KASPERSKY lab

KASPERSKY SECURITY FOR BUSINESS PORTFOLIO 2015

‘THE POWER TO PROTECT YOUR ORGANISATION’

Every business, regardless of size, is at risk from malware threats. Kaspersky Lab is in a unique position to see and discover many of these threats.

And the threat level is escalating. New malware targeting individuals and businesses like yours now exceeds 325,000 unique threats– every day.

At Kaspersky Lab, we are concerned about these threats and the risk they pose to your business — that's why we are advising organisations like yours to ensure that their IT security strategy meets three key criteria:

- **First,** you need access to superior threat intelligence. This is a deep understanding of what a threat looks like — how it is written and compiled. It's important that your security system is continuously fed by expert information and that your vendor scours malware hot zones around the globe to see what's coming next.

- **Secondly,** your security must include tools and techniques able to detect and eliminate known, unknown and advanced malware. At the same time, your security software should minimise the burden on your systems and maintain fast scanning times, so your business is not disrupted.

- **Thirdly,** because business IT environments have become increasingly complex, this technology needs to extend its reach across physical, mobile and virtual endpoints - seamlessly and efficiently through a single platform, with no software conflicts, multiple consoles or security gaps.

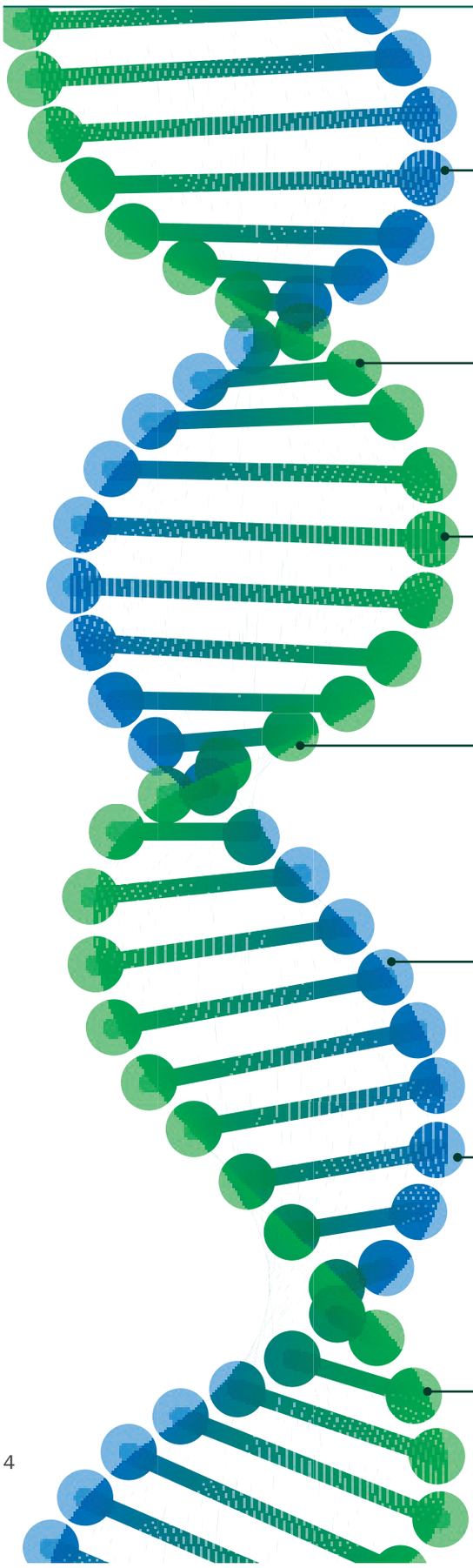
Only Kaspersky can offer the world-leading threat intelligence your company needs, and the technology to put it to work - all built into a unique comprehensive security platform.

Kaspersky solutions are designed with the flexibility to align with your business objectives. This means we are always on standby to protect your organisation against threats to your physical and virtual endpoints, mobile devices, mail systems, servers, gateways, and SharePoint portals.

Contact us or your IT reseller today about any of the products, solutions and services in this document. Let us show you how we can work together to protect your business from cyber-threats.

Join over 400 million users and over 270,000 corporate clients protected by Kaspersky Lab products and technologies.

SECURITY INTELLIGENCE IS IN OUR DNA



Expertise from the top down

Leading global threat intelligence, including the GREAT team

Respected among top security organisations

Technology driven

Recognised as leaders in independent tests

Leading the discovery of the most complicated threats

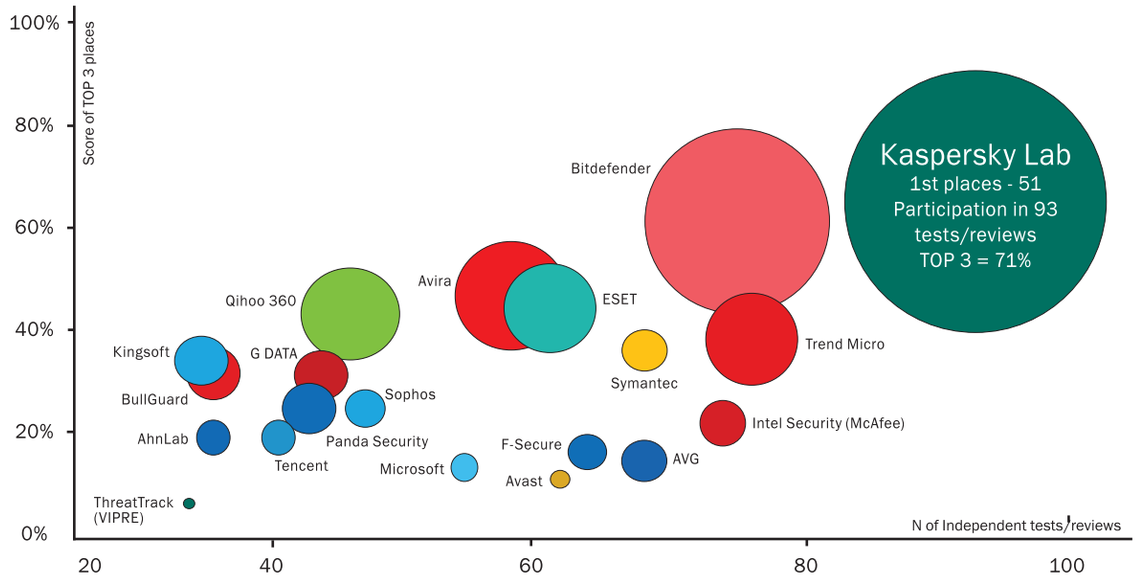
See and predict security incidents with Kaspersky Security Network

KASPERSKY LAB PROVIDES BEST IN THE INDUSTRY PROTECTION*

INDUSTRY-LEADING PROTECTION — AN INDEPENDENTLY PROVEN FACT

During 2014 Kaspersky Lab products participated in **93 independent tests and reviews**. Our products received **66 top-three finishes**, equal to a **71% TOP3 score**, and achieved **first place 51 times** — in well over half of all tests.

No product or solution by any of our leading competitors comes even close.



* Notes: According to summary results of independent tests in 2014 for corporate, consumer and mobile products. Summary includes tests conducted by the following independent test labs and magazines: Test labs: AV-Comparatives, AV-Test, Dennis Technology Labs, MRG Effitas, NSS Labs, PC Security Labs, VirusBulletin The size of the bubble reflects the number of 1st places achieved.

ABOUT OUR ANTI-MALWARE TECHNOLOGY

IT security software is only as effective as the security engine at its core. Patch management, MDM, encryption, device controls, anti-phishing — all these technologies and many more provide additional, valuable layers of security. Organisations should not compromise on security against known, unknown and advanced threats.

Kaspersky Lab's security engine is continuously powered and enhanced by our unmatched, dynamic threat intelligence. It's our single focus on security, combined with our threat intelligence and global experience, that sets us apart.

The industry-leading performance of the anti-malware engine built into the Kaspersky Endpoint Security for Business platform is proven through multiple, ongoing independent tests. Your own due diligence will confirm that Kaspersky security is unmatched.

Here's what makes anti-malware protection from Kaspersky Lab so powerful, and so much more effective than the rest.

KEY PRODUCT FEATURES

- **Known, Unknown and Advanced Threat Detection**
- **Behavioral Analysis & Heuristics**
- **Kaspersky Security Network for Cloud-Assisted Protection**
- **Active Disinfection**
- **Encryption and Ransomware Defense**
- **Automatic Exploit Prevention**
- **HIPS - (Network Attack Blocker) & Personal Firewall**
- **Simple, Transparent Management Console**

HIGHLIGHTS

A MULTI-LAYERED APPROACH

Kaspersky Lab's multi-layered approach is one reason why we are able to provide the most effective security in the marketplace today. Because Kaspersky Lab technologies are developed in-house, layer upon layer of powerful, streamlined protection is able to work seamlessly together with minimal impact on performance.

Each layer of protection addresses cyber-threats from a different perspective, allowing IT professionals to implement tightly interlocking technologies, providing security that is both deep and wide.

WORLD-LEADING THREAT INTELLIGENCE — YOUR ASSURANCE OF ONGOING PROTECTION

Kaspersky Lab's Global threat intelligence is world-renowned, and that expertise is fed directly back into our security solutions, designed to evolve constantly in an ever-transforming IT world.

FEATURES

HEURISTIC SECURITY — REDUCING THE LOAD ON YOUR SYSTEMS

Pattern-based malware identification provides improved detection — delivering smaller update files as well as increased security.

BEHAVIORAL ANALYSIS

Kaspersky anti-malware includes two specific components for program activity analysis:

- **Emulator** — reproduces and verifies the program's intended activities.
- **System Watcher** — tracks the activities of programs already running, discerning and analysing behavior patterns characteristic of malware.

CLOUD-ASSISTED MALWARE DETECTION — KASPERSKY SECURITY NETWORK (KSN)

A real-time response to new and unknown malware threats. A constant flow of new data about attempted malware attacks and suspicious behavior, provided by over 60 million volunteer Kaspersky Lab software users, is used to help create instant file verdicts, allowing all customers to benefit from real-time protection with lower 'false positives'.

AUTOMATIC EXPLOIT PREVENTION

Automatic Exploit Prevention specifically targets malware that exploits software vulnerabilities in popular applications by recognising typical or suspicious behavior patterns. The technology then halts the exploit in its tracks, and prevents any downloaded malicious code from executing.

ENCRYPTION RANSOMWARE COUNTER-MEASURES

System Watcher saves copies of important files in temporary storage, in case a suspicious process attempts to access them. Should ransomware attempt to encrypt the originals, these files can be restored in their unencrypted state.

ACTIVE DISINFECTION

Uses different techniques for 'curing' any detected infection — preventing file and process execution including autostart, destroying malware, and 'rolling back' stored files to their original condition.

HOST-BASED INTRUSION PREVENTION SYSTEM (HIPS) - NETWORK ATTACK BLOCKER AND PERSONAL FIREWALL

Some program activities are sufficiently high risk to make restriction advisable, even though they may not be confirmed as malicious. Kaspersky Labs' Host-based Intrusion Prevention System (HIPS) restricts activities within the system according to the application's trust level — with the help of an application-level Personal Firewall, which restricts network activity.

Monitors suspicious activity on your network — and lets you pre-define how your systems will respond if any suspicious behavior is detected.

FREQUENT UPDATES

Updates protecting against new malware threats are delivered to your security database through the fastest update cycle in the industry, together with continuously updating data about newly discovered malware from the Kaspersky Security Network (KSN) cloud.

SECURITY PRODUCTS, SOLUTIONS AND SERVICES FOR BUSINESS

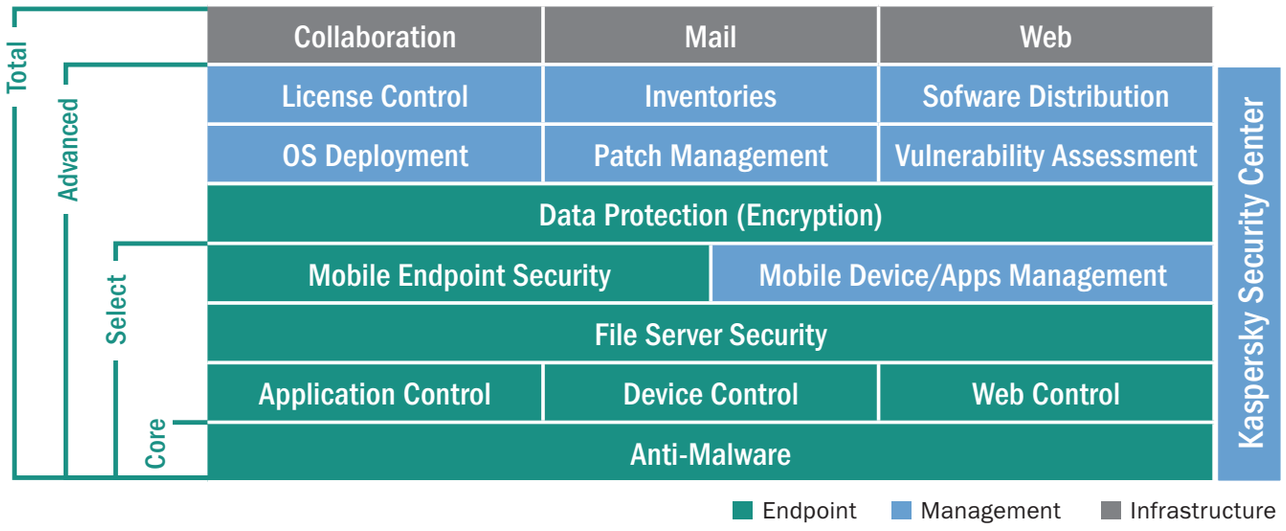
Kaspersky Endpoint Security for Business	Harnessing the expertise of the world's best threat intelligence ecosystem, Kaspersky Endpoint Security for Business provides a tiered security approach based on a single integrated platform incorporating features including robust application, device and web control tools, data encryption, mobile endpoint security and MDM, and systems and patch management. Everything is managed from one central console — Kaspersky Security Center. Kaspersky Total Security for Business adds mail, web and collaboration server security, safeguarding your perimeters and securing your complete enterprise IT environment.
Kaspersky Targeted Solutions	Standalone solutions allowing Kaspersky Lab security to be applied to specific areas of your IT system. Some solutions, like Kaspersky Security for Mobile, are also available as part of Kaspersky Endpoint Security for Business. Others, like Kaspersky Security for Virtualization, are available purely as targeted solutions. All are built on the same leading edge technologies and threat intelligence, and all physical, mobile and virtual endpoint security solutions are managed centrally through Kaspersky Security Center.
Kaspersky Threat Intelligence Services and Enterprise Solutions	Leveraging Kaspersky's threat intelligence, technical expertise, data and training skills to boost the security of your brand, your organisation and your employees Enterprise Solutions address security issues for specific industries and infrastructures, and specific forms of attack like Distributed Denial of Service (DDoS).
KASPERSKY SMALL OFFICE SECURITY	World-class protection made easy for very small businesses.

ABOUT KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Kaspersky Endpoint Security for Business offers a complete security solution, designed by the world's leading security experts. The deepest, most forward-looking protection, efficient performance and straightforward management build through progressive tiers to fully secure your business.

All components have been designed and built in-house to mesh together into a single security platform geared to your business needs. The result is a stable, integrated solution with no gaps, no compatibility issues and no additional workload as your security builds.

Administrators can see, control and protect their IT environment with Kaspersky Endpoint Security for Business. Tools and technologies are uniquely balanced across progressive tiers to meet your evolving security and IT needs. Kaspersky can make your job easier.

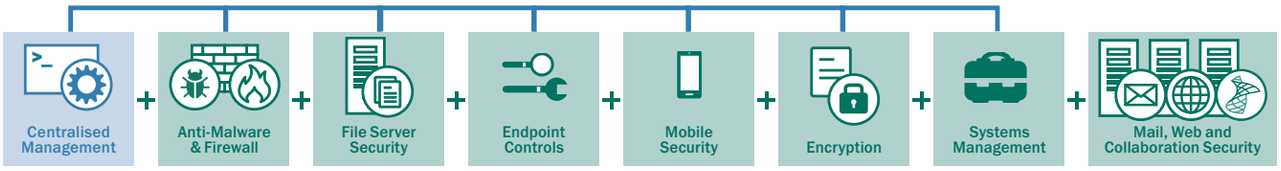


Kaspersky boasts a comprehensive list of technologies — all working together from the same codebase and further assisted by the cloud-based Kaspersky Security Network — to give our customers the world-class protection they need.

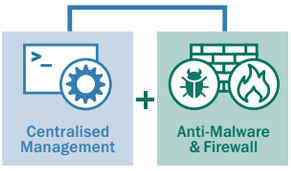
In short, we've delivered the industry's first Security Platform, built from the ground up, making it easy for the administrator to see, control and protect your world.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Powerful multi-layered protection against known, unknown and advanced threats, designed and built by the industry's leading security experts. Kaspersky Endpoint Security for Business, backed by world-renowned threat intelligence, provides unequalled IT security and control.



KASPERSKY ENDPOINT SECURITY FOR BUSINESS — CORE



Best-in-class anti-malware protection — the foundation of the Kaspersky Lab security platform

Kaspersky Lab's multi-layered protection technologies are developed in-house by people passionate about security. The result, independent tests confirm, is the most powerful and effective security solution in the industry — there is no better protection for your organisation.

Protection from Known, Unknown and Advanced Threats — unique, sophisticated technologies identify and eliminate existing and emerging threats.

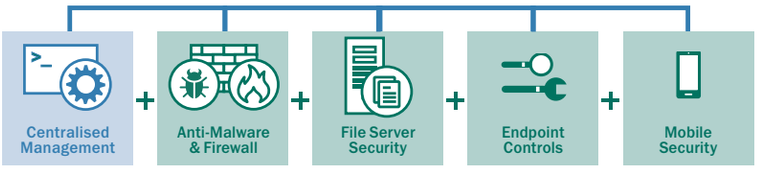
Automatic Exploit Prevention — proactively targets and identifies unknown and advanced threats.

Cloud-Assisted Protection — using real-time information from the worldwide Kaspersky Security Network.

System Watcher — Provides a unique file-restore function should the system be impacted.

Host-based Intrusion Prevention System (HIPS) with Personal Firewall —HIPS restricts activities according to the application's trust level – supported by an application-level Personal Firewall, which restricts network activity.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS — SELECT



Powerful, granular endpoint controls combined with proactive security and management for mobile devices and data

Application, web and device controls, including dynamic whitelisting supported by Kaspersky's unique in-house laboratory, add a further dimension to deep endpoint security. Corporate and employee owned (BYOD) mobile devices are also secured, and platforms are unified to be managed, together with all protected endpoints, though the Kaspersky Security Center console. File server protection ensures that infection cannot spread to secured endpoints through stored data.

ENDPOINT CONTROLS

Application Control with Dynamic Whitelisting — using real-time file reputations delivered by the Kaspersky Security Network, enables IT administrators to allow, block or regulate applications, including operating a 'Default Deny' whitelisting scenario in a live or test environment. Application Privilege Control and Vulnerability Scanning monitor applications and restrict those performing suspiciously.

Web Control — browsing policies can be created around pre-set or customisable categories, ensuring comprehensive oversight and adminstrative efficiency.

Device Control — granular data policies controlling the connection of removable storage and other peripheral devices can be set, scheduled and enforced, using masks for simultaneous deployment to multiple devices.

FILE SERVER SECURITY

Managed together with endpoint security through Kaspersky Security Center.

MOBILE SECURITY:

Powerful Security for Mobile Devices — advanced, proactive and cloud-assisted technologies combine to deliver multi-layered real-time mobile endpoint protection.

Web protection, anti-spam and anti-phishing components further increase device security.

Remote Anti-Theft — Lock, Wipe, Locate, SIM Watch, Alarm, Mugshot and Full or Selective Wipe all prevent unauthorised access to corporate data if a mobile device is lost or stolen. Administrator and end-user enablement, together with Google Cloud Management support, delivers quick activation if required.

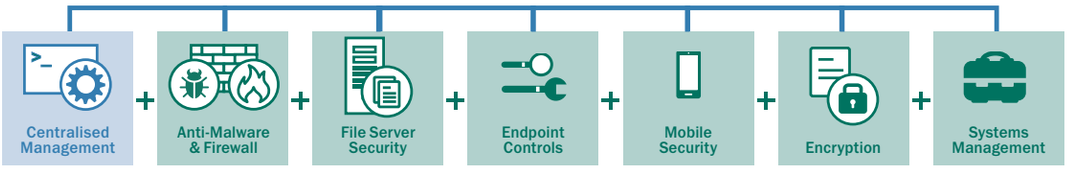
Mobile Application Management (MAM) — Controls limit the user to running whitelisted applications, preventing the deployment of unwanted or unknown software. '**Application Wrapping**' isolates corporate data on employee owned devices. Additional encryption or 'Selective Wipe' can be remotely enforced.

Mobile Device Management (MDM) — a unified interface for **Microsoft® Exchange ActiveSync** and **iOS MDM** devices with OTA (Over The Air) policy deployment. **Samsung KNOX** for Android™-based devices is also supported.

Self-Service Portal — allows self registration of employee owned approved devices onto the network with automatic installation of all required certificates and keys, and user/owner emergency activation of anti-theft features, reducing the IT administrative workload.

Kaspersky Endpoint Security for Business — SELECT also includes all components of the CORE tier.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS — ADVANCED



Systems management tools optimise IT efficiency and security, while integrated encryption protects sensitive data

Automated patch management and OS image management, remote software distribution and SIEM integration all help to streamline administration, while hardware and software inventories and license management provide visibility and control. Integrated encryption technology adds a powerful layer of data protection.

SYSTEMS MANAGEMENT

Vulnerability and Patch Management — automated OS and application vulnerability detection and prioritisation, combined with the rapid automated distribution of patches and updates.

Operating System Deployment — easy creation, storage and deployment of OS 'golden' images from a central location, including UEFI support.

Software Distribution and Troubleshooting — remote software deployment and application and OS update available on-demand or scheduled, including Wake-on-LAN support. Time-saving remote troubleshooting and efficient software distribution is supported through Multicast technology.

Hardware and Software Inventories and Licensing Management — identification, visibility and control (including blocking), together with license usage management, provides insight into all software and hardware deployed across the environment, including removable devices. Software and hardware license management, guest device detection, privilege controls and access provisioning are also available.

SIEM Integration — support for IBM® QRadar and HP ArcSight SIEM systems.

Role Based Access Control (RBAC) — Administrative responsibilities can be assigned across complex networks, with console views customised according to assigned roles and rights

ENCRYPTION

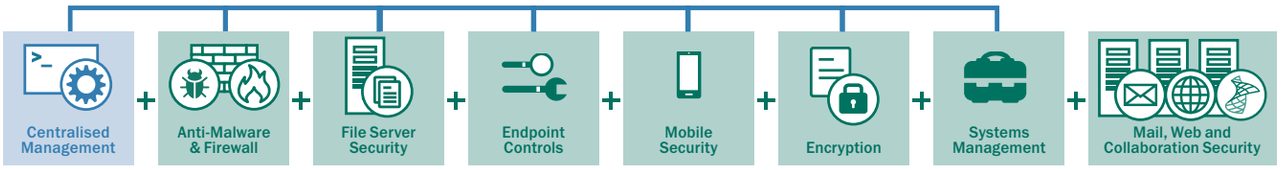
Powerful Data Protection — File/Folder (FLE) and Full Disk (FDE) encryption can be applied to endpoints. Support for "portable mode" ensures encryption administration across devices leaving administrative domains.

Flexible User Login — Pre-boot authentication (PBA) for added security includes optional 'single sign-on' for user transparency. 2-factor or token based authentication is also available.

Integrated Policy Creation — Unique integration of encryption with application and device controls provides an additional layer of enhanced security and administrative ease

Kaspersky Endpoint Security for Business — ADVANCED also includes all components of the SELECT and CORE tiers.

KASPERSKY TOTAL SECURITY FOR BUSINESS



Organisations who demand comprehensive security for their entire IT environment choose Kaspersky Total Security for Business

Kaspersky Total Security for Business delivers the most complete platform of protection and management offered in the industry today. Kaspersky Total Security for Business secures every layer of your network and includes powerful configuration tools to ensure your users are productive and free from the threat of malware, regardless of device or location.

MAIL SERVER SECURITY

Effectively prevents email based malware threats, phishing attacks and spam using cloud-based, real-time updates for exceptional capture rates and minimal false positives. Anti-malware protection for IBM® Domino® is also included. DLP functionality for Microsoft Exchange is available separately.

SECURITY FOR INTERNET GATEWAYS

Ensures secure Internet access across the organisation by automatically removing malicious and potentially hostile programs in HTTP(S) / FTP / SMTP and POP3 traffic.

COLLABORATION SECURITY

Defends SharePoint® servers and farms against all forms of malware. DLP functionality for Sharepoint, available separately, provides content and file filtering capabilities identify confidential data and protect against data leakage.

Kaspersky Total Security for Business also includes all components of the ADVANCED, SELECT and CORE tiers.

PRODUCT FEATURES

Which solution is right for you?

	Core	Select	Advanced	Total	Managed by Security Center	Available in a Targeted Solution
Anti-Malware	•	•	•	•	•	
Firewall	•	•	•	•	•	
Application Control		•	•	•	•	
Device Control		•	•	•	•	
Web Control		•	•	•	•	
File Server Security		•	•	•	•	•
Mobile Endpoint Protection		•	•	•	•	•
Mobile Device/ Apps Management		•	•	•	•	•
Encryption			•	•	•	
Vulnerability Assessment			•	•	•	•
Patch Management			•	•	•	•
Inventories			•	•	•	•
License Control			•	•	•	•
Software Distribution			•	•	•	•
Operating Systems Deployment			•	•	•	•
Collaboration Server Security				•		•
Mail Server Security				•	•	•
Internet Gateway Security				•		•
Virtual Infrastucture Security					•	•
Storage Server Security					•	•

• Included • Partially included — see product pages for details

KASPERSKY SECURITY FOR FILE SERVER

Kaspersky Security for File Server provides cost-effective, reliable, scalable security for shared file storage with no discernable impact on system performance.

HIGHLIGHTS

POWERFUL ANTI-MALWARE PROTECTION

Kaspersky's award-winning anti-malware engine provides powerful server protection, blocking even the latest known and potential malware threats from entering the local network via malicious or dangerous programs.

HIGH PERFORMANCE AND RELIABILITY

You can be confident that Kaspersky Security for File Server will not noticeably slow your system down or interfere with business operations under heavy network load conditions.

MULTIPLE PLATFORM SUPPORT

A single, effective security solution for heterogeneous server networks, supporting the latest platforms and servers including terminal, cluster and virtual servers, with no compatibility issues.

POWERFUL MANAGEMENT AND REPORTING

Effective, user-friendly management tools, information about server protection status, flexible time settings for scans and an extensive reporting system provide efficient control of file server security, all helping reduce the cost of ownership.

FEATURES

- **Real-time anti-malware protection** for file servers running the latest versions of Windows® (including Windows Server® 2012/R2), Linux® and FreeBSD (both including Samba).
- **Citrix and Microsoft® terminal server protection.**
- **Fully supports cluster servers.**
- **Scalability** — supporting and securing even the most complex heterogeneous infrastructures with ease.
- **Reliability, stability and high fault tolerance.**
- **Optimised, intelligent scan technology** including on-demand and scanning of critical system areas.
- **Trusted zones** help increase security performance while reducing resource levels needed for scanning.
- **Quarantine and back-up** of data prior to disinfection or deletion.
- **Isolation** of infected workstations.
- **Centralised installation, management and updates** with flexible configuration options.
- **Flexible incident response scenarios.**
- **Comprehensive reports** on network protection status.
- **Application status notification system.**
- **Support for Hierarchical Storage Management** (HSM) systems.
- **Proven Hyper-V and Xen Desktop support.**
- **VMware Ready.**
- **Support for ReFS.**

Kaspersky Security for File Server is included in Kaspersky Endpoint Security for Business — SELECT and ADVANCED, as well as Kaspersky Total Security for Business. It is also available to purchase separately as a Targeted Solution.

ABOUT OUR ENDPOINT CONTROLS TECHNOLOGY

Powerful endpoint control tools, tightly integrated with cutting-edge anti-malware and the industry's only dedicated Whitelisting laboratory helps protect your business from today's dynamic threat environment.

PROTECT, ENFORCE, CONTROL

- Vulnerabilities in trusted applications, web-based malware and lack of control over peripheral devices form part of an increasingly complex threat landscape. Kaspersky Lab's Application, Web and Device Control tools enable complete control over your endpoints without compromising on productivity.

APPLICATION CONTROL AND DYNAMIC WHITELISITING

Protect systems from known and unknown threats by giving administrators total control over the applications and programs allowed to run on endpoints, regardless of end user behavior. In addition, enable application integrity monitoring to evaluate application behaviour and prevent them from executing unexpected actions that could endanger the endpoint or network. Simplified, customisable or automated policy creation and enforcement enable:

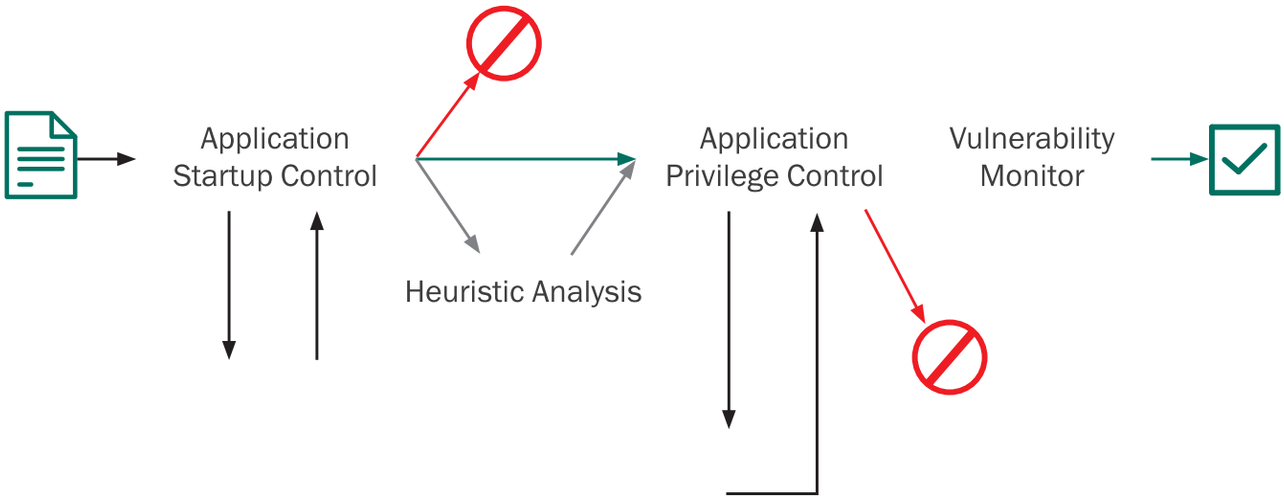
- **Application start-up control**: Grant, block, audit application launches. Drive productivity by restricting access to non-business-related applications.

- **Application privilege control**: Regulate and control application access to system resources and data. Classify applications as trusted, untrusted or restricted. Manage application access to encrypted data on endpoints, such as information posted via web browsers or Skype.

- **Application vulnerability scanning**: Proactive defense against attacks targeted at vulnerabilities in trusted applications.

Most control solutions offer only basic blocking/access functionality. Kaspersky Lab's control tools are unique in their use of cloud-based whitelisting databases, enabling near-real-time access to the latest application data.

Kaspersky Lab's application control technologies use cloud-based whitelisting databases to analyse and monitor applications at every stage: download, installation, execution.



Dynamic Whitelisting, which may be enabled via comprehensive 'Default Deny' blocks all applications attempting to run on any workstation, unless explicitly allowed by administrators. Kaspersky Lab is the only security company with a dedicated Whitelisting laboratory, maintaining a constantly monitored and updated database of more than 500 million programs.

Kaspersky Lab's **Default Deny can be applied in a test environment**, enabling administrators to establish application legitimacy before blocking. In addition, application categories based on digital signatures can be created, preventing users from starting legitimate software that's been modified by malware or comes from a suspicious source.

EASY ADMINISTRATION

All Kaspersky Lab control tools integrate with Active Directory, so setting blanket policies is simple and fast. All endpoint controls are managed from the same console, through a single interface.

WEB CONTROLS

Monitor, filter and control the web sites that end users can access in the workplace, increasing productivity while protecting against web-based malware and attacks.

Kaspersky Lab's advanced web controls are built on a constantly updated directory of web sites, grouped into categories (e.g. adult, games, social networks, gambling,). Administrators can easily create policies to prohibit, limit or audit end user use of any individual sites or categories of site, as well as create their own lists. Malicious sites are automatically blocked.

By restricting their use, Kaspersky Lab's web controls help prevent data loss via social networks and instant messaging services. Flexible policies enable administrators to allow browsing at certain times of the day. Integration with Active Directory means policies can be applied across the organisation quickly and easily.

For added security, Kaspersky Lab's web controls are enabled directly at the endpoint, meaning policies are enforced even when the user is not on the network.

DEVICE CONTROLS

Disabling a USB port doesn't always solve your removable device problems. For example, a disabled USB port impacts on other security measures, such as token-based VPN access.

Kaspersky Lab's device controls enable a more granular level of control at bus, type and device level – maintaining end user productivity while optimising security. Controls can be applied right down to the specific serial number of the device.

- Set connect/read/write permissions for devices, as well as time scheduling.
- Create device control rules based on masks, eliminating the need to physically connect devices in order to whitelist them. Whitelist multiple devices simultaneously.
- Control data exchange via removable devices inside and outside the organisation, reducing the risk of data loss or theft.
- Integrate with Kaspersky Lab's encryption technologies, to enforce encryption policies on specific device types.

Endpoint Controls technology is included in Kaspersky Endpoint Security for Business — SELECT and ADVANCED, and in Kaspersky Total Security for Business.

KASPERSKY SECURITY FOR MOBILE

Mobile devices are increasingly attractive to cybercriminals. Meanwhile, 'Bring Your Own Device' (BYOD) is contributing to an increasingly complex mix of devices, creating a challenging management and control environment for IT administrators.

Kaspersky Security for Mobile ensures your device is safe, no matter where it is. Protect against constantly evolving mobile malware. Quickly and easily gain visibility and control over the smartphones and tablets in your environment, from one central location and with minimal disruption.

KEY PRODUCT FEATURES

- Powerful Anti-Malware
- Anti-Phishing and Anti-Spam
- Web protection
- Application Control
- Rooting/jailbreak detection
- Containerisation
- Anti-Theft
- Mobile Device Management
- Self-Service Portal
- Centralised management
- Web Console
- Supported platforms:
  - Android™
  - iOS
  - Windows® Phone

HIGHLIGHTS

ADVANCED ANTI-MALWARE FOR MOBILE DEVICE AND DATA SECURITY

IIn 2014 alone, Kaspersky Lab dealt with almost 1.4 million unique mobile malware attacks . Kaspersky Security for Mobile combines anti-malware with deep layers of protection technologies, guarding against known and unknown threats to data stored on mobile devices.

MOBILE DEVICE MANAGEMENT (MDM)

Integration with all leading mobile device management platforms enables remote 'Over the Air' (OTA) deployment and control for easier usability and management of Android, iOS and Windows Phone devices.

MOBILE APPLICATION MANAGEMENT (MAM)

Containerisation and selective wipe capabilities enable separation of business and personal data on the same device — supporting BYOD initiatives. Combined with our encryption functionality and anti-malware, this makes Kaspersky Security for Mobile a proactive mobile protection solution, rather than one that simply attempts to isolate a device and its data.

CENTRALISED MANAGEMENT

Manage multiple platforms and devices from the same console as other endpoints — increase visibility and control without additional effort or technology to manage.

MOBILE SECURITY AND MANAGEMENT FEATURES

POWERFUL ANTI-MALWARE

Signature-based, proactive and cloud-assisted (via Kaspersky Security Network — KSN) protection from known and unknown mobile malware threats. On-demand and scheduled scans combine with automatic updates to increase protection.

ANTI-PHISHING AND ANTI-SPAM

Powerful Anti-Phishing and Anti-Spam technologies protect the device and its data from phishing attacks and help filter out unwanted calls and texts.

WEB CONTROL/SAFE BROWSER
Supported by Kaspersky Security Network (KSN), these technologies work in real time to block access to malicious and unauthorised web sites. A Safe Browser delivers constantly updated reputation analysis, ensuring safe mobile browsing.

APPLICATION CONTROL
Integrated with KSN, Application Controls restrict application use to approved software only, prohibiting use of grey or unauthorised software. Make device functionality dependent on installation of required applications. Application inactivity control enable admins to require user re-login if an application is idle for a defined period of time. This protects data even if an application is open when the device is lost or stolen.

ROOTING/JAILBREAK DETECTION
Automatic detection and reporting of rooting or jailbreaking can be followed with automatic blocking of access to containers, selective wiping or entire device wipe.

CONTAINERISATION
Separate business and personal data by 'wrapping' applications into containers. Additional policies, such as encryption, can be applied to protect sensitive data. Selective wipe enables the deletion of containerised data on a device when an employee leaves, without impacting on their personal data.

ANTI-THEFT
Remote Anti-Theft features including wipe, device lock, locate, SIM watch, 'mugshot' and 'alarm' device detection can be activated in the event of device loss or theft. Depending on the case, the anti-theft commands can be applied in a very flexible way. For example, integration with Google Cloud Messaging (GCM) allows delivering the commands almost immediately, increasing reaction times and improving security, while sending commands through the Self-Service Portal doesn't require actions from administrator.

MOBILE DEVICE MANAGEMENT (MDM)
Support for Microsoft® Exchange ActiveSync, Apple MDM and Samsung KNOX 2.0 – enables a wide range of policies, through a unified interface, regardless of the platform. E.g. Enforce encryption and passwords or control camera use, applying policies to individual users or groups, managing APN/VPN settings etc

SELF-SERVICE PORTAL
Delegate routine security management to employees, enable self-registration of approved devices. During new device enablement process, all required certificates can be delivered automatically through the portal, no need for administrator involvement. In case of the device loss, the employee can perform all available Anti-Theft actions through the Portal.

CENTRALISED MANAGEMENT
Manage all mobile devices centrally, from a single console, which also allows managing IT security for all other endpoints. Web Console allows administrators control and manage devices remotely, from any computer.

Kaspersky Security for Mobile is included in Kaspersky Endpoint Security for Business — SELECT and ADVANCED, as well as Kaspersky Total Security for Business. It is also available to purchase separately as a Targeted Solution.

ABOUT OUR ENCRYPTION TECHNOLOGY

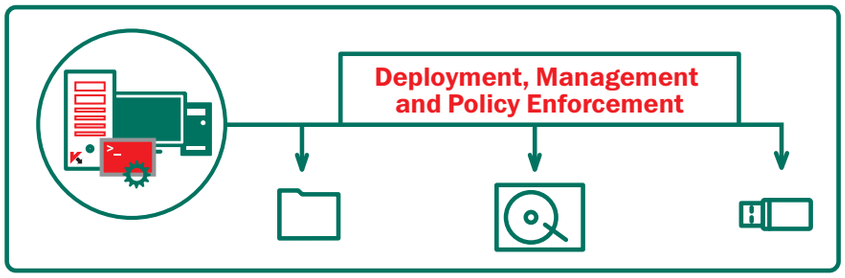
Prevent unauthorised data access caused by device loss, theft or data-stealing malware.

Proactive data protection and compliance is a global imperative. Kaspersky Lab's encryption technology protects valuable data from accidental loss, device theft and targeted malware attacks. Combining strong encryption technology with Kaspersky Lab's industry-leading endpoint protection technologies, our integrated platform protects data at rest and in motion.

Because it's from Kaspersky Lab, it's easy to deploy and administer from a centralized management console, using a single policy.

Prevent data loss and unauthorised information access with Kaspersky Lab's Encryption Technology:
- **Full Disk Encryption (FDE)**
- **File/Folder Level (FLE)**
- **Removable and Internal Devices**

ADMINISTERED THROUGH A SINGLE MANAGEMENT CONSOLE

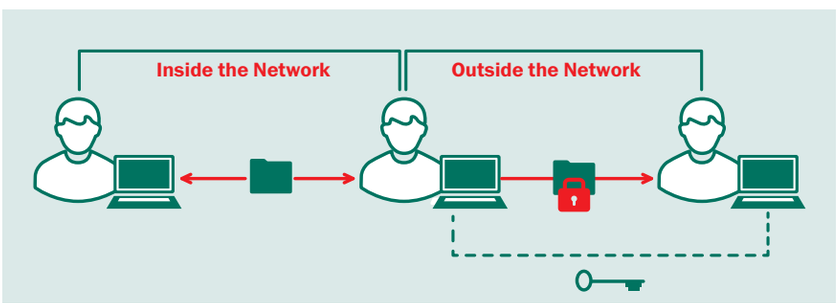


INDUSTRY STANDARD SECURE CRYPTOGRAPHY
Kaspersky Lab uses Advanced Encryption Standard (AES) with 256 bit key length with simplified key management and escrow. Supports Intel® AES-NI technology, UEFI and GPT platforms.

COMPLETE FLEXIBILITY
Kaspersky Lab offers file and folder level encryption (FLE) and full disk encryption (FDE), covering all possible use scenarios. Data may be protected on both hard drives and removable devices. 'Portable mode' enables the use and transfer of data on encrypted removable media, even on computers where encryption software is not installed — facilitating secure 'off perimeter' data exchange.

SINGLE SIGN-ON, END USER TRANSPARENCY
From set up to daily use, Kaspersky Lab's encryption technology works transparently across all applications, without impeding end user productivity. Single sign-on ensures seamless encryption — the end user may not even be aware the technology is running.

Kaspersky Lab's encryption enables seamless, transparent file transfer between users inside and outside the network.



ENCRYPTION FEATURES

SEAMLESS INTEGRATION WITH KASPERSKY LAB SECURITY TECHNOLOGIES

Complete integration with Kaspersky Lab's anti-malware, endpoint controls and management technologies for true multi-layered security built on a common code base. For example, a single policy could enforce encryption on specific removable devices. Apply encryption settings under the same policy as anti-malware, device control and other endpoint security elements. No need to deploy and manage separate solutions. Network hardware compatibility is automatically checked before encryption is deployed; support for UEFI and GPT platforms is standard.

ROLE BASED ACCESS CONTROL

In larger organisations, choose to delegate encryption management using role based access control functionality. This enables less complex encryption management.

PRE-BOOT AUTHENTICATION (PBA)

User credentials are required before the operating system even boots, providing an additional layer of security, with optional single sign-on. Kaspersky Lab's encryption technology PBA is also available for non-QWERTY keyboard layouts.

SMARTCARD AND TOKEN AUTHENTICATION

Supports Two Factor Authentication via popular makes of smartcards and tokens, eliminating the need for additional usernames and passwords and enhancing end user experience.

EMERGENCY RECOVERY

Administrators can decrypt data in the event of hardware or software failure. User password recovery for PBA or encrypted data access is implemented via a simple challenge/response mechanism.

OPTIMISED DEPLOYMENT, CUSTOMISABLE SETTINGS

For ease of deployment, Kaspersky Lab's encryption functionality is enabled only within the 'Advanced' and 'Total' tiers of Kaspersky Endpoint Security for Business, no need for separate installation. Encryption settings are pre-defined but can be customised for common folders such as My Documents, Desktop, new folders, file extensions and groups, such as Microsoft® Office documents or message archives.

Encyption technology is included in Kaspersky Endpoint Security for Business — ADVANCED, and in Kaspersky Total Security for Business.

KASPERSKY SYSTEMS MANAGEMENT

Enhance security, reduce complexity with centralised IT management tools.

Unpatched vulnerabilities in popular applications are one of the biggest threats to business IT security. This risk is compounded by increasing IT complexity — if you don't know what you've got, how can you secure it?

By centralising and automating essential security, configuration and management tasks, such as vulnerability assessment, patch and update distribution, inventory management and application rollouts, IT administrators not only save time, but optimise security.

Kaspersky Systems Management helps minimise IT security risks and cut through IT complexity, giving managers complete, real-time control and visibility over multiple devices, applications and users, from a single screen.

KEY PRODUCT FEATURES

- **Vulnerability Assessment and Patch Management**
- **Hardware and software inventories**
- **Remote software installation and troubleshooting, including remote office coverage**
- **Operating systems deployment**
- **SIEM integration**
- **Role-based access control**
- **Centralised management**

ENHANCE SECURITY

Increase IT security and reduce routine task loads with timely, automated patching and updates. Automated vulnerability discovery and prioritisation supports greater efficiency and reduces resource burden. Independent tests[1] show that Kaspersky Lab delivers the most comprehensive automated patch and update coverage in the fastest time.

CONTROL WITH FULL VISIBILITY

Total network visibility from a single console eliminates administrator guesswork and provides awareness of every application and device (including guest devices) entering the network. This drives centralised control of user and device access to organisational data and applications, in line with IT policies.

MANAGE CENTRALLY

Kaspersky Lab's Systems Management is a managed component of the Kaspersky Security Center. Each feature is accessed and managed through this central console, using consistent, intuitive commands and interfaces to automate routine IT tasks.

FEATURES

VULNERABILITY ASSESSMENT AND PATCH MANAGEMENT

Automated software scanning enables rapid vulnerability detection, prioritisation and remediation. Patches and updates can be delivered automatically, in the shortest timeframes[2], for Microsoft® and non-Microsoft software. Administrator is notified

1, 2 Patch Management Solutions Test commissioned by Kaspersky Lab and performed by AV-TEST GmBH (July 2013)

about patch installation status. Non-critical fixes can be postponed until after hours, even if computers are switched off, using Wake-on-LAN. Multicast broadcasting enables local distribution of patches and updates to remote offices, reducing bandwidth requirements.

HARDWARE AND SOFTWARE INVENTORIES
Automatic discovery, inventory, notification and tracking of hardware and software, including removable devices, provides administrators with detailed insight into devices and assets used on the corporate network. Guest devices can be detected and provided with Internet access. License control provides visibility into number of nodes and expiry date.

FLEXIBLE OPERATING SYSTEM AND APPLICATION PROVISIONING
Centralised, easy creation, storage, cloning and deployment of optimally secured system images. After hours deployment via Wake-on-LAN with post installation editing for greater flexibility. UEFI support.

SOFTWARE DISTRIBUTION
Deploy/update remotely, from a single console. Over 100 popular applications, identified via Kaspersky Security Network can be automatically installed, after hours if desired. Full support for remote troubleshooting, with enhanced security via user permissions and session logs/audits. Save on traffic to remote offices with Multicast technology for local software distribution.

SIEM INTEGRATION
Report directly and effect event transfers into leading SIEM systems — IBM® QRadar and HP ArcSight. Collect logs and other security-related data for analysis, minimising administrator workload and tools, while simplifying enterprise-level reporting.

ROLE-BASED ACCESS CONTROL
Distinguish administrative roles and responsibilities in complex networks. Customise console view according to role and rights.

CENTRALISED MANAGEMENT
One integrated administration console, Kaspersky Security Center, supports the administration of system security for desktop, mobile and virtual endpoint, across the network, through a single interface.

Kaspersky Systems Management is included in Kaspersky Endpoint Security for Business — ADVANCED, and in Kaspersky Total Security for Business, and is also available to purchase separately as a Targeted Solution.

KASPERSKY SECURITY FOR MAIL SERVER

Kaspersky Security for Mail Server provides outstanding protection for traffic running through mail servers from spam, phishing and both generic and advanced malware threats, even in the most complex heterogeneous infrastructures.

Protection against confidential data loss through emails and attachments is also provided for Microsoft® Exchange Server Environments.

HIGHLIGHTS

PROTECTION FROM MALWARE THREATS

Powerful protection from malware is provided by Kaspersky's award-winning anti-malware engine, supported in real time by the cloud-assisted Kaspersky Security Network, together with proactive exploit protection, and malicious URL filtering.

ANTI-SPAM PROTECTION

For Microsoft Exchange and Linux®-based mail servers, Kaspersky's cloud-assisted anti-spam engine has been proven to block up to 99.96% of time- and resource-wasting spam, with minimal false positives.

DATA LOSS PROTECTION AND CONTROL (MICROSOFT EXCHANGE SERVERS)*

By identifying the inclusion of business, financial, personal and other sensitive data in outgoing emails and attachments on Microsoft Exchange servers, and controlling the flow of this information, Kaspersky Security for Mail Servers keeps your and your employees' confidential data secure, and in compliance with data protection legislation. Sophisticated analytical techniques, including structured data searches and business-specific glossaries, help identify suspicious emails which can then can be blocked. The system can even alert the sender's Line Manager to the potential data security breach.

SIMPLE, FLEXIBLE ADMINISTRATION

User-friendly management and reporting tools and flexible scan settings give you efficient control of your mail and document security, helping to reduce the total cost of ownership.

FEATURES

- Real-time anti-malware protection supported by the cloud-assisted Kaspersky Security Network.
- Immediate protection against unknown exploits and even zero-day vulnerabilities.
- Advanced protection against spam — Kaspersky Lab's anti-spam engine blocks more than 99% of unwanted email traffic.
- Data Leakage Protection (Microsoft Exchange Servers)*. Detection of confidential information in emails and attachments, through categories (including personal details and payment card data), glossaries and deep level analysis using structured data.
- Real-time cloud-assisted anti-spam scanning of all messages on Microsoft® Exchange servers, including public folders, using Kaspersky Security Network.
- On-schedule scanning of emails and Lotus Domino databases.
- Scanning of messages, databases and other objects on IBM® Domino® servers.
- Message filtering by recognised attachment format, size and name.
- Easy and convenient anti-malware and anti-spam database update process.
- Backup storage of data prior to disinfection or deletion.
- Scalability and fault tolerance.
- Easy installation and flexible integrated administration.
- Powerful notification system.
- Comprehensive reports on network protection status.

*When purchasing this product, the option to prevent confidential data loss or leakage is sold separately.

KASPERSKY SECURITY FOR INTERNET GATEWAY

Kaspersky Security for Internet Gateway is a world-class anti-malware solution that ensures safe always-on Internet access for your entire workforce.

HIGHLIGHTS

POWERFUL PROTECTION REDUCES DOWNTIME AND DISRUPTION
Kaspersky Labs' award-winning anti-malware engine blocks the latest known and potential malware threats from entering the local network via malicious or dangerous programs.

PERFORMANCE EFFICIENCY THROUGH OPTIMISATION
Optimised, intelligent scanning technology and load balancing reduce the load on resources, helping to preserve valuable bandwidth without compromising on security performance.

MULTIPLE PLATFORM SUPPORT
Support for the latest platforms and servers, including proxy servers, ideal for heavy network traffic volumes in heterogeneous environments. Microsoft® Forefront® TMG support extends to corporate mail as well as web gateway protection.

STRAIGHTFORWARD MANAGEMENT AND REPORTING
Simple, user-friendly management tools, flexible scan settings and protection status reporting systems.

FEATURES

- **Always-on, proactive protection** from emerging and known malware threats.
- **Outstanding malware detection rates** combined with minimal false positives.
- **Optimised, intelligent scanning technology.**
- **Real-time scanning** of HTTP, HTTPS and FTP traffic from published servers.
- **Protection for Squid**, the most popular Linux proxy server.
- **Convenient tools** for installation, management and updates.
- **Flexible scanning tools and incident response scenarios**.
- **Load balancing** of server processors.
- **Scalability and fault tolerance.**
- **Comprehensive reporting** on network protection status.

FEATURES SPECIFIC TO MICROSOFT® FOREFRONT® TMG AND ISA SERVERS:

- Real-time monitoring of application status.
- Scanning of VPN connections.
- Real-time scanning of HTTPS traffic (TMG only).
- Email traffic protection (via POP3 and SMTP protocols).
- Backup storage (TMG only).

Kaspersky Security for Mail Server and Kaspersky Security for Internet Gateway are included in Kaspersky Total Security for Business, and are also available to purchase separately as Targeted Solutions.

KASPERSKY SECURITY FOR COLLABORATION

Data protection and control for collaboration platforms, including SharePoint farms.

HIGHLIGHTS

FULLY SECURING YOUR SHAREPOINT PLATFORM

Powerful protection against known, unknown and advanced threats is provided through the cloud-supported Kaspersky Security Network, while anti-phishing technology protects against web-based threats to collaborative data.

PREVENTING CONFIDENTIAL DATA LEAKAGE*

Using pre-installed or custom dictionaries and data categories, Kaspersky Security for Collaboration checks every document placed on SharePoint servers for sensitive information, word by word and phrase by phrase.

ENFORCING COMMUNICATION POLICIES

Content and filtering features help enforce your communication policies and standards, identifying and blocking inappropriate content while preventing the wasteful storage of inappropriate files and file formats.

FEATURES

ANTI-MALWARE PROTECTION

- **On-access scan** — files are scanned in real time, while uploading or downloading.
- **Background scan** — files stored on the server are regularly checked using the latest malware signatures.
- **Integration with Kaspersky Security Network** — providing real-time cloud-assisted protection against even zero-day threats.

SUPPORTS YOUR ORGANISATION'S COMMUNICATION POLICIES

- **File filtering** — helps enforce document storage policies and reduce the demands placed on storage devices. By analysing real file formats, regardless of the extension name, the application ensures that users cannot use a banned file type in violation of the security policy.
- **Protection for wikis/blogs** — protects all SharePoint repositories, including wikis and blogs.
- **Content filtering** — prevents the storage of files that include inappropriate content. The content of each file is analysed based on key words. Customers can also create their own custom dictionaries for content filtering.

CONFIDENTIAL DATA LOSS PREVENTION*

- **Document scanning for confidential information.** The solution integrates modules that identify specific types of data, confirming that it meets relevant legal standards — for example, personal data (defined by regulatory compliances, such as HIPAA or EU Directive 95/46EC) or PCI DSS standard data (Payment Card Industry Data Security Standard). Data is scanned against built-in, regularly updated thematic dictionaries and against customised dictionaries.
- **Structured data search** — if information presented in specific structures is found in a message, it will be treated as potentially confidential, ensuring control over sensitive data, such as customer databases, held in complex arrays.

FLEXIBLE MANAGEMENT

- **Ease of management** — an entire server farm can be centrally managed from a single console. An intuitive interface includes all the most commonly used administrative scenarios.
- **Single dashboard** — a clearly laid out dashboard provides real-time access to the current product status, database version and license status of all protected servers.
- **Backup of modified files** — in the event of any incident, the original files can be restored if required, and detailed back-up information about modified files can be used to support investigations.
- **Integration with Active Directory®** — enables the authentication of Active Directory users.

Kaspersky Security for Collaboration is included in Kaspersky Total Security for Business, and is also available to purchase separately as a Targeted Solution.

*When purchasing this product, the option to prevent confidential data loss or leakage is sold separately.

KASPERSKY SECURITY FOR STORAGE

High-Performance Protection for EMC, NetApp, Hitachi and IBM® Storages.

HIGHLIGHTS

POWERFUL, REAL-TIME ANTI-MALWARE PROTECTION
'Always-on' proactive protection for network attached storage (NAS) solutions. Kaspersky's powerful anti-malware engine scans every file launched or modified for all forms of malware including viruses, worms and Trojans. Advanced heuristic analysis identifies even new and unknown threats.

OPTIMISED PERFORMANCE
High performance scanning, featuring optimised scan technology and flexible exemption settings, delivers maximum protection while minimising the impact on the system's performance.

RELIABLE
Exceptional fault-tolerance is achieved through a straightforward architecture using unified components designed and built to work together flawlessly. The result is a stable, resilient solution which, if forced to shut down, will restart automatically for reliable and continuous protection.

EASY TO ADMINISTER
Servers are remotely installed and protected 'out-of-the-box' with no reboots and are administered together through a simple, intuitive central console — Kaspersky Security Center — along with your other Kaspersky security solutions.

FEATURES

ALWAYS-ON, PROACTIVE SECURITY
Kaspersky's industry-leading anti-malware scanning engine, built by the world experts in threat intelligence, provides proactive protection against emerging and potential threats using smart technologies for enhanced detection.

AUTOMATIC UPDATES
Anti-malware databases update automatically with no disruption to scanning, ensuring continuous protection, and minimising administrator workload.

EXEMPTED PROCESSES AND TRUSTED ZONES
Scan performance can be fine-tuned by created 'trusted zones' which, together with defined file formats and processes such as data backups, can be exempted from scanning.

AUTORUN OBJECT SCANNING
For increased server protection, autorun file and operating system scans can be run to prevent malware from launching during system start-up.

FLEXIBLE SCANNING FOR OPTIMISED PERFORMANCE
Reduces scanning and configuration time and promotes load balancing, helping to optimise server performance. The administrator can specify and control the depth, breadth and timing of scan activity, defining which file types and areas must be scanned. On-demand scanning can be scheduled for periods of low server activity.

PROTECTS HSM AND DAS SOLUTIONS
Supports offline scan modes for the effective protection of Hierarchical Storage Management (HSM) systems. Direct Attached Storage (DAS) protection also helps promote the use of low cost storage solutions.

SUPPORT FOR ALL MAIN PROTOCOLS
Kaspersky Security for Storage supports the main protocols utilised by different storage systems: CAVA agent, RPC and ICAP.

VIRTUAL SYSTEMS AND TERMINAL SERVER PROTECTION
Flexible security includes protection for virtual (guest) operating systems in Hyper-V and VMware virtual environments, and for Microsoft® and Citrix terminal infrastructures.

ADMINISTRATION

CENTRALISED INSTALLATION AND MANAGEMENT
Remote installation, configuration and administration including notifications, updates and flexible reporting are handled through the intuitive Kaspersky Security Center. Command line management is also available if preferred.

CONTROL OVER ADMINISTRATOR PRIVILEGES
Different privilege levels can be assigned to each server's administrator, enabling compliance with specific corporate IT security policies.

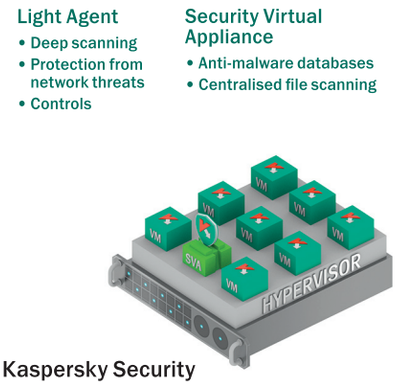
FLEXIBLE REPORTING
Reporting can be delivered via graphical reports or through reviewing Microsoft Windows® or Kaspersky Security Center's event logs. Search and filtering tools provide quick access to data in large-volume logs.

KASPERSKY SECURITY FOR VIRTUALIZATION

Kaspersky Security for Virtualization is a flexible solution which delivers both protection and performance for your environment.

LIGHT AGENT FOR ADVANCED PROTECTION

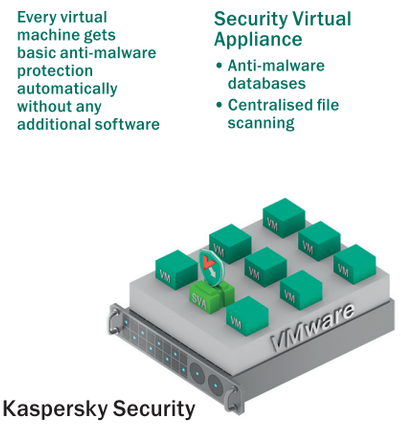
Kaspersky Security for Virtualization includes a powerful but lightweight agent which is deployed on each virtual machine. This allows for the activation of advanced endpoint security features. These include vulnerability monitoring, application, device and web controls, antivirus protection for instant messaging, mail and web, plus advanced heuristics. The result is powerful, multi-layered security combined with efficient performance.



Kaspersky Security for Virtualization
Light agent configuration

OPTIONAL AGENTLESS CONFIGURATION FOR VMWARE ENVIRONMENTS

Tight integration levels with VMware technologies mean that Kaspersky Security for Virtualization can also be very easily deployed and managed on this platform in an agentless security configuration. All security activity is concentrated in the Security Virtual Appliance, interfacing with vShield for instant automatic virtual machine protection and with vCloud for network protection.



Kaspersky Security for Virtualization
Agentless configuration*

KEY PRODUCT FEATURES

- Centralised management via Kaspersky Security Center
- Centralised SVA based VM protection
- Advanced anti-malware
- Host-based Intrusion Prevention (HIPS) - Network attack blocker and firewall
- Endpoint controls for applications, web access and peripherals
- Cloud-assisted security via Kaspersky Security Network
- Anti-phishing
- Anti-virus for IM, mail and Internet traffic
- No additional installation or reboots for new VMs**

FLEXIBLE LICENSING

Depending on your needs, Kaspersky Security for Virtualization is available in the following license options:

- Machine-based licensing:
  - Per desktop
  - Per server
- Resource-based licensing:
  - Per core.

MULTIPLE PLATFORMS: SINGLE COST

A single license of Kaspersky Security for Virtualization includes support for virtual environments based on Citrix, Microsoft® and VMware.

SECURITY VIRTUAL APPLIANCE (SVA)

Kaspersky Lab provides two compelling solutions in this space, both of which rely on a Security Virtual Appliance.

Kaspersky Lab's Security Virtual Appliance (SVA) centrally scans all VMs in the host environment. This architecture provides efficient VM protection without sacrificing endpoint resources, eliminating AV scanning, update 'storms' and 'instant-on' gaps, and generating greater consolidation ratios.

INTEGRATION WITH PLATFORM ARCHITECTURE

Kaspersky Security for Virtualization supports VMware, Microsoft® Hyper-V® and Citrix Xen platforms and their core technologies.

VMware	Microsoft Hyper-V	Citrix Xen
High availability	Dynamic memory	Dynamic memory control
vCenter integration	Cluster shared volumes	VM protection & recovery (VMPR)
vMotion – host DRS	Live backup	Xenmotion (live migration)
Horizon view (full clones and linked clones)	Live migration	Multi-stream ICA
		Citrix receiver
		Personal vdisk

* Advanced security features such as file quarantine, HIPS, vulnerability scanning and endpoint controls are not available in this configuration.
** For non-persistent VMs, instant protection is available after including the light agent into the VM's image. For persistent VMs, the administrator must deploy the light agent manually during installation.

KASPERSKY THREAT INTELLIGENCE SERVICES

As a CISO/senior-level security professional, it is your responsibility to protect your organisation against today's threats, and to anticipate the dangers that lie ahead in the coming years. This demands a level of strategic security intelligence that very few companies have the resources to develop in-house.

Kaspersky Lab is a valuable business partner, always available to share up-to-the-minute intelligence via different channels, helping your SOC/IT security team remain fully equipped to protect the organisation from any online threat.

CYBERSECURITY EDUCATION
Kaspersky Lab's Cybersecurity Education program has been developed specifically for any organisation looking to promote the role of cybersecurity in order to better protect its infrastructure and intellectual property.

The program covers everything from security fundamentals to advanced digital forensics and malware analysis, helping customers to improve their cybersecurity knowledge in three main areas:

- Fundamental knowledge of the topic
- Digital Forensics and Incident Response
- Malware Analysis & Reverse Engineering

THREAT DATA FEEDS
Kaspersky Lab's Threat Data Feeds are designed to integrate up-to-the-minute security intelligence into existing Security Information and Event Management (SIEM) systems, providing an additional layer of protection.

MALWARE ANALYSIS; DIGITAL FORENSICS; INCIDENT RESPONSE
Kaspersky Lab's Investigation Services can help organisations formulate their defense strategies though providing in-depth threat analysis and advising on appropriate steps toward resolution of the incident.

Three levels of investigation are offered:

- Malware Analysis — helping you to understand the behavior and objectives of specific malware files that are targeting your organisation.
- Digital Forensics — providing a complete picture of the incident and how your organisation is affected.
- Incident Response — a full cycle incident investigation that includes an on-site visit from Kaspersky Lab's experts.

BOTNET THREAT TRACKING
Kaspersky Lab's expert solution tracks the activity of botnets and provides rapid (within 20 minutes) notification of threats associated with the users of individual online payment and banking systems. You can use this information to advise and inform your customers, security services providers and local law enforcement agencies about current threats.

INTELLIGENCE REPORTS
Kaspersky Lab's Intelligence Reports gives access to up-to-the-minute, relevant information based on more than 80 million user statistics gathered across 200 countries, increasing your awareness and knowledge of the threats your organisation faces.

Kaspersky Lab's knowledge, experience and deep intelligence has made it the trusted partner of the world's premier law enforcement and government agencies. You can leverage this intelligence in your organisation today.

KASPERSKY ENTERPRISE SOLUTIONS

DDOS PROTECTION — TOTAL DEFENSE AND MITIGATION

Taking care of every stage necessary to defend your business from Distributed Denial of Service attacks.

Kaspersky DDoS Protection provides everything your business needs to defend against — and mitigate the effects of — all types of DDoS attack. This includes continuous analysis of all of your online traffic, alerting you to the possible presence of an attack and then receiving your redirected traffic, cleaning your traffic and returning 'clean' traffic to you.

KASPERSKY FRAUD PREVENTION — FOR BANKS AND FINANCIAL INSTITUTIONS

A comprehensive, highly tailored and easy-to-use technology platform addressing fraud risks for online and mobile fi nancial transactions.

Kaspersky Fraud Prevention protects customers of financial organisations regardless of the type of device they us to access these services: PC, laptop, smartphone or tablet. The platform also includes a bank-side software component that detects malware and automatically identifies abnormal behaviour patterns in individual customers' transactions. Even if Kaspersky Fraud Prevention for Endpoints has not been installed, the Clientless Engine can prevent fraudulent transactions.

CRITICAL INFRASTRUCTURE PROTECTION

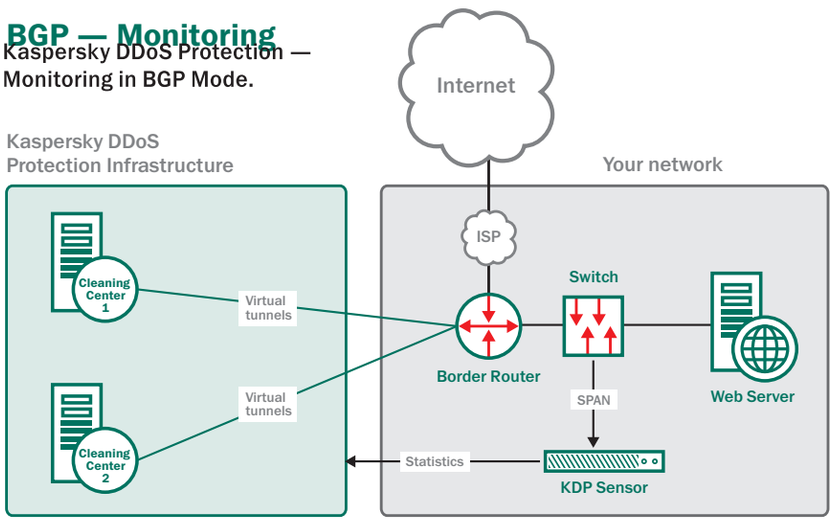
Securing industrial control systems and networks

Kaspersky Endpoint Security for Business delivers effective 'industrial mode' protection, guarding ICS/SCADA endpoints from the threats and vulnerabilities that form the backdoor of choice for many criminals targeting critical systems.

Working with leading industrial automation vendors such as Emerson, Rockwell Automation and Siemens, Kaspersky Lab has established many specialised procedures to ensure approval and compatibility with customer operational technology. This enables us to guarantee effective protection for critical infrastructures without impacting on operational continuity and consistency.

BGP — Monitoring

Kaspersky DDoS Protection — Monitoring in BGP Mode.



KASPERSKY SMALL OFFICE SECURITY

World-class Protection Made Easy for Small Businesses.

For your unique challenges: a unique solution. Powerful world-class protection that's quicker and easier than ever to use.

Specially designed for businesses with 25 users or less.
Easy to install and run — no training required.
Web console for internet-based administration from anywhere.

NO EXPERIENCE NEEDED
Kaspersky Small Office Security is designed for even the most non-technical person to install and run with ease. It's packed with straight forward 'wizards' to automatically guide you through things like:

- Setup, including removing any existing anti-malware
- Setting the controls and choosing the policies that work best for you and your business
- Automatically downloading these changes onto several computers at once

Everything is administered through a web-based dashboard so that you, or anyone else you choose, can manage your IT security remotely through the internet.

Kaspersky Small Office Security delivers outstanding security, but runs so smoothly and efficiently in the background that you almost forget it's there.

MULTIPLE LAYERS OF PROTECTION
Kaspersky Small Office Security applies layer upon layer of protection to your PCs and Macs, servers, tablets and smartphones. All the security tools your growing business needs, and more, are included. You can trust Kaspersky Small Office Security to handle your IT security, leaving you free to run your business.

- Cloud-assisted, real-time protection from new and emerging cyber-threats.
- Secures Windows® and Mac computers, Windows servers and Android™ mobile devices.
- Award-winning 'Safe Money' safeguards on-line financial transactions from online hackers and identity thieves.
- Controls to let you manage employee web surfing and social networking.
- Encryption to protect confidential business and customer data.
- Anti-phishing technologies to protect against fake and malicious websites.
- Powerful spam filtering.
- Secure password management.*
- Automatic back-up of your data via Dropbox to prevent lost data.

HELPS SAVE YOU MONEY
As well as protecting against hacker attacks aimed at stealing your money, Kaspersky Small Office Security helps you keep your employees more productive by regulating their web access and setting controls on when they can surf or message. Advanced security features like encryption assure your customers that their data is safe in your hands, increasing your sales potential and customer satisfaction.

* Effective for 32 bit applications only. Includes Android and iOS devices.

WHY CHOOSE KASPERSKY LAB BUSINESS SOLUTIONS?

- We're a technology-driven company from top to bottom – starting with our CEO, Eugene Kaspersky.
- Our Global Research & Analysis Team (GReAT), an elite group of IT security experts, have been the first to uncover many of the world's most dangerous malware threats and targeted attacks.
- Many of the world's most respected security organisations and law enforcement agencies have actively sought our assistance.
- Since Kaspersky Lab develops and perfects all of its own core technologies in-house, our products are naturally more stable and more efficient.
- Each year Kaspersky Lab participates in more independent tests than any other vendor – and we come top in a much higher percentage of tests than any other vendor!
- The most widely respected industry analysts – including Gartner, Inc, Forrester Research and International Data Corporation (IDC) – rate us as a Leader within many key IT security categories
- Over 130 OEMs – including Microsoft®, Cisco® Meraki, Juniper Networks, Alcatel Lucent and more – use our technologies within their own products and services.

That's what makes the difference!

KASPERSKY LAB WORLDWIDE

Kaspersky supports local and global businesses from offices throughout the world. To find out more about how to buy Kaspersky Security for Business solutions, please contact your local partner.

www.kaspersky.com.au

APAC

Australia
China
Hong Kong
India
Korea
Malaysia

Europe

Austria
France
Germany
Italy
Netherlands
Portugal
Spain
Norway
Switzerland
United Kingdom

Emerging Markets

Latvia
Poland
Romania
Slovenia
South Africa
Turkey
Ukraine
United Arab Emirates

Japan

Japan (Tokyo)

North America

Canada
United States of America (Boston)
United States of America (Miami)

Russia and CIS

Russia
Kazakhstan

Contact us on **1300 930 655**
or email **anz_sales@kaspersky.com**

Twitter.com/
Kaspersky

Facebook.com/
Kaspersky

Youtube.com/
Kaspersky

Kaspersky Lab, Australia and New Zealand
www.kaspersky.com.au

All about Internet security:
www.securelist.com

Find a partner near you:
www.kaspersky.com/au/buyoffline

© 2015 Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners. Mac is a registered trademark of Apple Inc. Cisco and iOS are registered trademarks or trademark of Cisco Systems, Inc. and/ or its affiliates in the U.S. and certain other countries. IBM and Domino are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. Microsoft, Windows, Windows Server, Forefront and Hyper-V are registered trademarks of Microsoft Corporation in the United States and other countries. Android™ is a trademark of Google, Inc.

Catalog_SP1/Feb15/Global/ANZ

KASPERSKY lab