our proven Global Threat Intelligence. We have made more APT discoveries than any other security vendor, so we have an unequalled understanding of the nature of modern threats, and can help you to better protect against them.

**Automatic real-time response**
At the instant a threat is detected, the system will automatically roll back any changes the malware has already instigated, as detected by our dynamic behavior monitoring engine.

**Continuous dynamic protection from zero-day threats and exploits**
Automatic Exploit Prevention has been developed to prevent cybercriminals from targeting application vulnerabilities on protected machines. Automated Patch Management adds a further layer of security.

**FIPS 140-2 Certified Data Protection**
Powerful, user-transparent encryption fully secures confidential and sensitive data on the move, on portable devices and at rest.

**Reliable protection against ransomware**
Keep your data safe, avoid funding cybercriminals through ransom payments and protect shared folders from advanced crypto-lockers with our anti-ransomware technologies.

**A lower TCO and a higher ROI through unified & centralized management**
Manage multiple platforms and all endpoint devices from the same console – increasing visibility and control with no additional investment in software, equipment or human resources.

# 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.

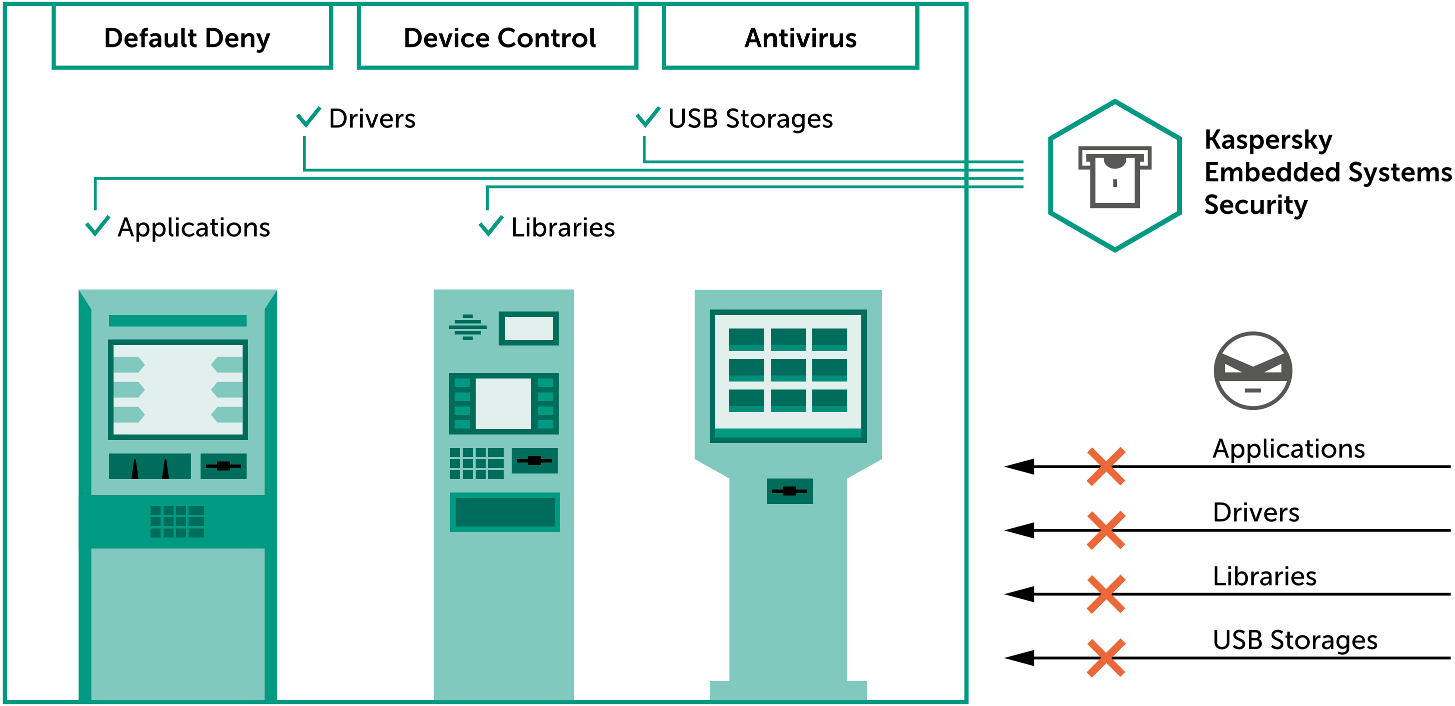
Kaspersky Embedded Systems Security offers a ‘Default Deny only’ operational mode, where system requirements start from 256Mb of RAM and 50Mb HDD space for Windows XP for low-end hardware systems.

There’s also an on-demand scan mode supplied by an optional Antivirus module, including a 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



# Cybersecurity Services

## Threat Intelligence, Security Training, Incident Response and Assessment from the world leader

60% of large enterprises plan to utilize threat intelligence services in their security strategy.

Sophisticated threats are constantly emerging, and cybercriminals are developing innovative techniques to outsmart established security technologies. Traditional security solutions such as antivirus, firewall and intrusion prevention systems alone are no longer enough for comprehensive protection – today, a new security approach based on threat intelligence and extensive expertise is required to fill this security gap.

By sharing our up-to-the-minute intelligence with our customers, Kaspersky Lab helps enterprises to guard against threats. Our broad range of intelligence services helps ensure your Security Operations Center (SOC) and/or IT security team is equipped to protect the business from the latest online threats.

### Cybersecurity Training

Cybersecurity awareness and education are critical requirements for enterprises faced with increasing volumes of constantly evolving threats.

Your in-house security specialists need to be skilled in the advanced security techniques that form a key component of effective enterprise threat management and mitigation strategies, while all employees should have a basic awareness of the dangers, and of how to work securely.

We offer a portfolio of Cybersecurity Awareness training, as well as a broad curriculum of training programs ranging from basic to expert level in digital forensics and malware analysis.

- **Cybersecurity Awareness** helps enterprises improve their employees' security skills – and, as a result, their corporate security.
- **Security Education for IT Security Professionals**, at all levels, improves the skills of your in-house security experts and minimizes the risk of incidents.

## Threat Intelligence

Does your SIEM system have adequate cyberthreat detection capabilities? Can you be sure that you'll be warned in good time about the most dangerous threats? Our portfolio of Threat Intelligence Services is designed to equip enterprises to manage these risks:

- **Threat data feeds:** enhance your SIEM solution and improve forensic capabilities using our up-to-the-minute cyberthreat data.
- **APT Intelligence Reporting** delivers exclusive, proactive access to descriptions of high-profile cyber-espionage campaigns, including Indicators of Compromise (IOCs).
- **Customer-specific Threat Intelligence Reporting** identifies externally available critical components of your network.

## Expert Services

Is your in-house expertise sufficient to resolve a cyber-incident? Is your IT infrastructure and are your specific applications fully secured against potential cyber-attack? Our Expert Services are designed to mitigate and resolve these risks:

- **Penetration Testing:** Learn how to identify the weakest points in your infrastructure and avoid damage caused by cyberattacks. Ensure compliance with government, industry and corporate standards (e.g. PCI DSS).
- **Application Security Assessment** Uncover vulnerabilities in applications, from large cloud-based solutions, ERP systems, online banking and other specific business apps to embedded and mobile apps on different platforms.
- **Digital Forensics and Malware Analysis:** Reconstruct a detailed picture of any incident using comprehensive reports, including incident remediation steps.

# Cybersecurity Awareness

## Building a safe corporate cyber-environment with gamified training

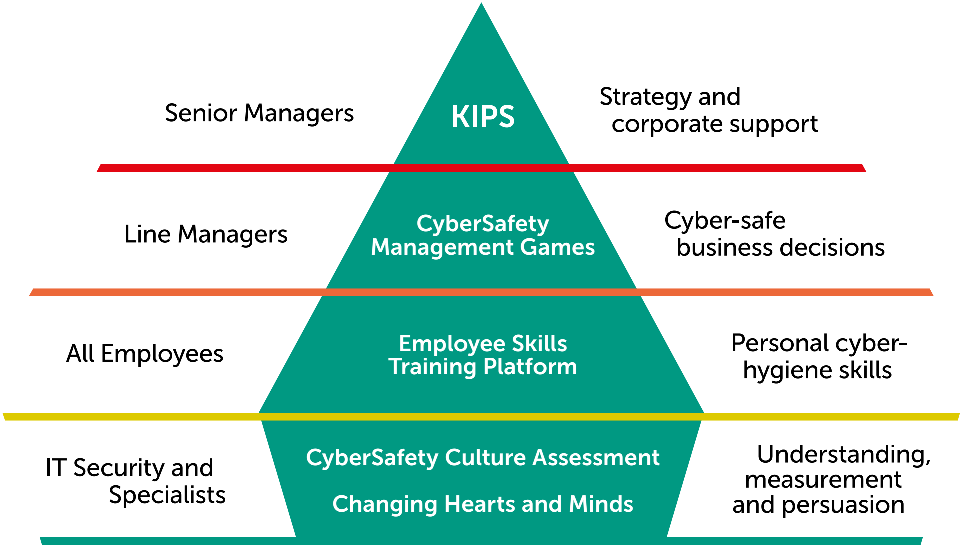
More than 80% of all cyber-incidents are caused by human error. On average, enterprises pay $861,000 to recover from a security breach, while SMBs spend $86,500. Phishing attacks alone cost up to $400 per employee per year.

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 has launched 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


Senior Managers
KIPS
Strategy and corporate support
Line Managers
CyberSafety Management Games
Cyber-safe business decisions
All Employees
Employee Skills Training Platform
Personal cyber-hygiene skills
IT Security and Specialists
CyberSafety Culture Assessment
Changing Hearts and Minds
Understanding, measurement and persuasion

## 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.

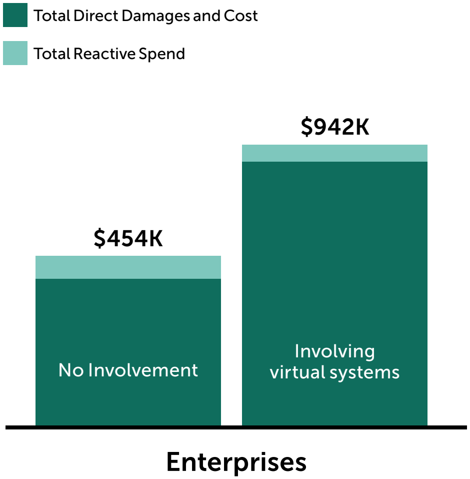
- Educational plans and best practices provided by Kaspersky Lab facilitate program implementation and help the customer's IT Security and T&D teams get the most out of Security Awareness initiatives.

# Cloud Security

## Borderless security engineered for your hybrid cloud

When it comes to virtual systems security, enterprises look for the right balance between protection and performance, as well as the most advanced security capabilities to keep business-critical processes safe.

On average, data breaches involving virtual systems are more than twice as costly as those involving physical machines.



Source: KasperskyLab Global Risks Survey 2015

As enterprises continue to roll out virtualized environments across more of their IT estate, there is an increasing need for security designed specifically for virtualization. But finding a solution which provides security capabilities both for your growing Virtual Desktop Infrastructure (VDI) and your virtual server environment, while retaining all the performance benefits of virtualization, is not easy. With all its advantages, virtualization also creates additional 'attack surfaces', presenting cybercriminals with even more opportunities to target very large businesses.

The solution securing your virtualized infrastructure should deliver uninterrupted protection, providing enhanced functionality while still preserving the efficiency of your virtual infrastructure.

The unique architecture of Kaspersky Lab's specialized solution provides efficient multi-layered virtual machine (VM) protection without sacrificing performance. The result is significantly higher consolidation ratios than with traditional anti-malware solutions. Scanning and update storms are now eliminated, together with windows of vulnerability or 'instant-on' gaps. With additional layers of protection combined with network attack blocking mechanisms, Kaspersky Lab's solution takes corporate virtualization platform security to a new level.

For a large Enterprise, the average cost of recovering from a virtual security breach is over US$940.000, twice as much as for a comparable incident involving only physical infrastructure.

While an attack on physical nodes leads to the temporary loss of access to business-critical information in 36% of incidents reported, this rises to 66% when the breach affects virtual servers and desktops.

## The Solution: Kaspersky Security For Virtualization

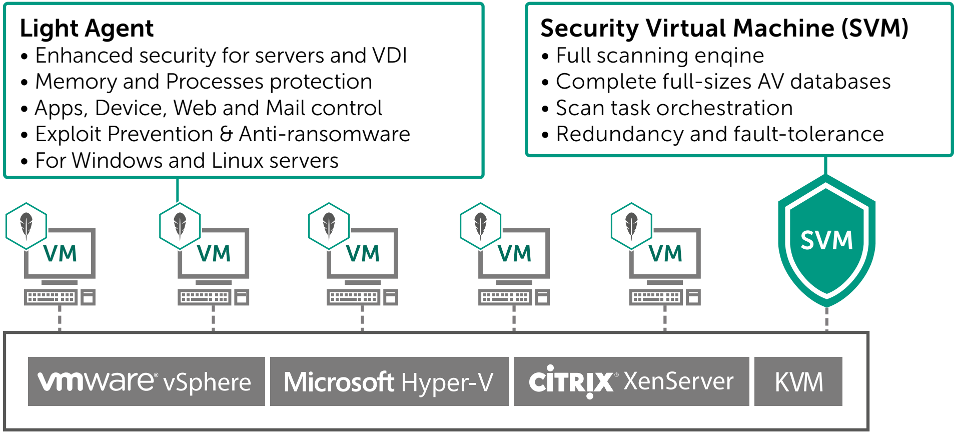
Kaspersky Lab offers two technologies which allow you to achieve that perfect balance of optimum security and preserved performance.

While our agentless solution operates in harness with core hypervisor technologies (such as VMware NSX), our light agent solution offers additional layers of protection to each VM.

To protect VMs, enterprises need only deploy a single Security Virtual Machine (SVM), to which file-level scan tasks can be offloaded. This SVM provides centralized anti-malware protection for all VMs on the host with no extra resource consumption. Built-in fault tolerance and redundancy gives your security solution the reliability you need for successful business operations.

Deploying a Light Agent on each VM means that multi-layered protection and feature-rich security controls can be added to the mix. Security for your VMs, whether agentless, light agent based or both, can be managed, together with your physical endpoints servers and your mobile devices, from  a single console.

## Kaspersky lab’s unique Light Agent technology



**Light Agent**
- Enhanced security for servers and VDI
- Memory and Processes protection
- Apps, Device, Web and Mail control
- Exploit Prevention & Anti-ransomware
- For Windows and Linux servers

**Security Virtual Machine (SVM)**
- Full scanning enqine
- Complete full-sizes AV databases
- Scan task orchestration
- Redundancy and fault-tolerance

Kaspersky Security for Virtualization is tightly integrated with most popular virtualization platforms — VMware vSphere with NSX, KVM, Microsoft Hyper-V and Citrix XenServer. Our security solution is optimized to safeguard platform performance by fully exploiting your hypervisor’s own core technologies – complementing and enhancing security in, for example, VMware Horizon and Citrix XenDesktop VDI.

Kaspersky Security for Virtualization can be licensed in two ways, depending on your business needs and the characteristics of your virtual infrastructure: by the number of virtual machines (desktops plus servers) or by the number of host server physical processor cores.

# Data Center Security

## Empowering your data center to detect and respond to the most advanced cyberthreats

Software-defined data centers need just as much protection as their traditional counterparts. Fail in this, and your virtualized systems and data storages become the weakest link in your data center security chain.

Large enterprises are processing ever-increasing levels of data. To keep pace with this escalation, organizations need to rethink not just how they store and access data, but how they preserve its safety and integrity. The larger the infrastructure, the greater the quantity of sensitive business data retained, and the more power and reliability demanded of the security solution protecting it.

Regardless of whether you operate your own data center or use the services of third party (through Infrastructure-as-a-Service or IaaS), your security solution should not only protect all critical data effectively and continuously: it should also preserve the performance of data center infrastructure.

Any data center offers numerous attack surfaces vulnerable to potential exploitation. And as your data center grows in size, it's bound to grow in complexity also, offering even more opportunities to the cybercriminal fraternity. Your security solution must step up to the challenge and scale effectively, which means fully integrating with your existing IT environment, or it will drag down data center performance levels and reduce overall operational efficiency as you grow.

## The Solution: Kaspersky Security For Data Centers

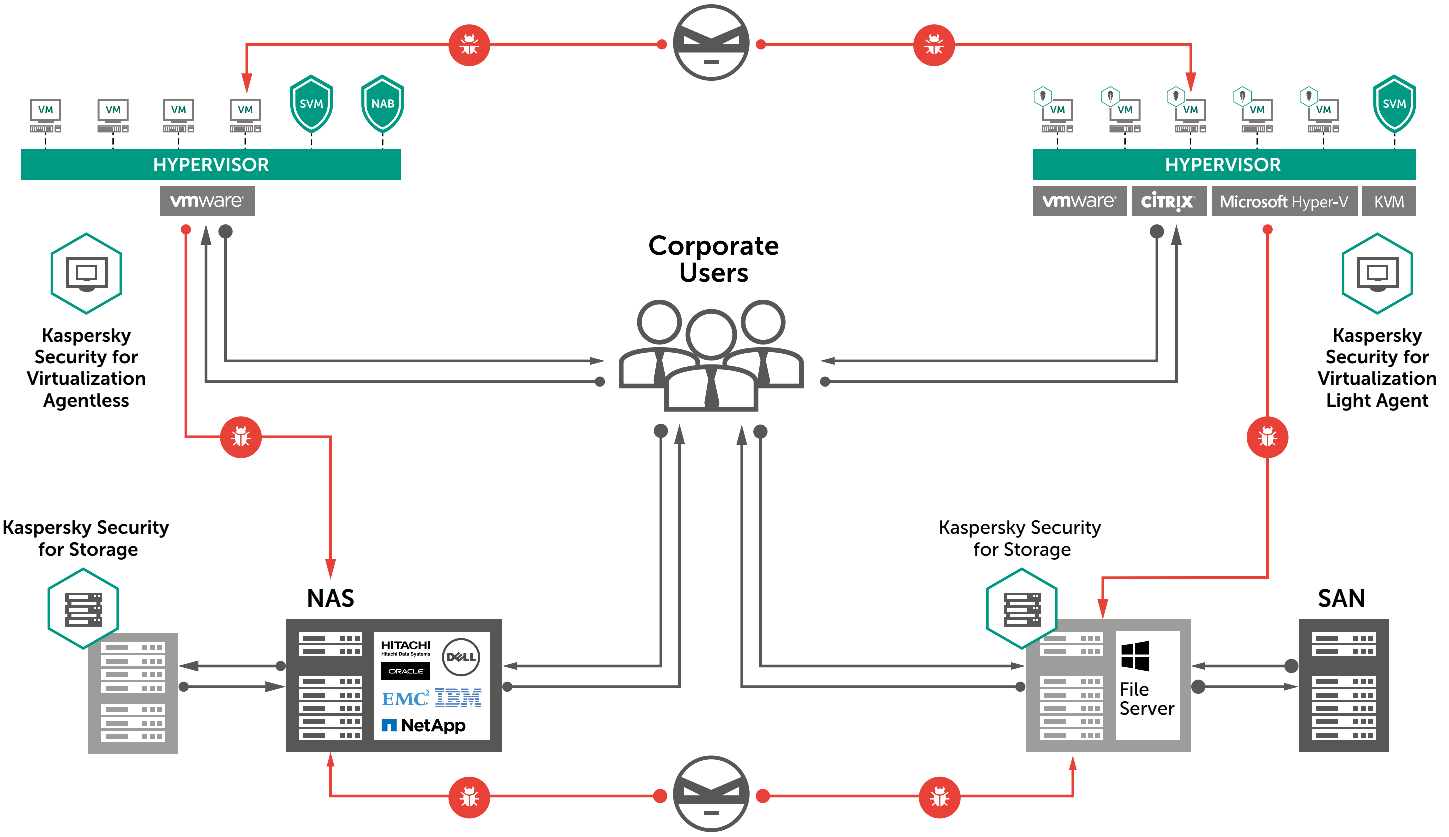
We offer solutions that focus on protecting the two essential areas of your data center: your virtual infrastructure and your data storage systems. Perfect for to multi-hypervisor and multiple storage systems environments, Kaspersky Lab's solution features:

- Security specifically built for major virtualization platforms, including VMware with NSX, Citrix, Microsoft and KVM.
- Security for network attached storage (NAS) systems including EMC, NetApp, DELL, IBM, Hitachi and Oracle.

Kaspersky Security for Data Centers is based on our award-winning security engine and operates as a single integrated platform, making it easy to manage and to integrate with different data center configurations. Centralized administration means your team can apply unified security policies across your entire data center, helping to reduce operating costs.

**This comprehensive solution:**

- Protects your data and systems against cyber-attack
- Provides effective tools for maintaining high levels of performance and business continuity
- Lets your team manage the security of all virtual and physical machines in the data center from a single centralized console


VM
VM
VM
VM
SVM
NAB
HYPERVISOR
vmware
Kaspersky Security for Virtualization Agentless
VM
VM
VM
VM
VM
SVM
HYPERVISOR
vmware
CITRIX
Microsoft Hyper-V
KVM
Kaspersky Security for Virtualization Light Agent
Corporate Users
Kaspersky Security for Storage
NAS
HITACHI
Hitachi Data Systems
DELL
ORACLE
EMC²
IBM
NetApp
Kaspersky Security for Storage
File Server
SAN

# Mobile Security

## Integrated security and management tools supporting your mobile strategy

Over a typical three-month period in 2016, we detected over 3.5 million malicious installation packages, over 83,000 ransomware Trojans, and over 27,000 banking Trojans, all targeting our customers' mobile devices.

Malicious software, websites and phishing attacks aimed at mobile devices continue to proliferate, while the capabilities of mobile devices 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) has expanded the range of devices operating on the corporate network , creating 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 personal use increase the chance of a company's IT security being breached. Once hackers access unsecured personal information on a mobile device, gaining access to 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.)

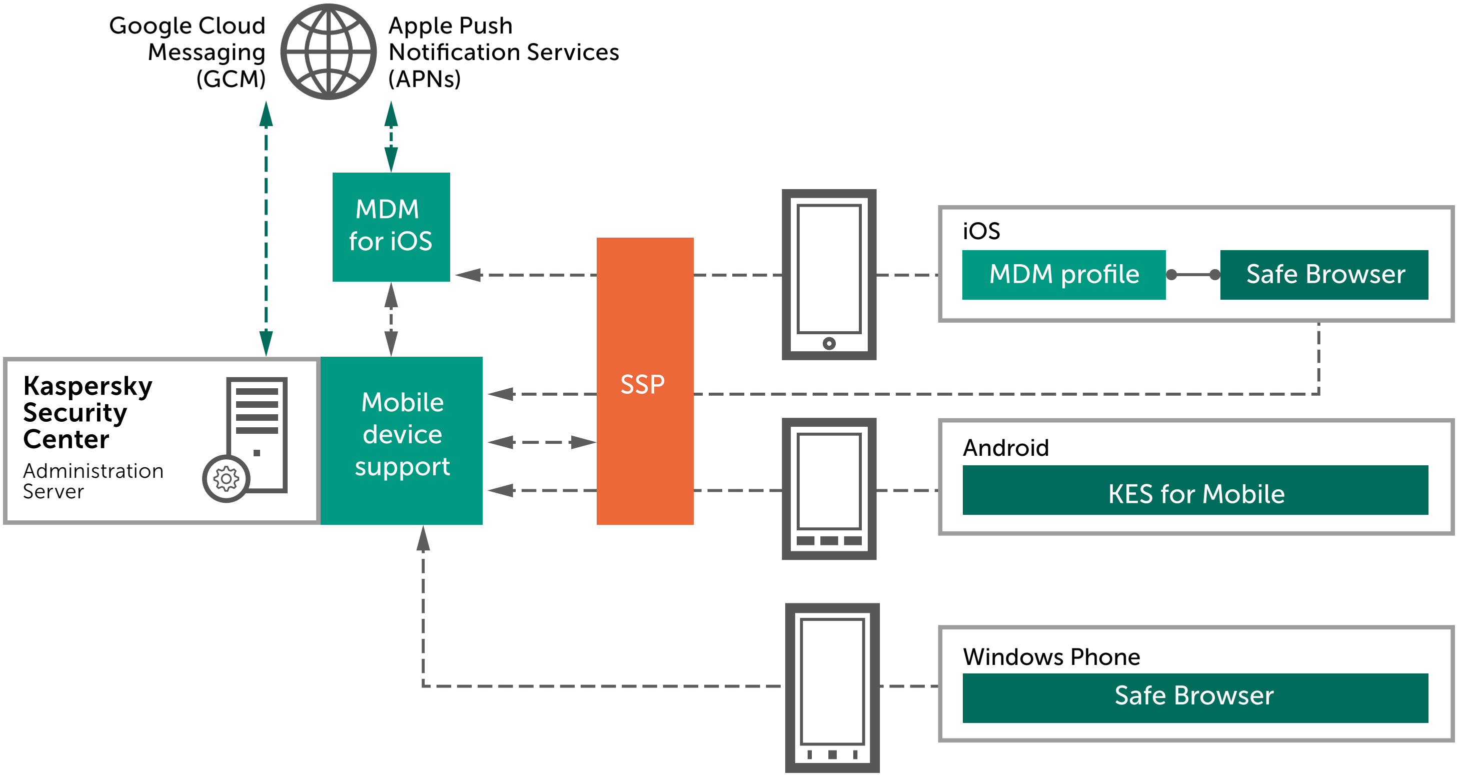
### The Solution: Kaspersky Security for Mobile

Kaspersky Security for Mobile solves these issues by providing multi-layered protection and a wide range of mobile device management (MDM) and mobile application management (MAM) functions. These significantly reduce the time needed for maintenance of mobile devices and provide secure mobile access to corporate systems.

- **Mobile Security:** Our mobile security technologies deliver multi-layered defense against the latest mobile threats plus a whole host of anti-theft features that can be operated remotely.
- **Mobile Device Management:** Integration with all major platforms allows device control and scanning over-the-air (OTA), which significantly improves the protection and management of devices based on Android, iOS and Windows phones.
- **Mobile Application Management:** Isolated containers for applications and the option to selectively clear the device's memory enables corporate and personal information stored on the employee's device to be ring-fenced.

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.

## Solution architecture



# DDoS Protection

## Total defense against all forms of DDoS attack to your infrastructure

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.

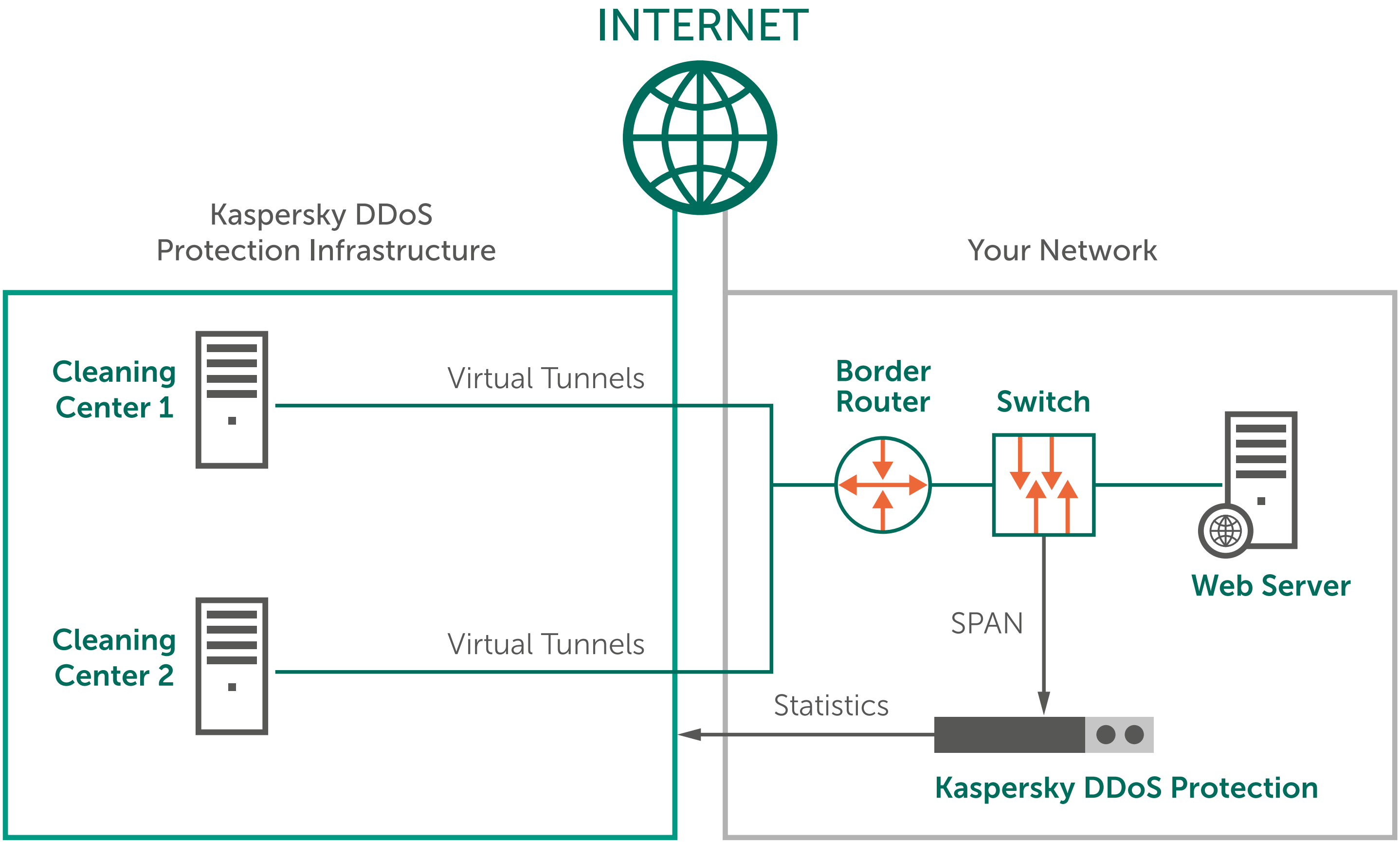
With the flexibility to address different configurations, we can ensure that we fully meet the needs of your business and its online assets.

## 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 Control



# 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. Recent research has found that cyber-attacks cause 35% of industrial network malfunction incidents.

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 technological processes by detecting and preventing actions (intentional or accidental) that could disrupt or halt vital services.

### The Solution: Kaspersky Industrial CyberSecurity

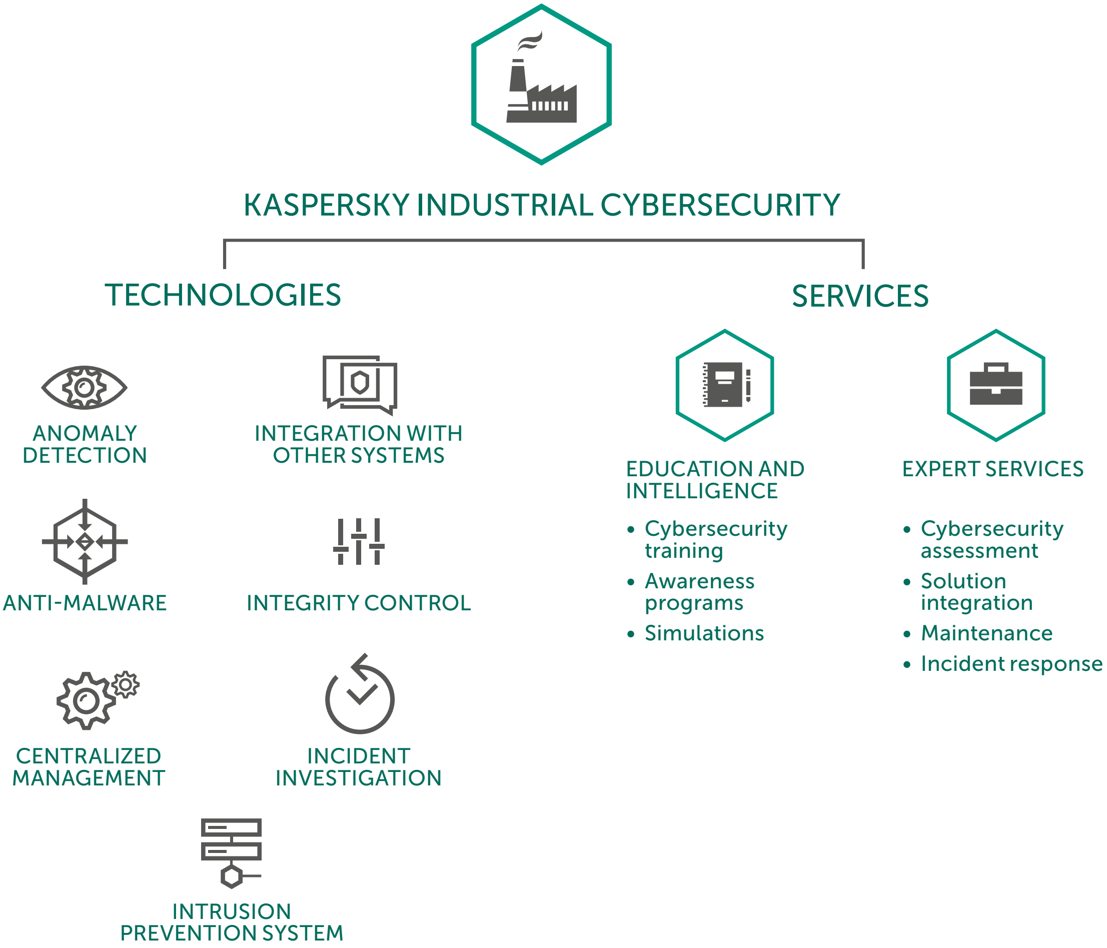
Kaspersky Industrial CyberSecurity is a portfolio of technologies and services designed to secure every industrial layer, including SCADA servers, HMI panels, engineering workstations, PLCs, network connections and people – without impacting on operational continuity and the consistency of the technological 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 technological process delays.



## KASPERSKY INDUSTRIAL CYBERSECURITY

### TECHNOLOGIES

ANOMALY DETECTION

INTEGRATION WITH OTHER SYSTEMS

ANTI-MALWARE

INTEGRITY CONTROL

CENTRALIZED MANAGEMENT

INCIDENT INVESTIGATION

INTRUSION PREVENTION SYSTEM

### SERVICES

EDUCATION AND INTELLIGENCE

- Cybersecurity training
- Awareness programs
- Simulations

EXPERT SERVICES

- Cybersecurity assessment
- Solution integration
- Maintenance
- Incident response

# Fraud Prevention

## Proactive detection of cross-channel fraud in Real Time

Nowadays digital banking is one of the key elements necessary for financial services business growth and customer acquisition. However, digital banking has already become attractive not only for customers, but also to fraudsters.

Cybercriminals have become increasingly adept at developing sophisticated tools that bypass traditional protection, provide a route into banking systems, gain access to customer accounts, and allow attackers to initiate and tamper with transactions.

Reacting to fraud attacks after they occur may have been acceptable a few years ago, but today this simply doesn't deliver the protection that banks and customers demand.

Deloitte believes that the financial services sector faces the greatest economic risk related to cybersecurity and will be forced to devote greater resources to enhancing the security, vigilance and resilience of their cybersecurity model.

## The Solution: Kaspersky Fraud Prevention

Kaspersky Fraud Prevention boosts a bank's existing security system, providing a new level of protection against fraud. The solution protects users' digital accounts, computers, mobile devices, and the bank's systems.  By protecting customer accounts and transactions, Kaspersky Fraud Prevention helps banks to increase customer loyalty.

Kaspersky Fraud Prevention belongs to a next generation of systems, allowing for the real-time analysis of behavior, devices and the user environment. Using machine learning, the solution detects advanced fraud scenarios and money laundering schemes. It also enables the bank's anti-fraud team to gather accurate information about each incident, including the details used to gain access to the account.

This information may reveal, for example, that a bank is not liable for a fraud incident, subsequently reducing costs for damages and compensation.

Kaspersky Fraud Prevention adds a vital defensive layer to a bank's existing fraud protection.

- **Kaspersky Fraud Prevention Clientless Malware Detection** provides server-side technologies that protect 100% of your customers regardless of what device or platform they are using. The system allows your bank to detect access by infected customers at the earliest possible point.

- **Kaspersky Fraud Prevention for Mobile** helps to protect users who access their bank accounts from mobile devices (Android, iOS and Windows Phone).

- **Kaspersky Fraud Prevention for Endpoints** runs on your customers' Windows PCs and Mac computers to provide powerful root-cause prevention against malware and internet-based attacks.

- **Kaspersky Fraud Prevention Cloud** is a product for fraud detection in on-line and mobile banking. Main functionality includes Risk Based Authentication, Behavior Analysis, Continuous Session Anomaly Detection and Passive Biometrics based on machine learning and statistic models.

This comprehensive fraud prevention solution:

- Adds multi-channel security for digital banking and payments
- Proactively detects advanced fraud schemes in real time before transaction processing
- Helps protect all kinds of users – regardless of device
- Delivers 'frictionless' security, for a seamless user experience
- Helps banks to boost customer retention, attract new customers, and increase the adoption and usage of high-margin online and mobile banking.
- Reduces costs by means of automation and machine learning.

# Premium Support And Professional Services

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

When a security incident results in IT system downtime, the consequences can affect all aspects of a company's operations. To avoid such eventualities, 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.

### Premium Support: MSA Enterprise

Kaspersky Lab's Maintenance Service Agreement (MSA) programs are for enterprises that depend on their IT infrastructure for business continuity and the ongoing delivery of mission-critical processes. MSA Enterprise is specially designed for large enterprises with complex environments requiring dedicated, personalized, proactive support around the clock.

### Professional Services

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, and working with your change control policy.

Implementation Service: Offers expert assistance and support to make Kaspersky Lab product deployment seamless and trouble-free, and to ensure you operate according to best practices, using optimal settings and making the best use of Kaspersky Lab's centralized management software.

- Health Check Service: Following a complete audit of your product settings and network environment,  our experts generate a comprehensive report with actionable recommendations on how to improve security and/or systems management efficiency.

Kaspersky Premium Support and Professional Services deliver access to the security experts who know the quickest, safest and most effective way to resolve your issues, as well as providing:

- Incident response SLAs
- Tailor-made patches
- High priority response to malware incidents
- Monitoring and reporting
- A single point of contact

# About Kaspersky Lab

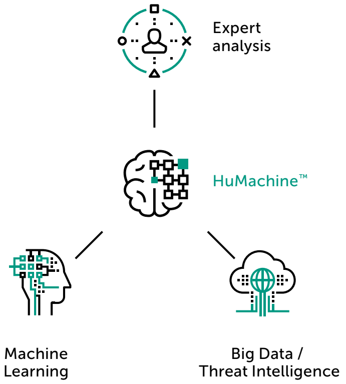
Kaspersky Lab is one of the world's fastest-growing cybersecurity companies and the largest one that is privately owned.

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. Firmly positioned as one of the top four leading vendors of security solutions for endpoint users, we continue to improve our market position. Our company is named a 'Leader' in endpoint protection by the 'big three' analyst agencies (Gartner, IDC and Forrester).

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**