KASPERSKY lab

ENTERPRISE SECURITY. POWERED BY INTELLIGENCE.

# Kaspersky Security Solutions for Enterprise 2016

# SECURING THE ENTERPRISE

Cyber-threats are becoming ever more sophisticated. Without effective solutions to mitigate them, enterprises are at the mercy of cyber-attacks that drain financial resources, disrupt business continuity, leave confidential data exposed and cause reputational damage. A successful attack is extremely damaging to any enterprise, regardless of the industry in which it operates.

## TAKING ENTERPRISE SECURITY SERIOUSLY

The costs of a security breach are substantial: In Kaspersky Lab's 2015 Global IT Security Risks Survey, we found that the average direct recovery cost to an enterprise is US$551,000 – in addition to indirect costs averaging US$69,000. 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 to 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: best intelligence combined with the best technologies delivers the best protection.

# ENDPOINT SECURITY

*Next-generation protection against known, unknown and advanced threats targeting your endpoints and users*

Vulnerabilities in popular programs such as Java, Internet Explorer and Adobe are responsible for some of the biggest security breaches. And it's not only zero-day vulnerabilities that are the problem: In 2015, more than 40% of breaches came from well-known vulnerabilities that were between two and four years old. A full 84% of all cyberattacks occur on the application layer.

Enterprise IT environments are complex. Hackers and cyber-criminals use increasingly sophisticated methods of attack against them. Without adequate measures to manage their IT security, enterprises expose themselves to unnecessary risk.

The majority of enterprise cyberattacks are initiated through the endpoint. If an enterprise can effectively secure every corporate endpoint, be it static, virtual or mobile, it has a strong foundation for an effective security strategy.

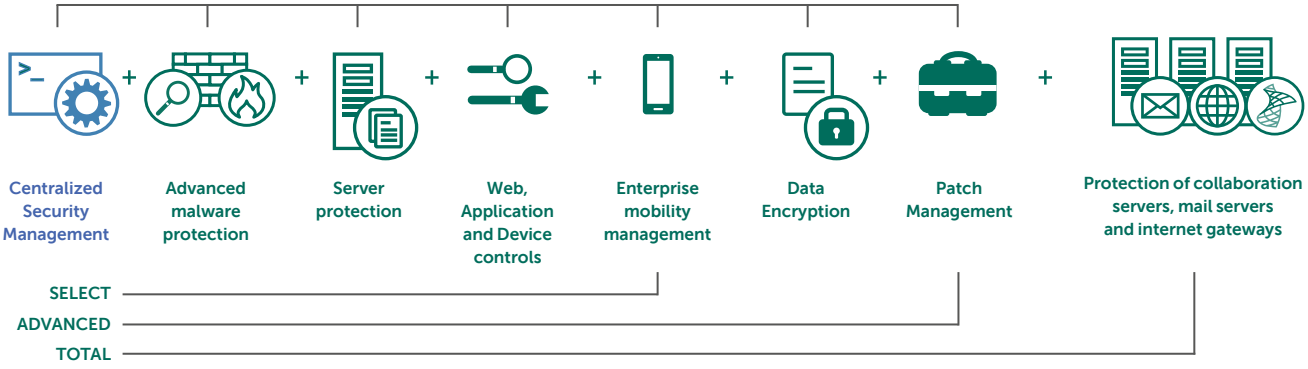
To deliver zero-second protection against unknown and advanced threats and the effective detection of targeted attacks, Kaspersky Lab technologies and threat intelligence continually evolve to protect your business from even the latest, most sophisticated threats and exploits.

This protection is further enhanced by powerful control and data protection tools: Application Control with Default Deny and System Hardening, integrated Full Disk and File Level Encryption with Secure Preboot, Intelligent applications and System Patching, and Centralized Security Management with Kaspersky Security Center.

**THE SOLUTION: KASPERSKY ENDPOINT SECURITY FOR BUSINESS**

Kaspersky Lab offers a range of security solutions with tailored tools and technologies that deliver a range of tools and capabilities with increasing functionality. All components are developed in-house and form a common platform which can be easily adapted to meet the changing needs of business.

## EDITIONS OF KASPERSKY ENDPOINT SECURITY FOR BUSINESS




### SELECT

Our SELECT edition includes tools to manage and protect endpoints, servers and mobile devices. There are also control tools inside: including device control and application control with Default Deny mode. These allow administrators to effectively apply policies, ensuring the security of critical IT infrastructure elements of any organization. This edition also includes server protection with anti-cryptor for shared folders functionality.

### ADVANCED

The ADVANCED edition includes all the tools from SELECT as well as data encryption, including Full Disk and File Level, and Removable Storages encryption. Vulnerability assessment tools and the automatic patching of operating systems and applications are also included the ADVANCED edition, as is application control for servers.

### TOTAL

Kaspersky TOTAL Security for Business includes additional technologies to protect mail servers, internet gateways and collaboration servers.

# VIRTUALIZATION SECURITY

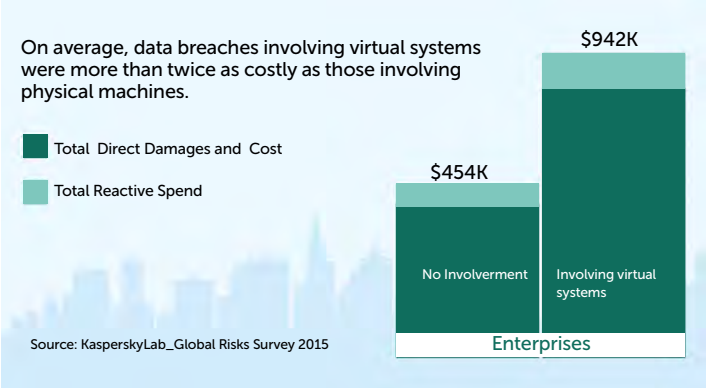
*Superior, flexible and efficient protection for virtual servers and VDI*

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.

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 the benefits it provides, virtualization also creates a number of 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 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

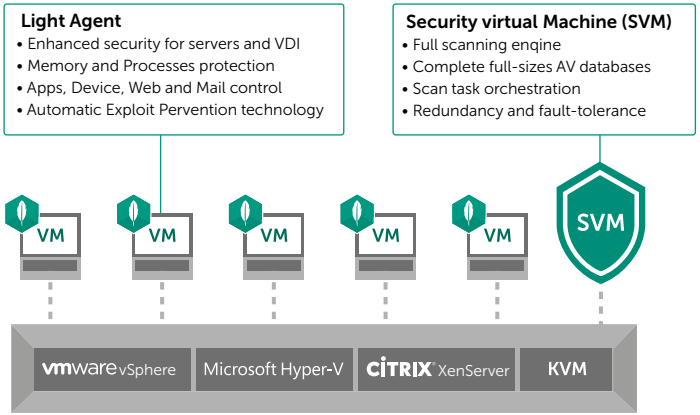
Kaspersky Lab offers two technologies which allow you to achieve that perfect balance of optimum security and preserved performance.

While our agentless solution operates in harness with core hypervisor technologies, 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




Kaspersky Security for Virtualization is tightly integrated with most popular virtualization platforms - VMware vSphere, 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.

# MOBILE SECURITY

*Advanced security, management and control for smartphones and tablets*

In Q3 2015, Kaspersky Lab Mobile Security solutions detected 323,374 new malicious mobile programs – a 1.1-fold increase on Q2 2015 and a 3.1-fold increase on Q1.

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 cyber-criminals. The rising use of personal devices for business purposes (BYOD) expands the range of devices 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 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 users' corporate systems and business data is simple.

### NO PLATFORM IS SAFE

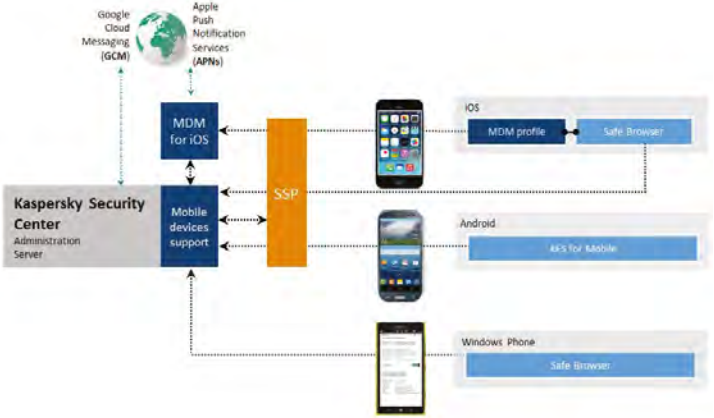
Cybercriminals use a variety of methods to gain unauthorized access to mobile devices, including infected applications, public Wi-Fi-networks with low security levels, phishing attacks and infected text messages. When a user inadvertently visits a malicious website – or even a legitimate website infected 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 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 the scan and control of devices 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 containerized.

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

# ANTI TARGETED ATTACK

*Specialized intelligence-led protection against 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 are everywhere.

Most enterprises have already made a major investment in intraditional 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.

Advanced, targeted threats can typically remain undetected for 200 days or more, while cybercriminals silently gather valuable information and / or impact vital business processes. Prevention-based security technologies may well detect individual incidents, but will generally fail to recognize that these are just a part of a far more dangerous and complex ongoing attack.

Left unchecked, a targeted attack is likely to cause severe damage to the business, including:

- High losses

  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.
- Competitive espionage
- Confidential data loss
- Remote control by the attacker of apparently 'authorized' business processes
- Stealth manipulation of financial and other critical data

**In a survey of Enterprise organizations conducted by Kaspersky Labin 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 PLATFORM

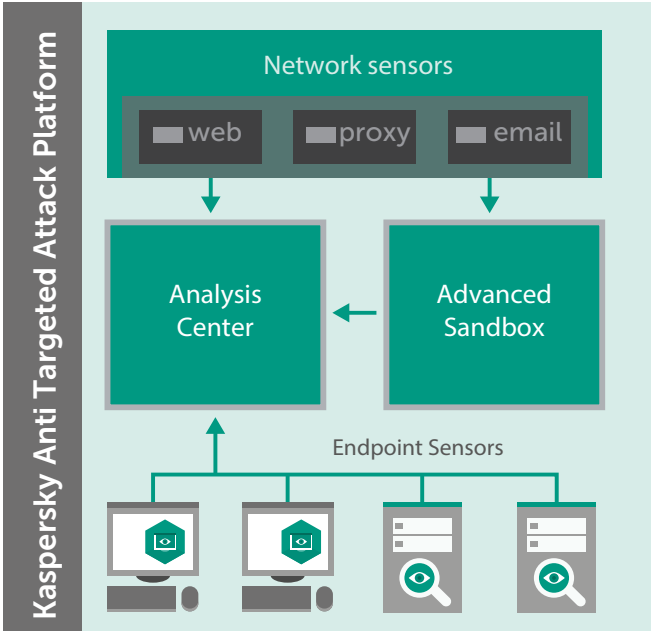
The Kaspersky Anti Targeted Attack Platform is part of an adaptive, integrated approach to enterprise security. Real time monitoring of network traffic, combined with object sandboxing and endpoint behavior analysis, delivers detailed insights into precisely what's happening right across a business's 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 threats landscape – the Kaspersky Anti Targeted Attack Platform delivers the 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 PRIVATE SECURITY NETWORK


*All the benefits of cloud-based threat intelligence within your perimeter*

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 on its own cannot tackle.

Kaspersky Security Network delivers Kaspersky Lab's security intelligence to every system connected to the Internet, ensuring the quickest reaction times, 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 enterprises haven't been able to avail themselves of cloud-based security solutions.

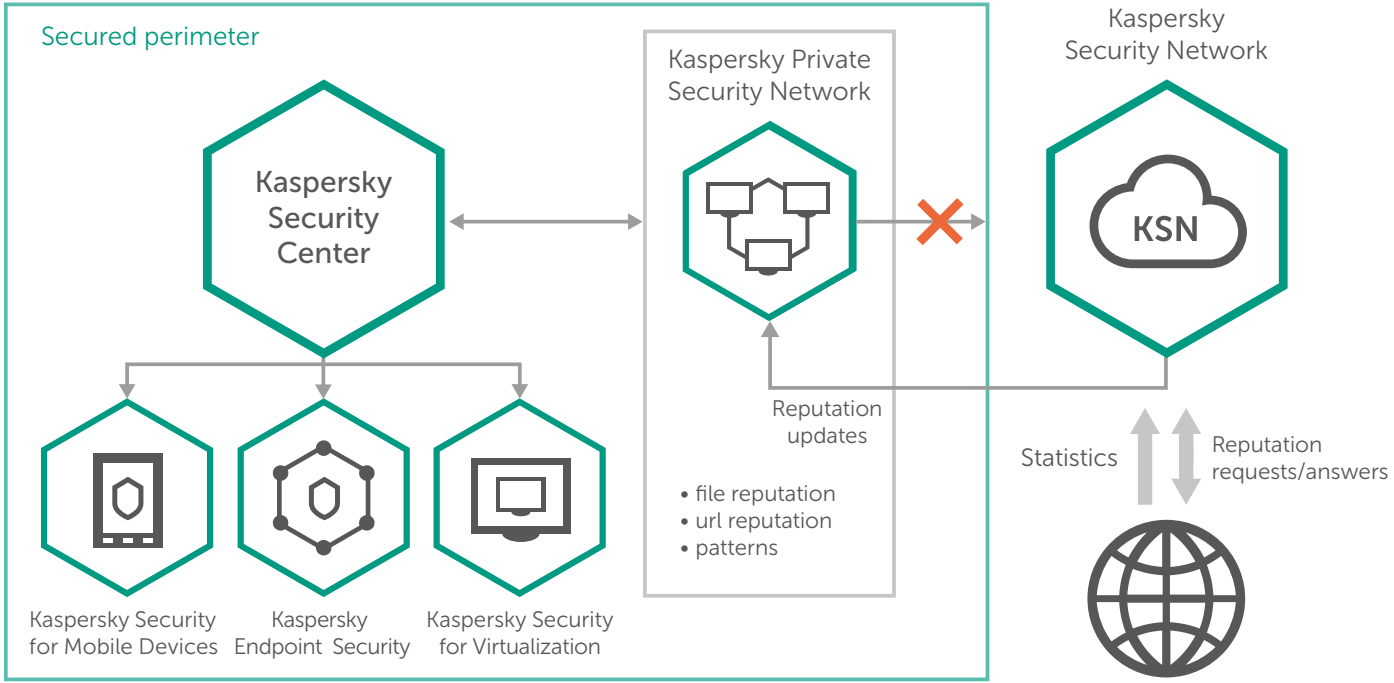
## THE SOLUTION: KASPERSKY PRIVATE SECURITY NETWORK

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:

- Identifies the source of malware and prevents it from spreading
- Identifies and differentiates between targeted attacks and more general threats
- Minimizes damage caused by cybersecurity incidents
- Assesses incident investigation and remediation requirements
- Reduces false positives
- Complies with strict regulatory, security and privacy standards.

Kaspersky Private Security Network can become a source of unique threat intelligence and information for other solutions the enterprise may be running: Security Operations Center (SOC), SIEM, governance, risk management and compliance, forensics and remediation processes. All these capabilities can be integrated with Kaspersky Private Security Network data feeds, delivering a unique insight into your organization's security and threat readiness.



# SECURITY FOR DATA CENTERS

*Specially designed security technologies for critical areas of data center infrastructure*

Business continuity remains a critical factor for enterprises choosing a security solution.

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 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

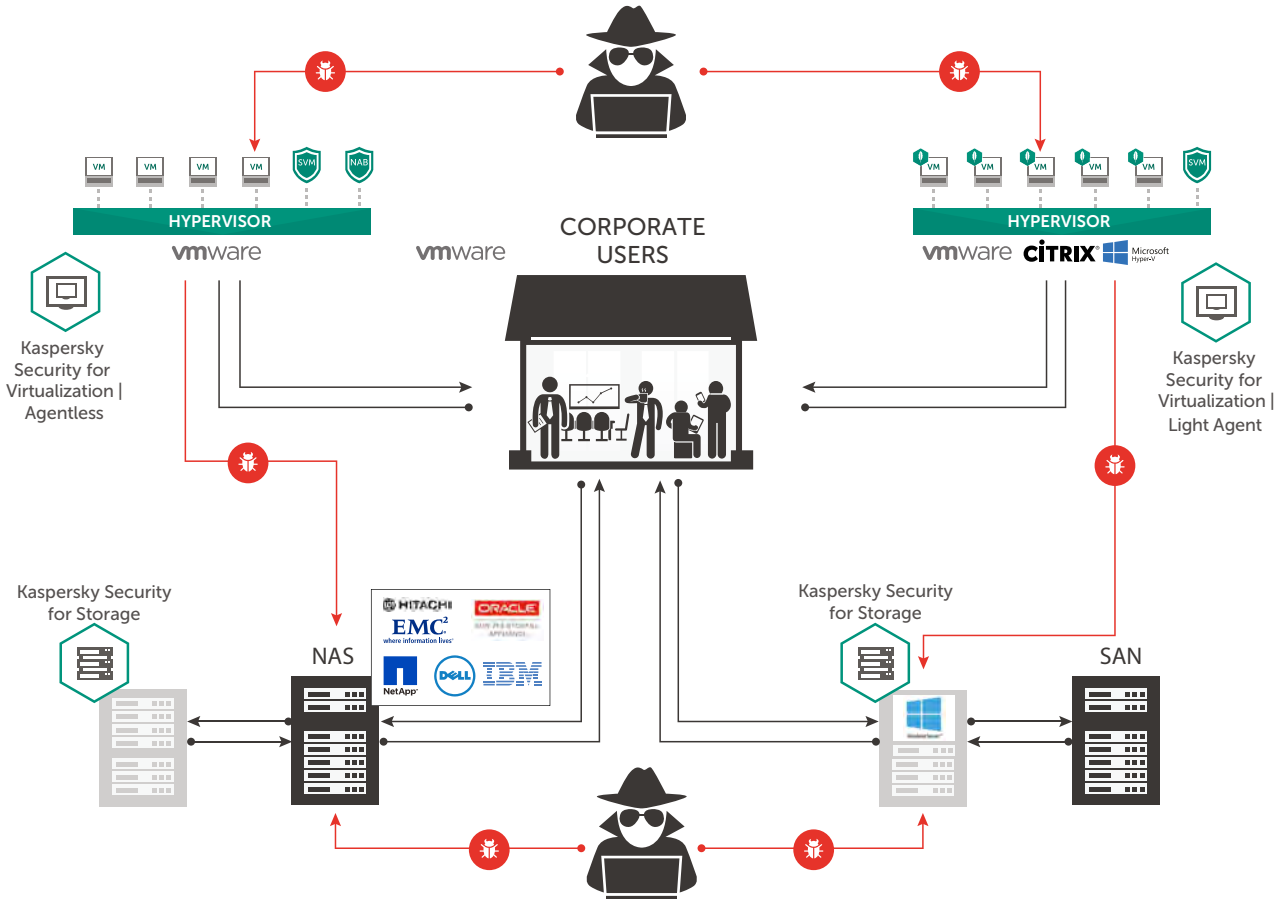
We offer solutions that focus on protecting the two essential areas of you data center: your virtual infrastructure and your data storage systems. Ideally suited to multi-hypervisor and multiple storage systems environments, Kaspersky Lab's solution features:

- Security specifically built for major virtualization platforms, including VMware, 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 integrate with different data center configurations, and to manage. 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


HYPERVISOR
vmware
vmware
CORPORATE USERS
HYPERVISOR
vmware CITRIX Microsoft Hyper-V
Kaspersky Security for Virtualization | Agentless
Kaspersky Security for Virtualization | Light Agent
Kaspersky Security for Storage
NAS
Kaspersky Security for Storage
SAN

# SECURITY INTELLIGENCE SERVICES

*World-leading threat intelligence, expert services and security training*

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 anti-virus, firewall and intrusion prevention systems alone are no longer enough for comprehensive protection – today, a new security approach based on human reaction is required to fill this security gap.

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

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 a business's Security Operations Center (SOC) and/or IT security team is equipped to protect the business from the latest online threats.

## CYBERSECURITY TRAINING

Security employees 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 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 knowledge – and their company security as a result.
- **Security Education for IT Security Professionals**, 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 forensics capabilities using our up-to-the-minute cyberthreat data feeds.
- **APT Intelligence Reporting** delivers exclusive, proactive access to descriptions of high-profile cyber-espionage campaigns, including Indicator of Compromise (IOCs).
- **Customer-specific Threat Intelligence reporting** identifies externally available critical components of your network.

## EXPERT SERVICES

Is your in-house expertise enough to resolve a cyber incident? Is your IT infrastructure or are your specific applications fully secured against potential cyberattacks? 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. Comply with government, industry and corporate standards (e.g. PCI DSS).
- **Application Security Assessment** uncovers 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.

# PROTECTION AGAINST DDOS ATTACKS

*Total defense against all types of DDoS attacks*

A single DDoS attack can cost a company between US$52,000 and US$444,000, depending on the size of the business. The cost of organizing a DDoS attack? Around US$200...

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 types of attacks calls for more rigorous protection.

Unlike virus 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

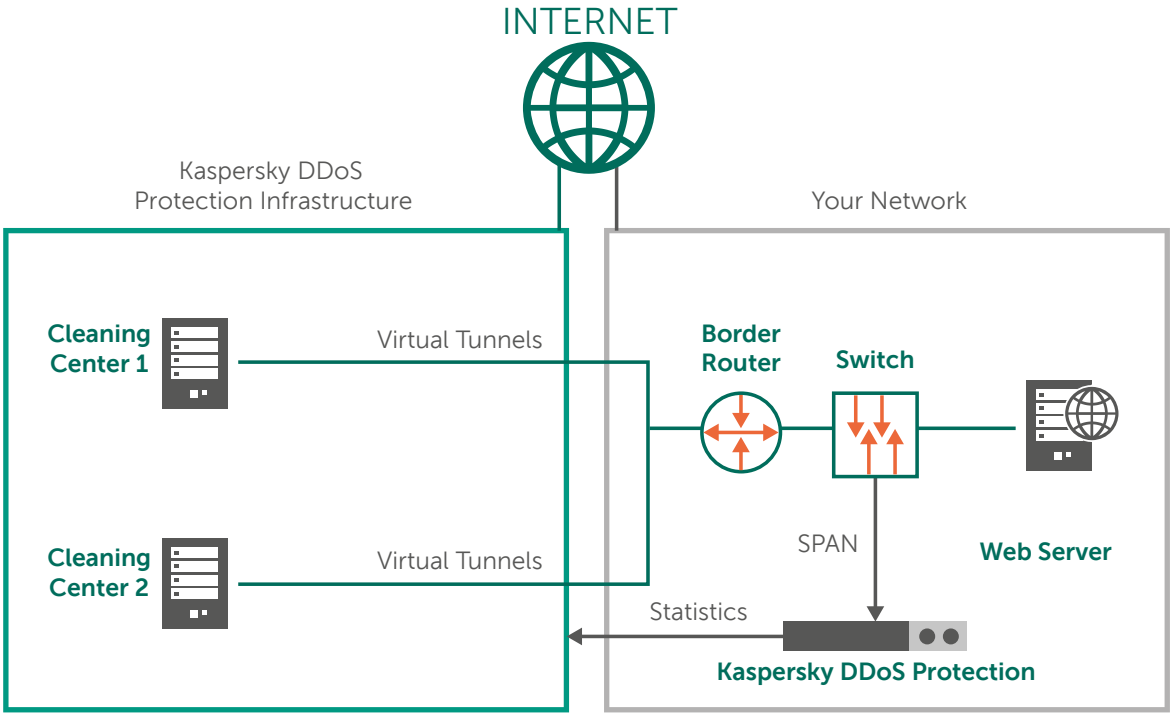
Kaspersky DDoS Protection delivers a total, integrated DDoS attack protection and mitigation solution that takes care of every stage necessary to defend your business against all types of DDoS attack.

Kaspersky DDoS Protection starts with special sensor software that runs on client infrastructure to monitor network traffic. By continually building up statistical and behavioral analysis data, the sensor enhances its ability to detect even subtle anomalies that may signal the start of a DDoS attack. In the event of an attack, we at Kaspersky Lab alert the customer and offer the option of redirecting traffic to one of our Cleaning Centers for remediation. To protect customer privacy, none of our processes views the content of customer traffic – they only view metadata.

## KASPERSKY DDOS PROTECTION ARCHITECTURE

This total defense solution provides:

- Special software sensors, operating within the client's IT infrastructure
- A distributed network of traffic clearing centers
- Alerts about possible attacks
- Safety of traffic: the clearing center filters traffic only during an attack
- Detailed post-attack analysis and reporting on where and how the attack took place




KASPERSKY DDOS PROTECTION ARCHITECTURE

# FRAUD PREVENTION

*Reducing fraud risk for online and mobile financial transactions*

In Q1 of 2015 alone, Kaspersky Lab solutions blocked attempts to launch malware capable of stealing money via online banking on the computers of 929,082 users. This figure represents a 64.3% increase compared to the previous quarter.

Cyber-criminals 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 them 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 helps financial institutions to stop hackers from achieving their goal by actively preventing Account TakeOver, Transaction Tampering, and Identity Theft - eliminating the threat of fraud before it happens.

The solution 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 show, 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 User Assessment Service** protects digital banking accounts from Account TakeOver attempts from criminals trying to gain fraudulent access to your legitimate customer accounts.

This comprehensive fraud prevention solution:

- Adds multi-channel security for digital banking and payments
- Provides proactive, root-cause fraud prevention that allows your bank to react faster
- 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.

# EMBEDDED SYSTEMS SECURITY

*Powerful protection specifically designed for critical payment systems*

Embedded systems are a particular security concern as they tend to be geographically scattered, challenging to manage and rarely updated. Operating as they do with real money and credit card credentials, ATMs and Point of Sale devices are targets of choice for cybercriminals, so require the highest levels of focused, intelligent protection.

The Payment Card Industry Data Security Standard (PCI DSS) regulates many technical requirements and settings for credit card data based systems. However, security regulations for ATMs and Point of Sale devices appear to cover only antivirus based security. A purely antivirus approach is of limited effectiveness against current ATM/POS threats, as has been amply demonstrated in recent attacks. Now is the time to apply approaches like Device Control and Default Deny, already well-proven technologies in other security contexts, to your critical embedded systems. Most ATMs still run on the Windows XP OS family even though, after 12 years, support for Windows XP Embedded ended on January 12, 2016 and for Windows Embedded for Point of Service on April 12, 2016. There will be no further security updates or technical support for the Windows XP operating system.

The overall replacement of ATM and POS systems software is a long, expensive, and painful process. Besides which, replacing software often means replacing still-functional, but obsolete, hardware as well.

**THE SOLUTION: KASPERSKY EMBEDDED SYSTEMS SECURITY**

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

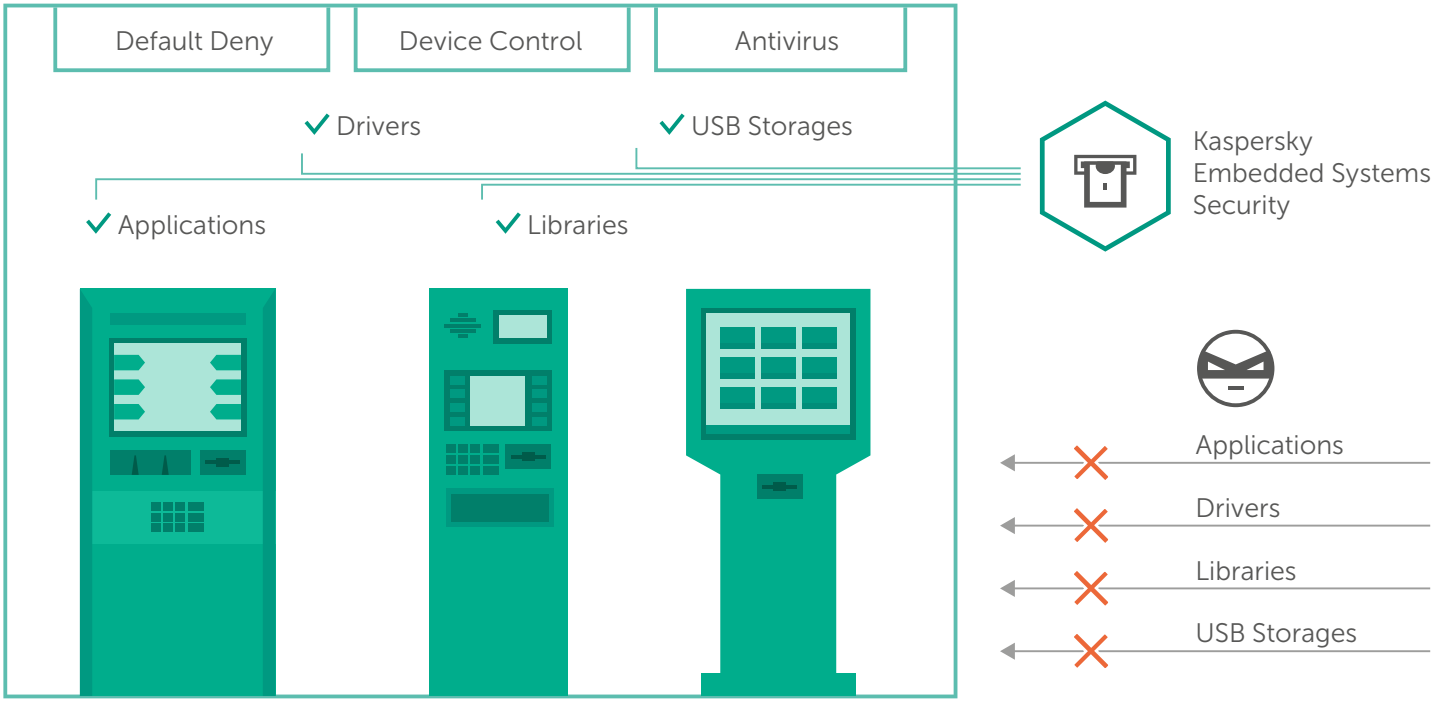
Default Deny for Application, Drivers and Libraries, boosted by Device Control functionality, is the only approach which can ensure the safety of obsolete critical systems still in use.

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 is also an on-demand scan mode supplied by an optional Antivirus module. This module is powered by the Kaspersky Security Network, with patch management facilities as 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

Kaspersky Embedded Systems Security mitigates security risks for embedded systems. The solution has been designed specifically for ATM and POS 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.



# 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 found that cyberattacks caused 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. All critical infrastructure needs the highest possible level of protection against a growing range of threats.

At the same time, industrial environments need an integrated solution that increases the availability of technological processes by detecting and preventing actions (intentional or accidental) that result in the disruption or halting of vital processes.

**THE SOLUTION: KASPERSKY INDUSTRIAL CYBERSECURITY**

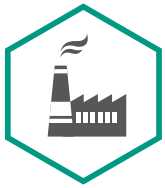
Kaspersky Industrial CyberSecurity is designed specifically with the unique needs of industrial organizations in mind, including a special focus on preserving the continuity of technological processes. Flexible, versatile settings mean the solution can be configured to meet the unique needs and requirements of individual industrial facilities.

The solution is designed to protect complex environments, built on various industrial control systems. The numerous possibilities of Kaspersky Industrial CyberSecurity allow organizations to configure a solution in strict accordance with the requirements of their specific industrial control system environment. Optimal configuration for the security technologies and services will be selected after a full infrastructure audit is 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 CERTS and regulators has enabled us to take a leadership role in addressing the unique requirements of industrial cybersecurity.

This highly specialized solution:

- Provides holistic cybersecurity 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

- VULNERABILITY MANAGEMENT
- ANTI-MALWARE
- CENTRALIZED MANAGEMENT
- INTRUSION PREVENTION SYSTEM
- INTEGRATION WITH OTHER SYSTEMS
- INTEGRITY CONTROL
- INCIDENT INVESTIGATION

### SERVICES

**EDUCATION AND INTELLIGENCE**

- CYBERSECURITY TRAINING
- INTELLIGANCE REPORTING
- SIMULATIONS

**EXPERT SERVICES**

- CYBERSECURITY ASSESSMENT
- SOLUTION INTEGRATION
- MAINTENANCE
- INCIDENT RESPONSE

# TARGETED SECURITY SOLUTIONS

*A cost-effective way to put Kaspersky Lab technologies precisely where you need them*

One-size-fits-all solutions can't meet the specific requirements of different devices – all devices within the corporate network need reliable, specialized protection. Kaspersky Lab's range of targeted security solutions ensures the security of individual network components – file and mail servers, internet gateways, collaboration servers.

## SECURITY FOR MAIL SERVER

Kaspersky Security for Mail Server protects mail traffic against spam, phishing links and malware. It supports common email platforms such as Microsoft Exchange, Linux Mail Server and IBM Domino. In addition, a Data Loss Prevention (DLP) module to control the spread of confidential information has been implemented for the Microsoft Exchange email platform.

## SECURITY FOR FILE SERVER

Kaspersky Security for File Server is an efficient, reliable and scalable solution for the protection of general-access file storage, with no noticeable effect on system performance. The solution provides protection against malware for servers based on Linux and Windows.

## SECURITY FOR INTERNET GATEWAY

Kaspersky Security for Internet Gateway checks HTTP and FTP traffic and provides comprehensive protection for your perimeter against malware and dangerous programs by blocking the latest current and potential threats.

## SECURITY FOR COLLABORATION

Kaspersky Security for Collaboration provides the maximum level of security for the entire SharePoint environment and its users. The solution combines effective technologies to protect against malicious attacks and confidential data leaks with ease of management and use.

# 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 an eventuality, Kaspersky Lab offers a choice of premium support programs that treat your IT security issues as high priority at all times and help 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 that require 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.

- The 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, have optimal settings and make the best use of Kaspersky Lab's centralized management software.
- Health Check Service: Following a complete audit of a customer's 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:

- Incident response SLAs
- Tailor-made patches
- High priority response to malware incidents
- Monitoring and reporting
- 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.

KASPERSKY lab