▶ KASPERSKY BUSINESS PRODUCTS 2013

See. Control. Protect.

KASPERSKY^{lab}

▶ ABOUT KASPERSKY LAB

Kaspersky Lab is the world's largest independent security software company. We provide the best possible IT security for your organization through a combination of powerful anti-malware protection, flexible control tools, encryption technology and systems management tools. Kaspersky security extends from the endpoint to your servers and gateways, and our unique integrated design approach means you can secure and control all your physical, virtual and mobile devices from a single central management console, whatever the size of your infrastructure. Kaspersky technology is also used worldwide inside the products and services of industry-leading IT manufacturers and publishers.

▶ THE INDUSTRY'S ONLY TRULY INTEGRATED SECURITY PLATFORM

ONE CONSOLE

Kaspersky products are designed so that, from one 'single pane of glass', the administrator can view and manage the entire security scene — virtual machines, physical and mobile devices alike.

ONE PLATFORM

At Kaspersky Lab, we have developed our own console, security modules and tools in-house rather than acquiring them from other companies. The same programmers working from the same codebase have developed technologies that talk together and work together. The result is stability, integrated policies, useful reporting and intuitive tools.
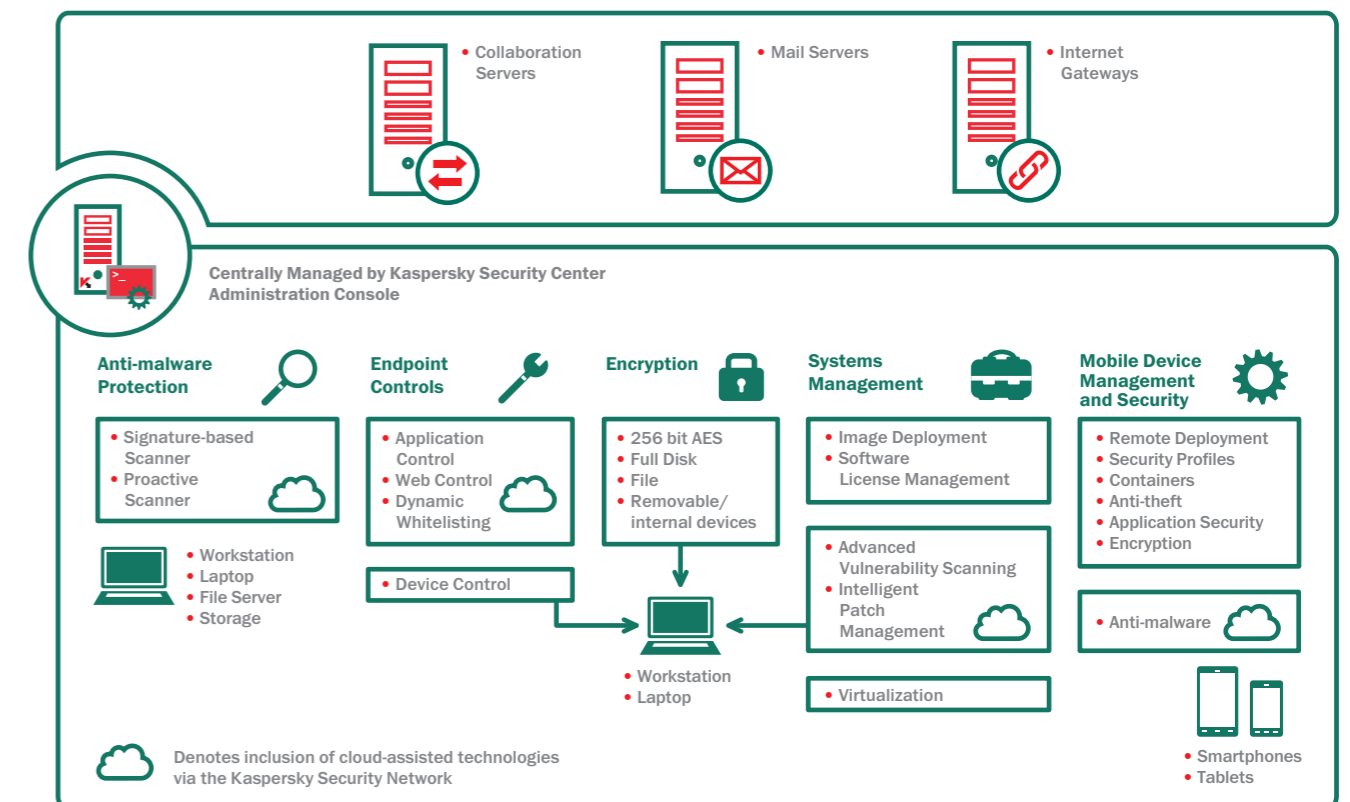
ONE COST

All Kaspersky products and tools are from one vendor, delivered in one installation — so you don't have to go through a new budgeting and justification process every time to bring your security risks in line with your business objectives.

▶ THE RIGHT SOLUTION FOR YOU

Kaspersky Security for Business delivers the right solution for your organization — hether you are looking to protect and control your endpoints (from workstations to smartphones and virtual machines) to secure your servers and gateways, or to remotely manage your entire security environment.

Kaspersky boasts a comprehensive list of technologies, from encryption and mobile device management to patch management and licence inventories. All work seamlessly together, supported by the cloud-based Kaspersky Security Network, to give our customers the world-class protection they need to combat ever more sophisticated and diverse cyber threats.

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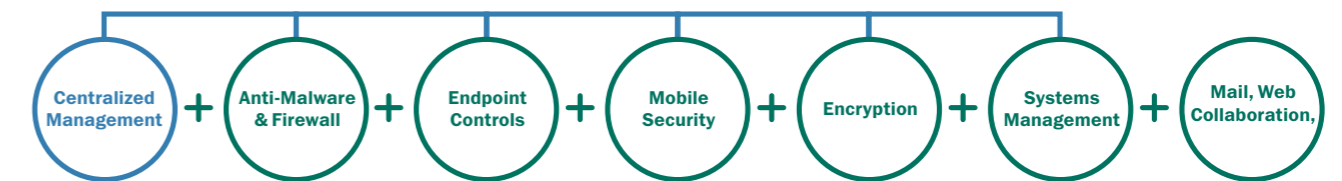

- Collaboration Servers
- Mail Servers
- Internet Gateways

Centrally Managed by Kaspersky Security Center Administration Console

Anti-malware Protection
- Signature-based Scanner
- Proactive Scanner

- Workstation
- Laptop
- File Server
- Storage

Endpoint Controls
- Application Control
- Web Control
- Dynamic Whitelisting

- Device Control

Encryption
- 256 bit AES
- Full Disk
- File
- Removable/internal devices

- Workstation
- Laptop

Systems Management
- Image Deployment
- Software License Management

- Advanced Vulnerability Scanning
- Intelligent Patch Management

- Virtualization

Mobile Device Management and Security
- Remote Deployment
- Security Profiles
- Containers
- Anti-theft
- Application Security
- Encryption

- Anti-malware

- Smartphones
- Tablets

Denotes inclusion of cloud-assisted technologies via the Kaspersky Security Network

► KASPERSKY SECURITY FOR BUSINESS
Our technologies, and how they work together 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 Servers		●	●	●	●	●
Mobile Endpoint Agent		●	●	●	●	●
Mobile Device Management		●	●	●	●	●
Encryption Technology			●	●	●	
OS Image Management			●	●	●	●
License Management			●	●	●	●
Vulnerability Management			●	●	●	●
Patch Management			●	●	●	●
Network Admission Control			●	●	●	●
Collaboration				●	●	●
Mail Servers				●		●
Internet Gateways				●		●
Virtualization					●	●
Storage					●	●

► KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Centralized Management + Anti-Malware & Firewall + Endpoint Controls + Mobile Security + Encryption + Systems Management + Mail, Web Collaboration,

CORE TIER
Starting from a foundation of Kaspersky's award-winning and powerful non-server anti-malware technology and a protective firewall, we add Kaspersky Security Center — our intuitive administration console. For customers who require anti-malware only, this is the solution.

SELECT TIER
Building on the CORE level, we've added **File Server Security, Application Whitelisting and Control, Device Control and Web Control** to the protection roster. Also included is a **Mobile Protection Solution** which consists of an **endpoint security agent** and **Mobile Device Management (or MDM)**. If your needs include protecting a mobile workforce and enforcing IT policy, SELECT might be the right tier for you.

ADVANCED TIER
At the ADVANCED tier, Kaspersky adds **data protection** in the form of file or full-disk **encryption.** Another new offering, **Kaspersky Systems Management**, combines security with IT efficiency. This broad set of features includes essential tools allowing the administrator to:

- Create images and deploy systems using the Image Management module.
- Prioritize the treatment of hardware and software vulnerabilities with a powerful combination of Advanced Vulnerability Scanning and Intelligent Patch Management.
- Track license usage and compliance with Software License Management.
- Set data and infrastructure access policies for users and guests with Network Admission Control.
- Deploy and install updates and new software to users remotely from the central console.

KASPERSKY TOTAL SECURITY FOR BUSINESS
Our flagship offering, Kaspersky Total Security for Business, combines all three previous tiers and further enhances your security posture with additional Web, Mail and Collaboration Server protection. This is the perfect solution for organizations with broad security requirements who demand the best protection for each network.
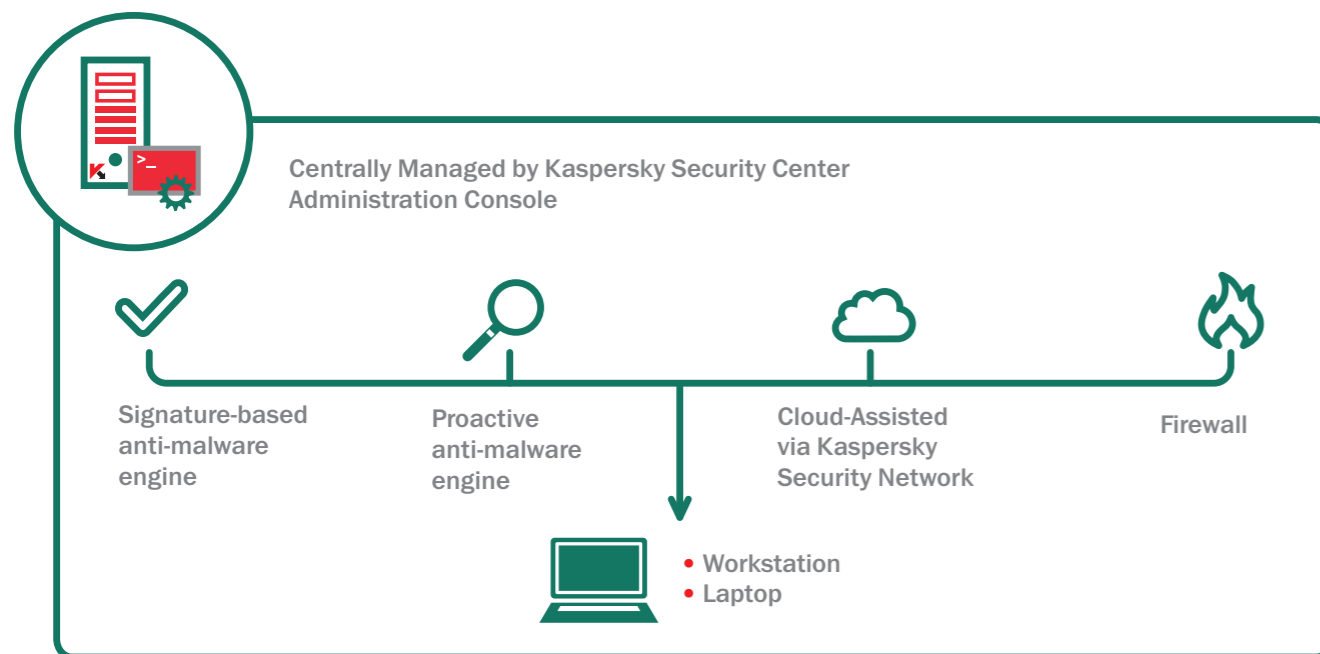
▶ KASPERSKY ENDPOINT SECURITY FOR BUSINESS
Core
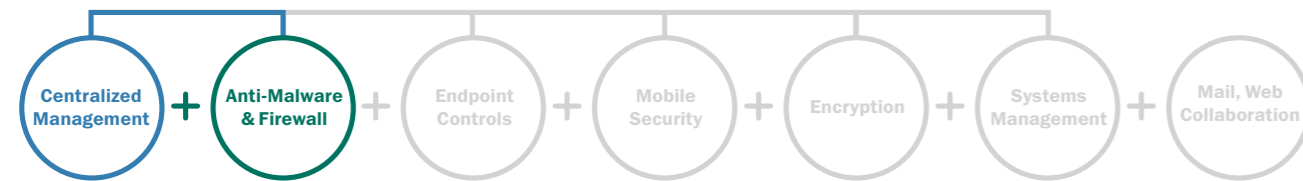
Award-winning anti-malware with centralized deployment, management and reporting.

A layered security model begins with best of breed anti-malware. Because Kaspersky has long been known as the leader in detection and removal of malicious software, there is no better foundation. The Kaspersky Endpoint Security for Business 'Core' tier is centrally managed by the Kaspersky Security Center and is assisted by the cloud-based Kaspersky Security Network.

Kaspersky Endpoint Security for Business Core Tier — Powerful Anti-Malware featuring Cloud-Assisted Protection.

KEY FEATURES:

POWERFUL ENDPOINT ANTI-MALWARE
Kaspersky's scanning engines operate at multiple levels in the operating system, rooting out malware.

CLOUD ENABLED PROTECTION
With the cloud-based Kaspersky Security Network, users are protected in real time against new threats.

CENTRALIZED MANAGEMENT
Administrators can centrally remove existing antivirus software, configure and deploy Kaspersky, and perform reporting — all from the same console.

ENDPOINT ANTI-MALWARE FEATURES:

FREQUENT UPDATES AND SIGNATURE-BASED PROTECTION
Industry-proven traditional signature-based method for detecting malware threats.

BEHAVIORAL ANALYSIS PERFORMED BY SYSTEM WATCHER
The Kaspersky Security Network (KSN) provides a response to suspected threats, much faster than traditional methods of protection. KSN's response time can be as little as 0.02 seconds!

HOST-BASED INTRUSION PREVENTION SYSTEM (HIPS) WITH PERSONAL FIREWALL
Predefined rules for hundreds of the most commonly used applications reduce time spent on configuring the firewall.

BROAD PLATFORM SUPPORT
Kaspersky offers endpoint security for Windows®, Macintosh® and Linux®, easing the workload of the administrator supporting diverse networks.

KASPERSKY SECURITY CENTER FEATURES:

ONE CENTRAL CONSOLE
For remote management of all your Kaspersky protected endpoints.

INTUITIVE USER INTERFACE
Clear, actionable information in an uncluttered dashboard allows administrators to view real-time protection status, set policies, manage systems and obtain reports.

WEB INTERFACE
Remotely monitors protection status and reports on key events from an accessible interface.
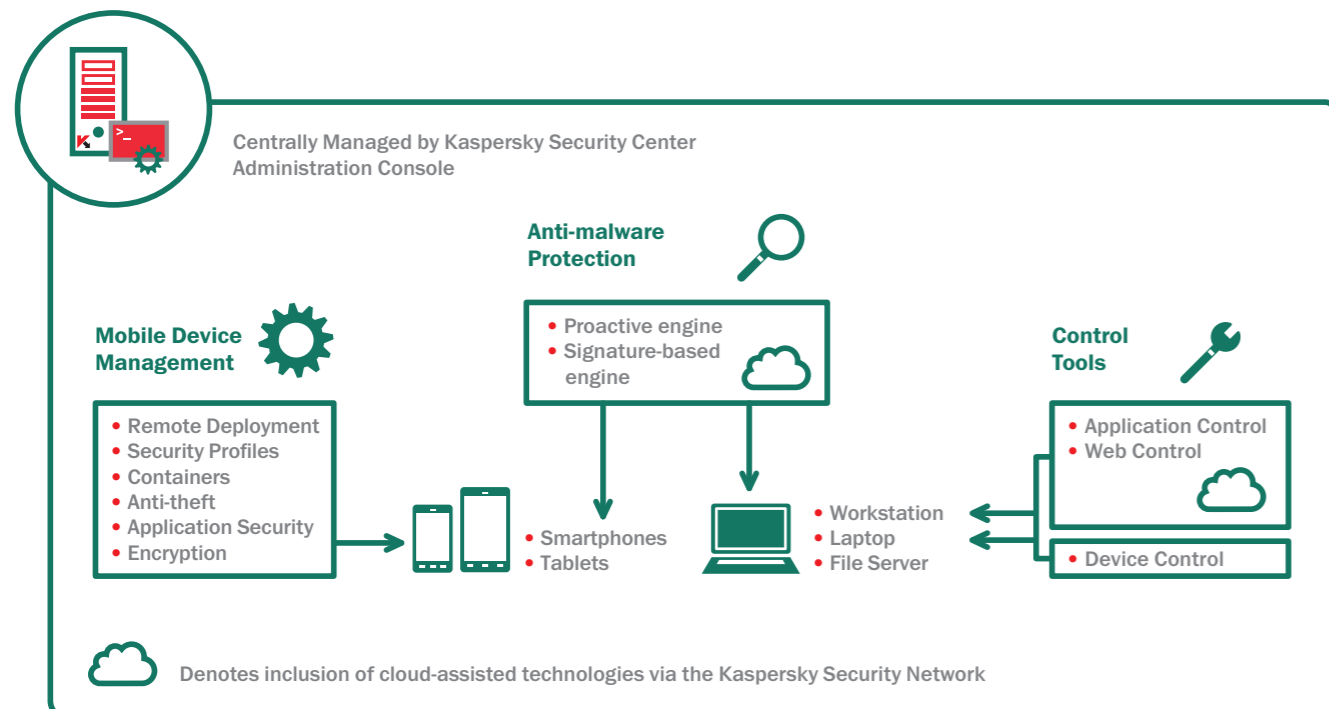
SCALABLE SUPPORT
Whatever your infrastructure size, Kaspersky Security Center offers deployment and management tools, flexible policy options and robust reporting to meet your growing needs.

► KASPERSKY ENDPOINT SECURITY FOR BUSINESS
Select

Centralized Management + Anti-Malware & Firewall + Endpoint Controls + Mobile Security + Encryption + Systems Management + Mail, Web Collaboration

Tools to enable a mobile workforce, ensure IT security policy conformity and block malware.

Kaspersky's 'Select' tier includes mobile device deployment and protection via Mobile Device Management (MDM) and mobile anti-malware. Endpoint control tools (web, device and application) help your organization enforce IT policy, keeping the essential elements of your IT environment secure.

Centrally Managed by Kaspersky Security Center Administration Console

Mobile Device Management
- Remote Deployment
- Security Profiles
- Containers
- Anti-theft
- Application Security
- Encryption

Anti-malware Protection
- Proactive engine
- Signature-based engine

- Smartphones
- Tablets

- Workstation
- Laptop
- File Server

Control Tools
- Application Control
- Web Control
- Device Control

Denotes inclusion of cloud-assisted technologies via the Kaspersky Security Network

Kaspersky Endpoint Security for Business — Select Tier. Featuring Control tools and Mobile Security.

KEY FEATURES:

POWERFUL ENDPOINT ANTI-MALWARE
Kaspersky's 'best of breed' scanning engine operates at multiple levels in the operating system, rooting out malware. The cloud-based Kaspersky Security Network (KSN) protects users in real time against new threats.

FLEXIBLE, GRANULAR CONTROL TOOLS
A cloud-based, categorized database of safe and unsafe applications and websites helps the administrator to set and enforce policies for applications and web surfing, while granular controls ensure that only specific devices can plug in to machines on the network.

EFFICIENT MOBILE DEPLOYMENT AND SECURITY FOR SMARTPHONES AND TABLETS
Agent-based mobile security is available for Android™, BlackBerry®, Symbian and Windows® Mobile devices. Mobile device policies and software can be securely deployed over the air to these and to iOS devices through Kaspersky MDM.

INTRODUCING IN THIS TIER:

ENDPOINT CONTROLS:

APPLICATION CONTROL
Enables IT administrators to set policies that allow, block or regulate applications (or application categories).

DEVICE CONTROL
Allows users to set, schedule and enforce data policies with removable storage and other peripheral device controls — connected to USB or any other bus type.

WEB CONTROL
Means that endpoint-based surfing controls follow the user — whether on the corporate network or roaming.

DYNAMIC WHITELISTING
Real-time file reputations delivered by the Kaspersky Security Network ensure your approved applications are malware free and help maximize user productivity.

KASPERSKY SECURITY FOR MOBILE:

INNOVATIVE ANTI-MALWARE TECHNOLOGIES
Combined signature-based, proactive and cloud-assisted detection results in real-time protection. A safe browser and anti-spam increase the security.

DEPLOYMENT WITH OVER THE AIR (OTA) PROVISIONING
The ability to pre-configure and deploy applications centrally using SMS, email and PC.

REMOTE ANTI-THEFT TOOLS
SIM-Watch, rRemote Lock, Wipe and Find all prevent unauthorized access to corporate data if a mobile device is lost or stolen.

APPLICATION CONTROL FOR MOBILE DEVICES
Monitors applications installed on a mobile device according to the pre-defined group policies. Includes a "Mandatory Application" group.

SUPPORT FOR EMPLOYEE OWNED DEVICES
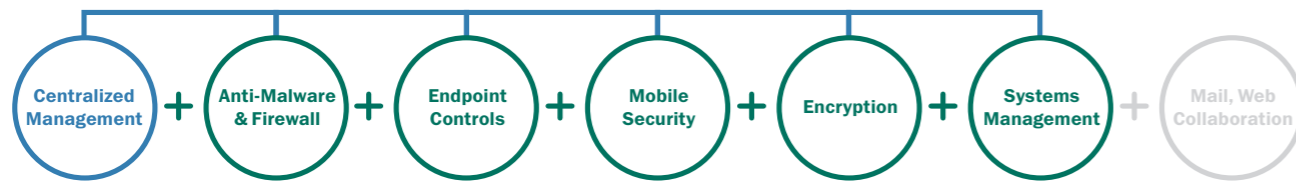Corporate data and applications are isolated in encrypted containers which are transparent to the user. This data can be wiped separately.

▶ KASPERSKY ENDPOINT SECURITY FOR BUSINESS
Advanced

Security tools combined with IT optimization features abound in this valuable array of solutions from Kaspersky Lab.

Kaspersky's Advanced tier delivers the protection and management solution your organization needs to enforce IT policy, keep users free from malware, prevent data loss, and enhance IT efficiency.
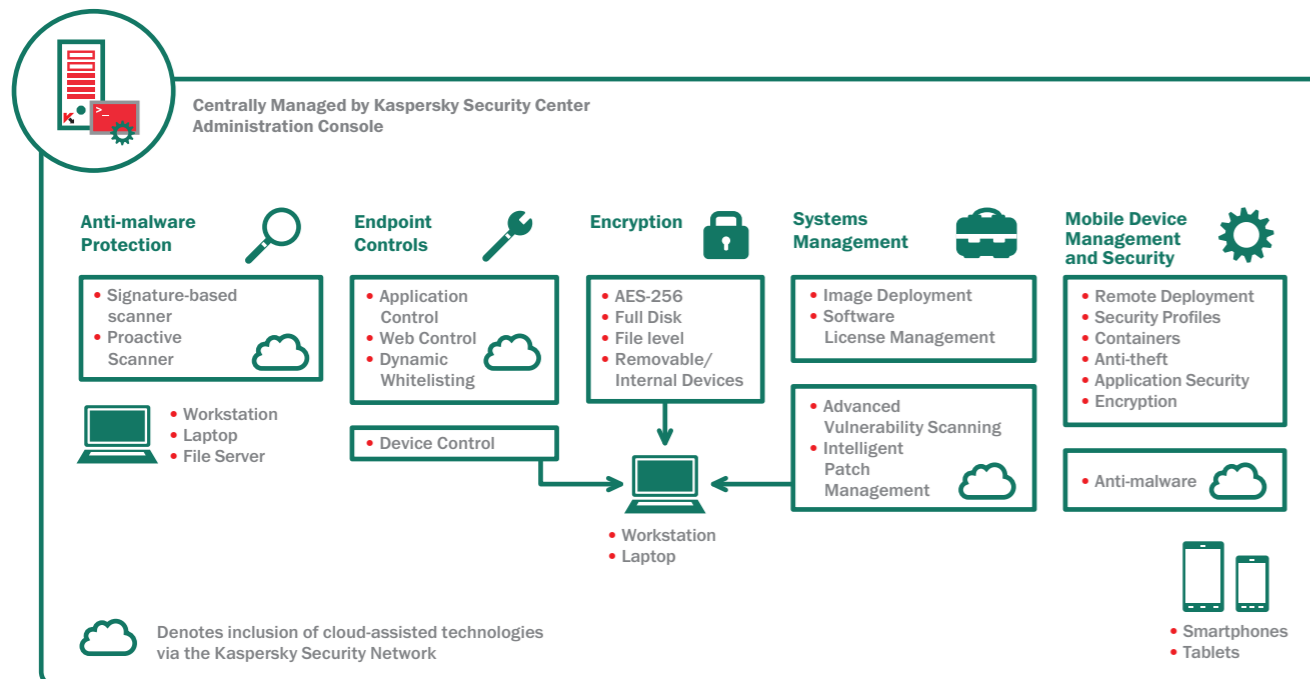
Kaspersky Endpoint Security for Business — Advanced Tier. Featuring Encryption Technology and Security Systems Management.

KEY FEATURES:

POWERFUL ENCRYPTION TECHNOLOGY
Full disk and folder level AES 256-bit encryption protects lost or stolen data, and allows secure data sharing via removable devices, email, network or web, all with transparency to the user.

SYSTEMS CONFIGURATION AND PATCH MANAGEMENT
Operating systems image creation and deployment, vulnerability scanning, automated patch management, Network Admission Control, inventories and license management combine to provide a fully integrated toolkit administered through a single, user-friendly central console.

MOBILE DEPLOYMENT AND SECURITY FOR SMARTPHONES AND TABLETS
Agent-based mobile endpoint security, and remote device and software policy management through Kaspersky MDM.

POWERFUL ENDPOINT ANTI-MALWARE AND FLEXIBLE CONTROLS
Kaspersky's cloud-assisted 'best of breed, anti-malware and granular applications, web and device control tools.

INTRODUCING IN THIS TIER:

ENCRYPTION AND DATA PROTECTION:

COMPREHENSIVE ENCRYPTION
Choose from full-disk or file level , backed by Advanced Encryption Standard (AES) with 256 bit encryption, to secure critical business information in the event of device theft or loss.

SECURE DATA SHARING
Create encrypted and self-extracting packages to ensure data is protected when sharing via removable devices, email, network or web.

SUPPORT FOR REMOVABLE DEVICES
Increases your security through policies that enforce the encryption of data on removable devices.

TRANSPARENCY FOR END-USERS
Kaspersky's encryption solution is seamless and invisible to users, and has no adverse impact on productivity. No impact on application settings or updates, either.

SYSTEMS CONFIGURATION AND PATCH MANAGEMENT:

PATCH MANAGEMENT
Advanced in-depth scanning for vulnerabilities combined with the automated distribution of patches.

OPERATING SYSTEM AND APPLICATION IMAGE DEPLOYMENT
Easy creation, storage and deployment of system images from a central location. Perfect for a migration to Microsoft® Windows® 8.
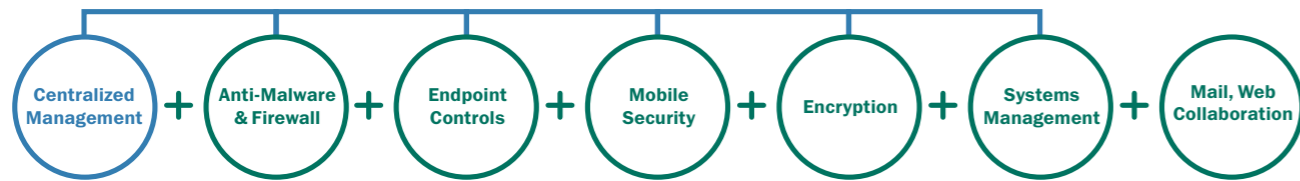
REMOTE DEPLOYMENT OF SOFTWARE
Central deployment of software to client machines, even to branch offices.

NETWORK ADMISSION CONTROL (NAC)
With Network Admission Control (NAC), you can create a network 'guest' policy. Guest devices (including mobile devices) are automatically recognized and sent to a corporate portal where the correct identification password enables them to use the resources you've approved.

HARDWARE, SOFTWARE AND LICENSE CONTROL
Hardware and software inventory reports help keep control over software license obligations. So you can save on costs by centrally provisioning software rights.

▶ KASPERSKY
TOTAL SECURITY
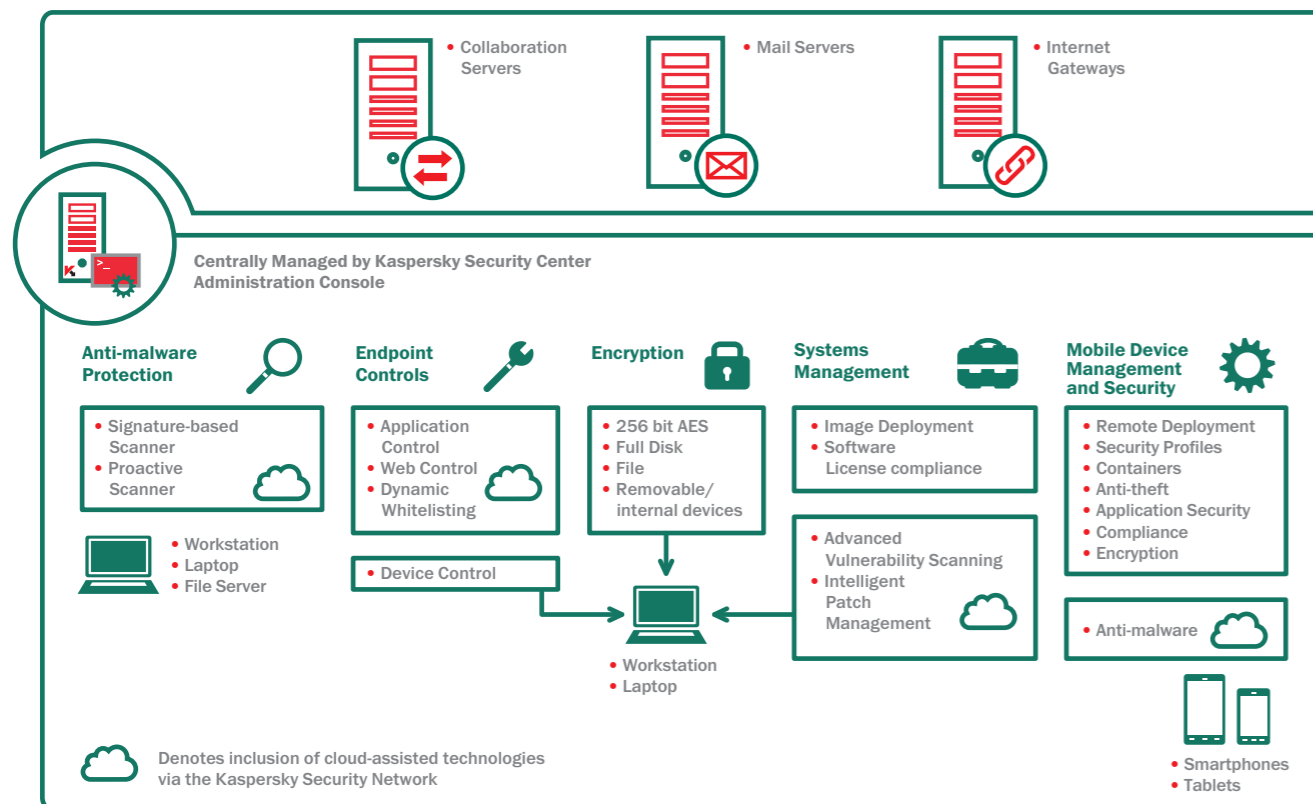# FOR BUSINESS

Centralized Management + Anti-Malware & Firewall + Endpoint Controls + Mobile Security + Encryption + Systems Management + Mail, Web Collaboration

End-to-end protection against malware, encryption, comprehensive IT efficiency and policy enforcement tools.

Kaspersky Total Security for Business delivers the most complete platform of protection and management offered in the industry today. 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.

- Collaboration Servers
- Mail Servers
- Internet Gateways

Centrally Managed by Kaspersky Security Center Administration Console

Anti-malware Protection
- Signature-based Scanner
- Proactive Scanner

- Workstation
- Laptop
- File Server

Endpoint Controls
- Application Control
- Web Control
- Dynamic Whitelisting

- Device Control

Encryption
- 256 bit AES
- Full Disk
- File
- Removable/ internal devices

- Workstation
- Laptop

Systems Management
- Image Deployment
- Software License compliance

- Advanced Vulnerability Scanning
- Intelligent Patch Management

Mobile Device Management and Security
- Remote Deployment
- Security Profiles
- Containers
- Anti-theft
- Application Security
- Compliance
- Encryption

- Anti-malware

- Smartphones
- Tablets

Denotes inclusion of cloud-assisted technologies via the Kaspersky Security Network

KEY FEATURES:

All the features of the previous three tiers, plus:

MAIL SERVER PROTECTION
Anti-malware and anti-spam protection of mail traffic for all popular mail systems

SECURITY FOR INTERNET GATEWAYS
Ensure secure internet access across the organization by automatically removing malicious and potentially hostile programs in HTTP(S)/FTP/SMTP and POP3 traffic.

COLLABORATION SECURITY
Kaspersky defends your SharePoint® servers against malware, while content and file filtering capabilities help prevent the storage of inappropriate content.

INTRODUCING IN THIS TIER:

MAIL SERVERS:

MAIL TRAFFIC PROTECTION
Protecting mail on the latest versions of major mail and collaboration platforms: Microsoft Exchange, IBM Lotus Domino and Linux-based mail servers.

KSN INTEGRATION FOR ANTI-SPAM
Increases spam detection rate thanks to integration with Kaspersky Lab's cloud-based threat identification engine (KSN).

REDUCED TRAFFIC LOAD
Cloud-enabled, intelligent spam filtering significantly reduces traffic load.

SYSTEM RESOURCE OPTIMIZATION
A new antivirus engine, load balancing of server resources and scan exclusions all reduce the load on your system.

INTERNET GATEWAYS:

HIGH PERFORMANCE
A powerful antivirus engine plus optimized, intelligent scanning technology and load balancing increase performance and reduce the resources needed for virus scanning.

MULTI-PLATFORM SUPPORT
Kaspersky Security for Internet Gateway supports most popular gateways based on the Windows and Linux platforms.

COLLABORATION

ANTI-MALWARE BARRIER FOR SHAREPOINT FARMS
Uses innovative detection technology designed to identify and block malware from attempted uploads or downloads in real time.

CONTENT FILTERING
Helps prevent inappropriate external uploads , enforcing internal communication policies and blocking storage of inappropriate files by file type or text content.

▶ KASPERSKY SECURITY FOR MOBILE

Complete mobile security combining Mobile Device Management (MDM) and Endpoint Security for Mobile Devices.

Kaspersky MDM makes the secure configuration of mobile devices painless and straightforward, while Kaspersky Endpoint Security for Mobile Devices provides the protection you need against today's threats — even on employee owned devices.

DETAILED FEATURES OF KASPERSKY SECURITY FOR MOBILE:

IT EFFICIENCY FEATURES:

SIMPLE CONFIGURATION VIA A SINGLE CONSOLE
Unlike other solutions, Kaspersky Lab allows administrators to use only one console to manage the security of mobile devices, physical endpoints, virtual systems, encryption and policy enforcement tools.

PRIVATE APPLICATION PORTAL
Administrators publish a corporate portal that contains links to approved applications. Users can be limited to only these applications only.

"OVER THE AIR" PROVISIONING
Secures phones remotely by sending either an email or SMS containing a link to the corporate portal where users can download the profile and applications you've approved. Access to data won't be granted until the user has accepted.

SECURE CONFIGURATION
Ensures hardware and software integrity by enabling rooting and jailbreak detection. Other security settings include 'camera disable', forced password and more.

COMPLIANCE AND POLICY ENFORCEMENT
Application control allows the monitoring and control of application usage on the device including 'Default Deny' and 'Default Allow' support.
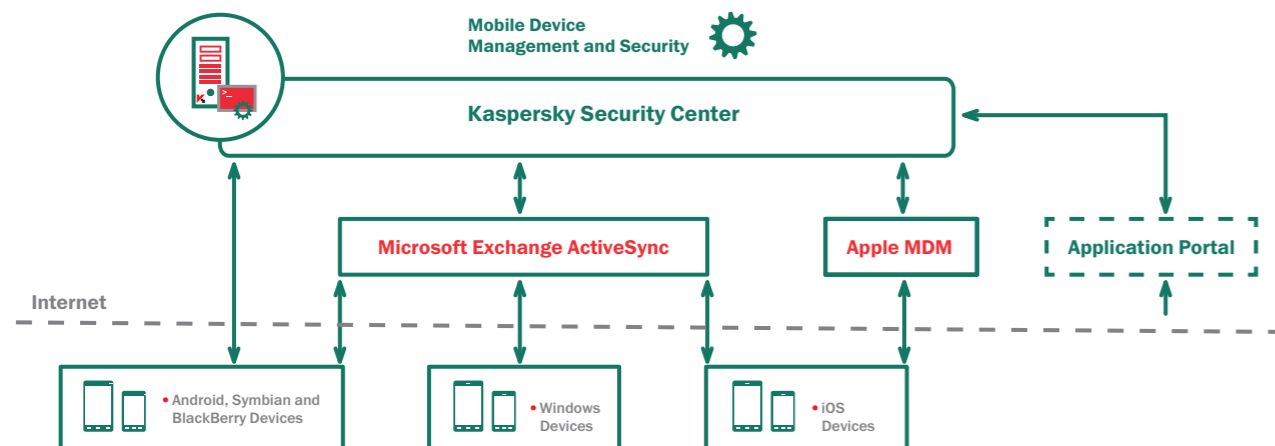
SECURITY RISK CONTROL:

ENCRYPTION
Data in motion is protected via transparent full-disk and file level data encryption which can also be applied to a container.

ANTI-THEFT
Administrators can remotely perform a full or selective device wipe, pinpoint the location of a missing device using GPS "Find" and receive notification if a SIM card is removed or swapped.

MOBILE ANTI-MALWARE
Kaspersky Lab's anti-malware engine features multiple layers of detection including cloud-assisted protection, and combines with a safe browser and powerful anti-spam to ensure the device is not compromised by malicious software.
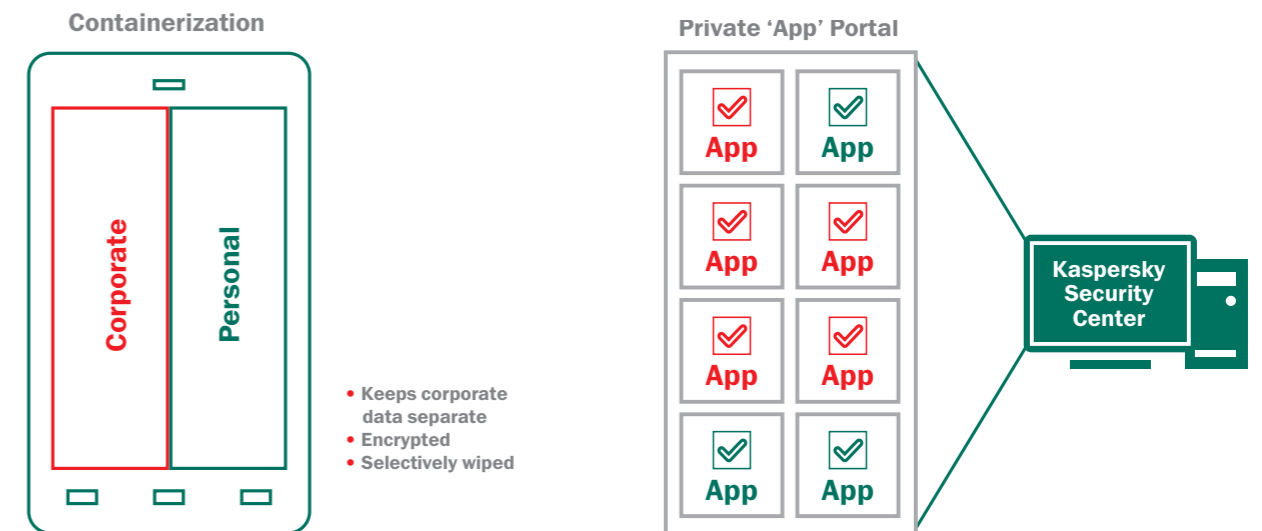
CORPORATE AND PERSONAL DATA INTEGRITY:

CONTAINERS
In support of an employee-owned device scenario, corporate data and applications can be placed in isolated "containers". This provides maximum security for corporate data, and optimal integrity for personal content.

REMOTE DATA SAFETY TOOLS
In the event a device is misplaced, Remote Lock can be engaged. Corporate data within a container on the device can be secured, encrypted, remotely managed and wiped independently of personal data on the device.

Containerization

Corporate | Personal

- Keeps corporate data separate
- Encrypted
- Selectively wiped

Private 'App' Portal

App | App
App | App
App | App
App | App

Kaspersky Security Center

PERFECT FOR "BRING YOUR OWN DEVICE" (BYOD) INITIATIVES

Many employees use their own devices for both personal and corporate tasks. In fact, some organizations encourage workers to choose their preferred smartphone or tablet from a retailer, and IT adds email and corporate access to the employee-owned device.

There are savings and productivity benefits, but BYOD can also open the organization to security risks. Corporate data, improperly secured and potentially co-mingled with personal items, can be easily exploited. Often these devices are also used by family members with no regard for application security. Some are even rooted or jailbroken.

Kaspersky Security for Mobile solves these problems by enabling secure configuration and deployment of smartphones and tablets using the same console as your network security. IT administrators can be confident that user devices are configured with the correct settings and can be secured in the event of loss, theft or user abuse.

Mobile Device Management and Security

Kaspersky Security Center

Microsoft Exchange ActiveSync | Apple MDM | Application Portal

Internet

- Android, Symbian and BlackBerry Devices
- Windows Devices
- iOS Devices

KASPERSKY SYSTEMS MANAGEMENT

Introducing Kaspersky Systems Management. This solution offers a broad set of powerful IT productivity tools written into the same code and managed from one console. The resulting platform provides the simplicity and automation you want — and the security and control you need.

DISPARATE IT TOOLS CREATE COMPLEXITY — AND COMPLEXITY IS THE ENEMY OF SECURITY.

Avoid duplication
Eliminate the duplication of effort involved in setting up individual systems for new and existing users. Using system provisioning technology, disk images can be created, managed and deployed from a central location.

Enhance security
Administrators tell us their days are often filled with ensuring patches are up to date. Kaspersky helps to remove complexity by identifying vulnerabilities that could be immediately exploited and which fixes can be postponed for after-hours. This prioritization helps administrators plan their day and increase their security posture.

Work efficiently
Administrators can remotely install images, updates, patches and applications. If a user has an issue, IT can remotely log in to the machine and troubleshoot the system. This means the administrator isn't wasting time by moving from desk to desk or spending frustrating hours providing less productive phone support.

These features and more are part of Kaspersky Systems Management and are accessed through the Kaspersky Security Center administration console. Because each tool doesn't require its own console, commands are consistent and intuitive, requiring no additional training.

SYSTEMS MANAGEMENT FEATURES:

OPERATING SYSTEM AND APPLICATION PROVISIONING
Easy creation, storage, cloning and deployment of system images from a central location. Ensure systems are delivered to the user without issues and with optimal security settings. This tool is well-suited for migration to Microsoft Windows 8.

STAY ON TOP OF VULNERABILITIES
A one-click hardware and software scan compares results across multiple vulnerability databases, so you can prioritize which vulnerabilities need immediate attention and which you can postpone for after-hours.

REMOTE, FLEXIBLE SOFTWARE INSTALLATION
Minimize network workload by using either manual or scheduled deployments.

REMOTE AGENTS
Assign a workstation in a remote or branch office as a central update agent. Save bandwidth by sending one update to a remote office — and using the assigned local workstation to distribute the update for that location.

SUPPORT FOR WAKE-ON-LAN TECHNOLOGY
For after-hours deployment or support, Kaspersky Systems Management can power-on a workstation remotely.

TROUBLESHOOTING TOOLS
Remotely and securely connect to a client system to fix issues — from the same administrative console.

SUPPORT FOR MICROSOFT WINDOWS SERVER UPDATE SERVICES (WSUS)
Kaspersky Systems Management regularly synchronizes data on available updates and hotfixes with servers, including Microsoft Windows Update, downloading them via Windows Update Services and efficiently distributing them.

NETWORK ADMISSION CONTROL (NAC)
With Network Admission Control (NAC), you can create a network 'guest' policy. Guest devices (including mobile devices) are automatically recognized and sent to a corporate portal where the correct credentials enable them to use the resources you've approved.

HARDWARE AND SOFTWARE INVENTORIES
PCs, hard drives and even removable devices are automatically discovered and inventoried. The introduction of a new device triggers a notification to the administrator. This feature enables the administrator to track the status and usage of hardware on the network.

LICENSE PROVISIONING AND CONTROL
Kaspersky Systems Management reports exactly what software is in use within your environment. This enables you to adjust your licensing costs and identify users who are out of compliance. When deployed with Kaspersky Lab's endpoint control tools, you can limit usage to only approved applications and versions - and restrict the number of licenses in use at any one time.

▶ KASPERSKY SECURITY FOR FILE SERVER

Kaspersky Security for File Server reliably protects servers running Microsoft® Windows®, Novell NetWare and Linux from all types of malicious programs.

Antivirus protection for shared file storage is essential, as a single infected file on a server could infect the workstations of all users of the resource. Proper protection of the file server not only ensures that users and their data are protected, but also eliminates the danger of malicious programs making their way into backup copies of files, which could cause repeated malware outbreaks and other incidents.

PRODUCT HIGHLIGHTS*

- Support for the latest versions of Microsoft® Windows® and Linux platforms
- Optimized usage of system resources
- Support for Hierarchical Storage Management systems (HSM)
- Protection of terminal servers and cluster servers
- VMware Ready certification
- NSS file system support
- Free BSD support

FEATURES

- Protection of file servers running Windows® (including Windows Server® 2008 R2), Linux (including Samba) and Novell NetWare
- Enhanced proactive protection from new malicious programs
- Real-time antivirus protection
- Treatment of active infections
- On-schedule scanning of file storage
- Scanning of critical system areas
- Isolation of infected workstations
- Scalability
- Backup storage of data prior to disinfection or deletion
- Centralized installation, management and updates
- Choice of installation and management methods
- Flexible system of scanning and incident response scenarios
- Application status notification system
- Comprehensive reports on network protection status

APPLICATIONS

- Kaspersky Anti-Virus for Windows® Servers Enterprise Edition
- Kaspersky Anti-Virus for Linux File Server
- Kaspersky Endpoint Security for Windows®
- Kaspersky Anti-Virus for Novell NetWare
- Kaspersky Security Center

▶ KASPERSKY SECURITY FOR MAIL SERVER

Kaspersky Security for Mail Server protects mail and groupware servers from malicious programs and spam.

The product includes applications that protect mail traffic for all popular servers, including Microsoft® Exchange, Lotus® Domino®, Sendmail, Qmail, Postfix, Exim and CommuniGate Pro. The solution can also be used to set up a dedicated mail gateway.

PRODUCT HIGHLIGHTS*

MAIL SERVER PROTECTION
Anti-malware and anti-spam protection of mail traffic for all popular mail systems.

SYSTEM RESOURCE OPTIMIZATION
A new anti-virus engine, load balancing of server resources and scan exclusions all reduce the load on your system.

KSN INTEGRATION FOR ANTI-SPAM
Increases spam detection rate thanks to integration with Kaspersky Lab's cloud-based threat identification engine (KSN).

REDUCED TRAFFIC LOAD
Cloud-enabled, intelligent spam filtering significantly reduces traffic load.

FEATURES

- Integrated protection of mail servers from all types of malicious programs
- Efficient protection against spam
- Real-time antivirus protection
- On-schedule scanning of emails and databases
- Protection for Sendmail, qmail, Postfix, Exim and CommuniGate Pro mail servers
- Scanning of messages, databases and other objects on Lotus® Domino® servers
- Scanning of all messages on the Microsoft® Exchange server, including public folders
- Filtration of messages by attachment type
- Scalability
- Support for Microsoft® Exchange Server 2007 clusters and DAG for Microsoft® Exchange Server 2010
- Backup storage of data prior to disinfection or deletion
- Isolation of infected objects
- Cancellation of repeated mail scanning
- Convenient tools for installation, management and updates
- Comprehensive reports on protection status
- Flexible system of scanning and incident response scenarios
- Application status notification system

APPLICATIONS

- Kaspersky Security for Microsoft® Exchange Servers
- Kaspersky Anti-Virus for Lotus® Domino®
- Kaspersky Security for Microsoft® Exchange Server 2003
- Kaspersky Security for Linux Mail Server

▶ KASPERSKY SECURITY FOR INTERNET GATEWAY

Kaspersky Security for Internet Gateway provides secure Internet access for all employees in an organization.

Kaspersky Security for Internet Gateway supports most popular gateways based on the Windows and Linux platforms. Known malicious and potentially dangerous programs running via HTT P, HTT PS, FT P, POP3 and SMTP protocols are automatically deleted from the data flow. Optimization technology, scalability and support for the latest platforms make it the ideal product for large organizations with huge volumes of traffic.

PRODUCT HIGHLIGHTS*

- Protection of Microsoft® Forefront® TMG
- Wide variety of policy management and configuration tools
- Scanning of VPN-connections

- Email traffic protection (via POP3 and SMTP protocols)
- Scanning of HTTP and FTP traffic from published servers
- VMware Ready certification

FEATURES

- Real-time scanning of internet traffic using HTTP, HTTPS, FTP, POP3 and SMTP protocols
- Integrated protection from all types of malicious programs
- Support for Squid, Blue Coat and Cisco® proxy servers
- Backup storage
- Load balancing of server processors

- Scalability
- Convenient tools for installation, management and updates
- Flexible system of scanning and incident response scenarios
- Comprehensive reports on network protection status

APPLICATIONS

- Kaspersky Anti-Virus for Microsoft® ISA Server and Forefront® TMG Standard Edition
- Kaspersky Anti-Virus for Microsoft® ISA Server Enterprise Edition

- Kaspersky Anti-Virus for Proxy Server

▶ KASPERSKY SECURITY FOR COLLABORATION

Kaspersky Security for Collaboration applies the latest in protection technologies to your Collaboration platform, combining ease of management and high malware detection rates.

Kaspersky Security for Collaboration uses Kaspersky's award-winning antivirus engine to protect Microsoft® SharePoint® environments. With award-winning malware detection technology, the product can protect a single server or entire SharePoint farms — while its content and file filtering capabilities help prevent storage of inappropriate content.

FEATURES

- Innovative malware detection technology is designed to identify and block threats from attempted uploads or downloads in real time
- Prevents end users from storing specified types of files, (e.g. music, video, executable files) or files with inappropriate text
- Global management settings can be configured on all protected servers from a single dashboard
- Simple, intuitive management — no special training needed
- Integration with Active Directory streamlines setup and user authentication
- Detailed logs and backup of modified files help support administrators responding to violations or security issues
- Detailed, flexible reporting
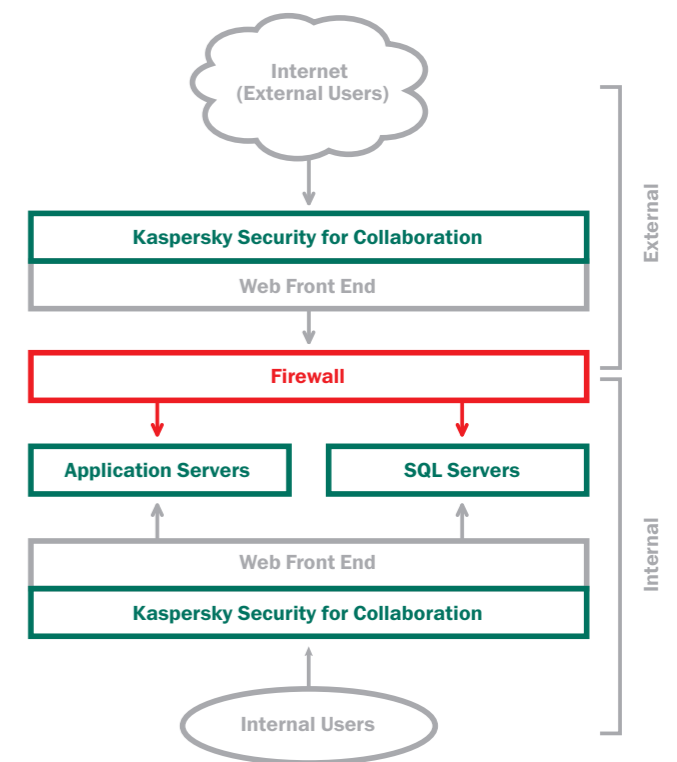
▶ KASPERSKY SECURITY FOR VIRTUALIZATION

Kaspersky Security for Virtualization – built for the unique requirements of virtualized IT environments — delivers award-winning anti-malware protection for virtualized servers, desktops and data centers.

Kaspersky Security for Virtualization is an agentless anti-malware solution that provides a more efficient way to protect your virtualized infrastructure — with greater performance and less impact on virtualization density. The application is easy to deploy and includes advanced management features that simplify a wide range of security tasks — across both physical and virtual computing assets.

PROTECTION AND PERFORMANCE FEATURES

- **Centralized security.** Kaspersky Security for Virtualization is a virtual appliance that plugs into VMware's vShield Endpoint – to deliver anti-malware scanning capabilities. It provides a single, centralised anti-malware engine and database for each physical host.

- **Advanced Antivirus Engine.** Kaspersky's award-winning anti-malware technologies — together with Kaspersky's industry-leading frequency of updates — help to protect against new and emerging threats. A heuristic analyzer combats polymorphic malware.

- **Automatic Protection.** New virtual machines are automatically provided with anti-malware protection — to help eliminate security gaps and misconfigurations. Any guest VM is always protected with the latest signature database regardless of whether a VM was previously off line.

- **Higher density virtualization.** Because Kaspersky Security for Virtualization is an agentless solution, it helps to eliminate 'Update Storms' and 'Scan Storms', achieve higher density virtualization, reduce impact on performance and address security gaps that can be introduced by some agent-based products.
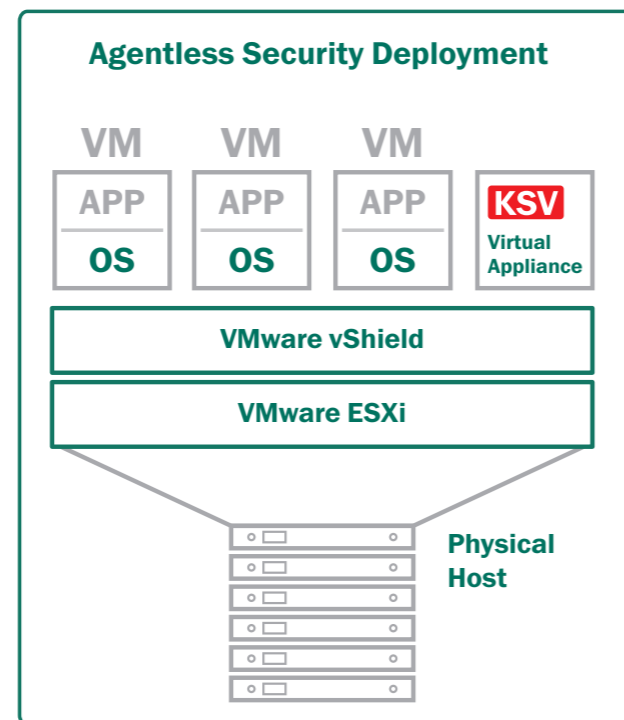
Kaspersky Security for Virtualization provides agentless antivirus for VMware deployments.

## MANAGEMENT FEATURES:

SINGLE MANAGEMENT CONSOLE.
Kaspersky Security Center — which is available at no additional cost — is a single management console that lets you manage the security of virtual machines, physical machines and mobile devices.

SUPPORTS VMWARE VMOTION.
By fully supporting VMware vMotion, Kaspersky Security for Virtualization ensures that protection is not interrupted when a workload is moved from one ESXi host to another. Provided the new host has the necessary licenses, the protection will follow the workload and all security settings will remain the same.

INTEGRATED WITH VMWARE VCENTER.
Kaspersky Security for Virtualization receives information about virtual machines from vCenter — including a list of all virtual machines and relevant parameters. In addition to giving the IT team better visibility, this integration with vCenter ensures that protection is automatically provided whenever a new virtual machine is configured.
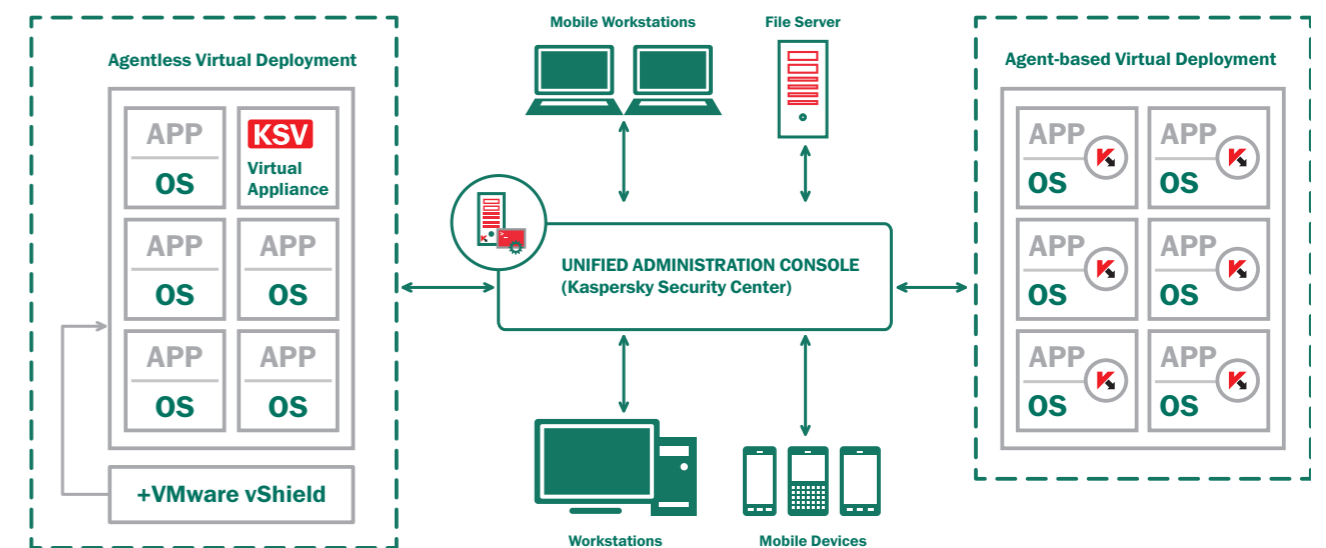
▶ KASPERSKY ANTI-VIRUS FOR STORAGE

Kaspersky Anti-Virus for Storage protects the EMC Celerra family of network storage products from all types of malware.

Data storage systems on a network provide employees working in organizations of all sizes with fast and easy shared access to information. However, if a corporate network is unprotected, access to shared files can lead to some very undesirable consequences. A single infected file stored on a system may compromise the entire network, potentially causing substantial business, financial and reputational damage. That is why comprehensive protection for network storage systems is absolutely essential.

Kaspersky Anti-Virus for Storage is fully compatible with the EMC Celerra range of products. It has been expertly designed to provide them with the highest levels of protection, detecting and neutralizing malware from files and archives stored in Celerra systems. The solution allows administrators to configure the system to perform scanning tasks in real-time as objects are saved and modified, or on-demand if required.

FEATURES

- Protection for EMC Celerra data storage systems
- Support for Windows Server® 2008 R2
- Support for Hierarchical Storage Management systems (HSM)
- Enhanced proactive protection from new malicious programs
- Real-time antivirus protection
- On-schedule scanning of file storage
- Scanning of critical system areas
- Optimized usage of system resources
- Backup storage of data prior to disinfection or deletion
- Scalability
- VMware Ready certification
- Centralized installation, management and updates through Kaspersky Security Center
- Integrates fully with the Kaspersky Endpoint Security for Business Platform and other Kaspersky Products
- Application status notification system
- Comprehensive reports on network protection status

KASPERSKY lab