

KASPERSKY LAB

---

Kaspersky™ Corporate Suite

**ANTI-VIRUS  
SOLUTION**

KASPERSKY CORPORATE SUITE

# Anti-Virus Solution

---

© KASPERSKY LAB LTD

Visit our WEB site: <http://www.kaspersky.com/>

---

# Contents

<b>1. KASPERSKY™ CORPORATE SUITE .....</b>	<b>5</b>
1.1. MAIN FUNCTION OF THE SOFTWARE PACKAGE .....	5
1.2. MAIN FEATURES OF THE KASPERSKY™ CORPORATE SUITE PACKAGE .....	6
1.3. COMPONENTS .....	8
<b>2. PROTECTING WORKSTATIONS.....</b>	<b>9</b>
2.1. KASPERSKY™ ANTI-VIRUS FOR WORKSTATIONS RUNNING WINDOWS 95/98/ME AND WINDOWS 2000/NT/XP (WINTEL). MAIN FEATURES.....	9
2.1.1. <i>Real-time protection</i> .....	9
2.1.2. <i>Filtering viruses out of email</i> .....	9
2.1.3. <i>Comprehensive control over e-mail messages</i> .....	10
2.1.4. <i>Protecting against macro-viruses</i> .....	10
2.1.5. <i>Monitoring data-integrity</i> .....	10
2.1.6. <i>Protecting data storage locations</i> .....	10
2.1.7. <i>Intercepting script-viruses</i> .....	11
2.1.8. <i>Centralized deployment and management</i> .....	11
2.1.9. <i>Automated updating</i> .....	11
2.1.10. <i>Universal boot system</i> .....	11
2.2. KASPERSKY™ ANTI-VIRUS FOR OS/2. MAIN FEATURES .....	12
2.2.1. <i>Two-level anti-virus protection</i> .....	12
2.2.2. <i>Compliant with the most popular OS/2 versions</i> .....	12
2.2.3. <i>User-friendly</i> .....	12
<b>3. PROTECTING FILE SERVERS.....</b>	<b>13</b>
3.1. KASPERSKY™ ANTI-VIRUS FOR WINDOWS 2000/NT SERVER. MAIN FEATURES 13	
3.1.1. <i>Real-time protection</i> .....	13
3.1.2. <i>Centralized deployment and management</i> .....	13
3.1.3. <i>Protecting data storage locations</i> .....	14
3.1.4. <i>Quarantine of dangerous and suspicious objects</i> .....	14
3.1.5. <i>Virus alerts broadcasting</i> .....	14
3.1.6. <i>Automated updating</i> .....	14

3.2.	KASPERSKY™ ANTI-VIRUS FOR NOVELL NETWARE. MAIN FEATURES ...	15
3.2.1.	<i>Full-scale anti-virus protection</i> .....	15
3.2.2.	<i>Integration into Novell Directory Service</i> .....	15
3.2.3.	<i>Centralized deployment and management</i> .....	15
3.2.4.	<i>Real-time configuration update</i> .....	16
3.2.5.	<i>Quarantine of dangerous and suspicious objects</i> .....	16
3.2.6.	<i>Virus alerts broadcasting</i> .....	16
3.2.7.	<i>Automatic disconnection of infected workstations</i> .....	16
3.2.8.	<i>Adjusting of CPU utilization</i> .....	16
3.2.9.	<i>Automated retrieve of updates via the Internet</i> .....	17
3.2.10.	<i>Multithreaded virus scanning</i> .....	17
<b>4.</b>	<b>PROTECTING MAIL SYSTEMS.....</b>	<b>18</b>
4.1.	KASPERSKY™ ANTI-VIRUS FOR MICROSOFT EXCHANGE SERVER. MAIN FEATURES	18
4.1.1.	<i>E-mail anti-virus security</i> .....	18
4.1.2.	<i>Protection of client workstations</i> .....	18
4.1.3.	<i>Comprehensive control over e-mail messages</i> .....	19
4.1.4.	<i>Flexible configuration for personal and public e-mail accounts</i>	19
4.1.5.	<i>Reliable quarantine of dangerous objects and alert broadcasting</i>	19
4.1.6.	<i>Real-time configuration update</i> .....	19
4.1.7.	<i>Centralized management</i> .....	20
4.1.8.	<i>Support for an unlimited number of e-mail accounts</i> .....	20
4.1.9.	<i>User-friendly</i> .....	20
4.2.	KASPERSKY™ ANTI-VIRUS FOR LOTUS NOTES/DOMINO. MAIN FEATURES	20
4.2.1.	<i>Constant protection of e-mail-traffic</i> .....	20
4.2.2.	<i>Comprehensive control over e-mail messages</i> .....	21
4.2.3.	<i>Virus alerts broadcasting</i> .....	21
4.2.4.	<i>Real-time virus neutralization</i> .....	21
4.2.5.	<i>User-friendly</i> .....	21
4.2.6.	<i>Automated updating</i> .....	21
<b>5.</b>	<b>PROTECTING LINUX/UNIX OPERATING SYSTEMS .....</b>	<b>22</b>
5.1.	KASPERSKY™ ANTI-VIRUS FOR LINUX/UNIX OPERATING SYSTEMS. MAIN FEATURES.....	22
5.1.1.	<i>Full-scale anti-virus protection</i> .....	22
5.1.2.	<i>Compliance with the most popular Linux and UNIX versions</i>	23

5.1.3.	<i>Unique combination of the most advanced anti-virus tools for Linux and UNIX</i> .....	23
5.1.4.	<i>Centralized protection of your e-mail systems</i> .....	24
5.1.5.	<i>Easy integration into third-party applications</i> .....	24
5.1.6.	<i>Automated retrieve of updates via the Internet</i> .....	24
5.1.7.	<i>Interactive management system</i> .....	24
<b>6.</b>	<b>KASPERSKY™ CORPORATE SUITE: PROTECTING WEB SERVERS</b>	<b>25</b>
6.1.	KASPERSKY™ WEB INSPECTOR.....	25
6.1.1.	<i>Monitoring changes</i> .....	25
6.1.2.	<i>Improved file analysis</i> .....	26
6.1.3.	<i>Back up</i> .....	26
6.1.4.	<i>Recovery of original content</i> .....	26
6.1.5.	<i>Real-time configuration update</i> .....	26
6.1.6.	<i>Immediate broadcast of warnings</i> .....	26
6.1.7.	<i>User-friendly</i> .....	27
<b>7.</b>	<b>PROTECTING DATA TRAFFIC PASSING THROUGH FIREWALLS</b>	<b>28</b>
7.1.	KASPERSKY™ ANTI-VIRUS FOR FIREWALL.....	28
7.1.1.	<i>Anti-virus solution for the Internet</i> .....	28
7.1.2.	<i>Compliance with all the most popular firewalls</i> .....	29
7.1.3.	<i>Advanced anti-virus technology</i> .....	29
7.1.4.	<i>Transparency of data traffic</i> .....	29
7.1.5.	<i>Reliable quarantine of dangerous objects and alert broadcasting</i>	29
7.1.6.	<i>Centralized management</i> .....	30
7.1.7.	<i>User-friendly</i> .....	30
<b>8.</b>	<b>MANAGEMENT OF ANTI-VIRUS PROTECTION</b> .....	<b>31</b>
8.1.	KASPERSKY™ ADMINISTRATION KIT.....	31
8.1.1.	<i>Remote management of the anti-virus tools</i> .....	31
8.1.2.	<i>Alerts broadcasting</i> .....	32
8.1.3.	<i>Cumulative reporting</i> .....	33
8.1.4.	<i>Isolating infected and suspicious objects</i> .....	33
<b>APPENDIX.</b>	<b>KASPERSKY LAB LTD.</b> .....	<b>34</b>

# **1. Kaspersky™ Corporate Suite**

## **1.1. Main function of the software package**

Kaspersky™ Corporate Suite is developed to provide the full-scale data-protection for corporate networks. Main advantage of this package is that it allows you to develop platform-independent and centrally-managed information security structure successfully protecting corporate networks of any size and complexity (with possible application to the remote sub-networks located overseas) against malicious code and hacker attacks.

Anti-virus software products in Kaspersky™ Corporate Suite provide the reliable control over all virus propagation sources in your system: they are used on workstations (DOS, Windows 95/98/ME, Windows 2000/NT/XP Workstation, OS/2, Linux), file servers (Windows 2000/NT Server, Linux, Novell NetWare, FreeBSD, OpenBSD, BSDi, Solaris) e-mail gateways (MS Exchange Server, Lotus Notes, Sendmail, Qmail, Postfix), CVP compatible firewalls (Check Point FireWall-1) and Web servers. Powerful and easy-to-use network management tools allow for centralized deployment and administration of the data-protection system on your computers and corporate networks.

At Kaspersky Lab, we strive for full and complete customer satisfaction. Kaspersky™ Corporate Suite allows you to create a dependable defense that is fully appropriate and compatible for your network configurations.

## **1.2. Main features of the Kaspersky™ Corporate Suite package**

### **1.       Reliable protection**

When developing a modern enterprise-wide data-security solution the main task is to implement a system with all its components operating trouble-free and in full co-operation. The time-tested reliable and effective Kaspersky™ Corporate Suite components successfully provide reliable anti-virus protection for hundreds of corporations around the world. The highest quality and effectiveness of Kaspersky Lab products is confirmed by numerous certificates received from the world's leading independent research centers and test labs that include: the certificate and the license from the State Technical Committee under the President of Russian Federation; the Checkmark certificate for three levels (Level 1, Level 2, and Trojan) from the West Coast Labs test center; the International Computer Security Association (ISCA) certificate; and the Microsoft Certificate for compatibility with the Windows operating system.

### **2.       Supporting various platforms**

The infrastructure of a modern enterprise is a complex multi-component computing environment that consists of various operating systems and applications operating simultaneously. Regarding this Kaspersky™ Corporate Suite was provided with multi-platform components protecting workstations, file servers, e-mail gateways, firewalls, and Web servers, and supports all the commonly used operating systems.

### **3.       Easy-to-integrate**

Kaspersky Lab strives to completely satisfy demands and to pay attention even to the most insignificant requests of its clients. Kaspersky™ Corporate Suite is developed to operate especially within corporation networks of any size and complexity. Due to application of the most up-to-date development methods the software product can be seamlessly integrated into the existing computing environment and customized to perform specific business tasks. As a result, you receive a complete information security solution that meets your system requirements and specific tasks of your business.

### **4.       Comprehensive protection of a corporate network**

Corporate network protection is successful only when it covers all nodes, data-transmission channels and storage locations. Kaspersky™ Corporate Suite provides comprehensive protection of a corporate network by effectively pro-

tecting workstations, file and mail servers, Web servers, and controlling data traffic passing via e-mail gateways and firewalls. Kaspersky™ Corporate Suite is powered by a unique management tool for advanced administration of the anti-virus system. Kaspersky™ Administration Kit allows for a centralized product deployment and management across the corporate network.

5. State-of-the-art set of anti-virus tools

Kaspersky™ Corporate Suite includes all the advanced tools for fighting against viruses: an anti-virus scanner that checks data storage locations on-demand; an anti-virus monitor that performs real-time virus-check of all files being used; an integrity checker to monitor data integrity on your computers; a unique script-virus background interceptor; a behavior blocker that provides 100% protection against micro-viruses. The combined use of these tools excludes the possibility of virus penetration, making your computing safe and secure. Employment of the Kaspersky™ Corporate Suite-integrated system of heuristic analysis allows you to prevent infection from even unknown viruses.

6. On-time detection of new viruses

Kaspersky Lab provides auto-installable updates for its anti-virus products on the daily basis. The company anti-virus experts monitor the world virus situation twenty-four hours a day. In case a new virus appears, they immediately develop the appropriate cure module and immediately deliver it to customers.

7. Extended services

Kaspersky™ Corporate Suite users may be provided with extended services for the purpose of development of a customized comprehensive data-protection system meeting all requirements of the corporate network. On your request Kaspersky Lab can contribute to inspection and analysis of your corporate network for the purpose of identification of the vulnerable points, to network testing and modification of the anti-virus software to meet the customer requirements, and to finishing of the customized anti-virus protection project. The company experts provide services for installation and setting of the software, and for training of the maintenance staff and users. Users of the Kaspersky Lab products are also provided with round-the-clock technical support by either phone or e-mail in Russian or English.

## 1.3. Components

### *What components the Kaspersky™ Corporate Suite package includes?*

Kaspersky™ Corporate Suite includes the following components:

- Protection for workstations — Kaspersky™ Anti-Virus for Windows 95/98/Me, Windows 2000/NT/XP Workstation, OS/2 and Linux.
- Protection for file servers — Kaspersky™ Anti-Virus for Windows 2000/NT Server, Netware, UNIX (FreeBSD, OpenBSD, BSDi, Solaris) and Linux.
- Protection for mail systems — Kaspersky™ Anti-Virus for Microsoft Exchange, Lotus Notes, Sendmail, Postfix, Exim and Qmail.
- Protection for WEB servers — Kaspersky™ WEB Inspector.
- Protection of data passing through firewalls — Kaspersky™ Anti-Virus for Firewall.
- Protection for pocket computers – Kaspersky™ Anti-Virus for Palm OS.
- Centralized deployment and management of the package components - Kaspersky™ Administration Kit.

## **2. Protecting Workstations**

### **2.1. Kaspersky™ Anti-Virus for workstations running Windows 95/98/Me and Windows 2000/NT/XP (Wintel). Main features**

#### **2.1.1. Real-time protection**

The background virus-interceptor - Monitor permanently resides in your Wintel workstation's memory, checking for viruses in files (including the archived) while they are started, created or copied, and also in the memory of started programs. The program comprehensively controls all the file operations preventing virus attacks.

#### **2.1.2. Filtering viruses out of email**

Kaspersky™ Anti-Virus for Wintel workstations automatically and in real time checks for viruses in all incoming and outgoing messages. Since the program supports all the major e-mail database formats (MS Outlook, MS Outlook Ex-

press, MS Exchange, Eudora, MS Mail, Pegasus Mail, Netscape Mail, JSMail, MIME, The BAT), it reliably protects against viruses in mail message storage locations. The built-in Mail Checker efficiently deletes viruses from e-mail messages, and completely recovers the original contents.

### **2.1.3.    Comprehensive control over e-mail messages**

Kaspersky™ Anti-Virus for Wintel workstations automatically checks for viruses in all elements of incoming and outgoing messages: the message body, embedded OLE objects, attached files (including archived or compressed files) and other messages of any nesting level.

### **2.1.4.    Protecting against macro-viruses**

Kaspersky™ Anti-Virus for Wintel contains special modules controlling macro-instructions that are executed. The unique macro control technology using the concept of behavior blocker allows the program to prohibit macro-viruses from being executed.

### **2.1.5.    Monitoring data-integrity**

Inspector, the Kaspersky™ Anti-Virus for Wintel workstations built-in integrity checker traces all changes on the local computer in background: appearance of new, deletion and modification of existing files and more. The program implements the control by calculating mathematical values known as checksums or CRC values (for Cyclic Redundancy Code) for disk sectors and files, and subsequently checking these against the existing copy of appropriate file/sector. If a virus-incidental action (such as unauthorized changes in a file or the system registry) is detected, the module allows removal of the malicious code and recovery of the original disk contents.

### **2.1.6.    Protecting data storage locations**

The anti-virus Kaspersky™ AV Scanner allows for the comprehensive check of local and network drive contents on-demand. You may run your scanner

manually or schedule its start using Kaspersky™ AV Control Centre included in the package.

### **2.1.7. Intercepting script-viruses**

To protect the user from script-viruses the package uses the built-in Script Checker module that completely solves this problem by integrating itself as a filter in-between the script-virus and its handler. This enables you to check for viruses in any script *before* it is executed.

### **2.1.8. Centralized deployment and management**

Kaspersky™ Anti-Virus for Wintel is completely integrated in the unique system of anti-virus protection management. Kaspersky™ Administration Kit enables you to centrally install and control Kaspersky™ Anti-Virus for NT Server from any (including the remote) computer; to define a timetable and an order in which the modules must be started; to automatically retrieve and enable anti-virus database updates via the Internet; to broadcast notifications on virus attacks; to review virus-check logs on workstations; and control access rights to change the program configuration.

### **2.1.9. Automated updating**

The Kaspersky™ AV Updater module allows for automated updating of anti-virus databases containing virus and remedy definitions, and of the software package components.

### **2.1.10. Universal boot system**

The product contains the built-in Rescue Disk Set module – a boot system that allows you to restore your PC at work in case it has been completely disabled as the result of a virus attack. Rescue Disk Set creates a set of Linux-based bootable diskettes with pre-installed Kaspersky™ Anti-Virus for Linux. This allows you to perform a "clean boot" and to restore infected hard disks with all

the commonly used file systems at once: FAT (DOS), FAT32 (Windows 95/98), NTFS (Windows NT/2000), HPFS (OS/2), EXT (Linux).

## **2.2. Kaspersky™ Anti-Virus for OS/2.**

### **Main features**

#### **2.2.1. Two-level anti-virus protection**

Kaspersky™ Anti-Virus for OS/2 provides your computer with a two-level anti-virus protection. The first level is an anti-virus scanner that may be started on demand or from a third-party scheduler. On the second level, viruses are neutralized with the world's first and only anti-virus monitor protecting all active processes in OS/2 from viruses in real-time. Combined use of these tools allows you full control over all virus propagation sources. The program successfully fights all types of malicious programs, including Internet-worms, Trojans, and computer viruses including viruses that were specially developed for OS/2.

#### **2.2.2. Compliant with the most popular OS/2 versions**

Kaspersky™ Anti-Virus for OS/2 may be used under the most popular versions of this operating system, including Warp, Merlin and Aurora.

#### **2.2.3. User-friendly**

Kaspersky™ Anti-Virus for OS/2 contains the simple and user-friendly Presentation Manager graphic interface. It utilizes the step-by-step method, offering a user recommendations for the next step. Main functions of the program can be activated by the touch of a single key.

## **3. Protecting File Servers**

### **3.1. Kaspersky™ Anti-Virus for Windows 2000/NT Server. Main features**

#### **3.1.1. Real-time protection**

Kaspersky™ Anti-Virus for 2000/NT Server includes a background virus interceptor, Kaspersky™ AV Monitor that permanently resides in the computer memory checking all used files (e.g. when these are opened or closed) in real-time. The module also allows checking-in the memory of running programs right after it is loaded, and also every time you update your anti-virus bases. If the infected memory of a program cannot be disinfected, this program is forced to abort the performance.

#### **3.1.2. Centralized deployment and management**

The product is completely integrated in the unique system of anti-virus protection control that was originally developed in Kaspersky Lab. Kaspersky™ AV Control Centre (client subsystem) and Network Control Centre (network sub-

system) enable you to centrally install and control Kaspersky™ Anti-Virus for NT Server from any (including the remote) computer; to define a timetable and an order in which the modules must be started; to automatically retrieve and enable anti-virus database updates via the Internet; to broadcast notifications on virus attacks and review virus-check logs.

### **3.1.3.    Protecting data storage locations**

The anti-virus Kaspersky™ AV Scanner allows for the comprehensive check of local and network drive contents on-demand or as scheduled. Combined use of Kaspersky™ AV Scanner and Kaspersky™ AV Monitor allows you full control over all virus propagation sources on your network.

### **3.1.4.    Quarantine of dangerous and suspicious objects**

Kaspersky™ Anti-Virus for 2000/NT Server has a special quarantine feature allowing to isolate infected and suspicious objects in a safe place and subsequently move the objects to a quarantine directory defined by a network administrator.

### **3.1.5.    Virus alerts broadcasting**

If Kaspersky™ Anti-Virus detects a virus trying to enter the server, it informs the system administrator and/or a group of users by sending a user-defined alert message to the pre-set addresses.

### **3.1.6.    Automated updating**

The Kaspersky™ AV Updater module allows for automated updating of anti-virus databases containing virus and remedy definitions, and of the software package components.

## **3.2. Kaspersky™ Anti-Virus for Novell NetWare. Main features**

Kaspersky™ Anti-Virus for NetWare is a unique anti-virus solution with a network management system, which is completely integrated in the Novell Directory Service (NDS). The program is a loadable module (NLM) for file and application servers running Novell NetWare. It effectively controls all file operations on a server. If the program detects a virus attack, it is able to efficiently repel it and quickly recover the system.

### **3.2.1. Full-scale anti-virus protection**

Kaspersky™ Anti-Virus for NetWare includes a full set of anti-virus tools: an anti-virus scanner that checks data storage locations and may be started on demand or by schedule; and an anti-virus monitor checking all used files (opened, copied, closed) in real-time. Combined use of these tools allows you to perform full control over all the virus propagation sources on your network.

### **3.2.2. Integration into Novell Directory Service**

Since all the main features of Kaspersky™ Anti-Virus for NetWare are completely integrated in NDS, it enables a network administrator to efficiently manage the program directly from the administrator console (NWAdmin or ConsoleOne).

### **3.2.3. Centralized deployment and management**

The program may be installed on NetWare servers from any workstation running Microsoft Windows NT/2000 within the network. Due to deep integration into the NWAdmin network management systems a network administrator is able to remotely manage Kaspersky™ Anti-Virus for NetWare: to schedule component starts, to change program settings, notification modes and the order of infected files processing, to plan downloading of the anti-virus database updates and etc.

### **3.2.4. Real-time configuration update**

To apply the changes you have made to the program settings, you do not need to restart the server. They will be activated right after you have confirmed them.

### **3.2.5. Quarantine of dangerous and suspicious objects**

Kaspersky™ Anti-Virus for NetWare has a special quarantine feature allowing to isolate infected and suspicious objects in a safe place and subsequently move the objects to a quarantine directory defined by the system administrator.

### **3.2.6. Virus alerts broadcasting**

If Kaspersky™ Anti-Virus detects a virus trying to enter the server, it informs the system administrator and/or a group of users by sending a user-defined alert message to the pre-set addresses.

### **3.2.7. Automatic disconnection of infected workstations**

If a certain workstation sends infected files to the server, Kaspersky™ Anti-Virus for NetWare may temporarily disable further access of this workstation to the server in order to prevent any further distribution of viruses on the network.

### **3.2.8. Adjusting of CPU utilization**

Kaspersky™ Anti-Virus for NetWare provides a comprehensive set of settings allowing the network administrator to adjust the CPU resources dedicated to program use.

### **3.2.9. Automated retrieve of updates via the Internet**

Kaspersky™ Anti-Virus for NetWare supports the automatic downloading and hookup of anti-virus database updates via the Internet. The procedure may be performed on demand or scheduled by a network administrator.

### **3.2.10. Multithreaded virus scanning**

Kaspersky™ Anti-Virus for NetWare now supports multithreaded virus scanning that allows for an unlimited amount of files being scanned simultaneously in real-time. This amount is limited only by the server's hardware configuration. The multithreaded virus scanning essentially increases the overall efficiency of the entire network by simultaneous processing of requests that arrived from many workstations at the same time.

## **4. Protecting Mail Systems**

### **4.1. Kaspersky™ Anti-Virus for Microsoft Exchange Server. Main features**

Kaspersky™ Anti-Virus for Exchange is a centralized anti-virus system for mail servers running Microsoft Exchange Server 5.x and 2000. The program provides centralized anti-virus filtering for the entire local and external e-mail traffic in real-time as well as on a user demand.

#### **4.1.1. E-mail anti-virus security**

Kaspersky™ Anti-Virus for Exchange integrates itself into the mail server as a supplemental module and permanently checks for viruses in all e-mail messages in protected mailboxes and folders.

#### **4.1.2. Protection of client workstations**

Kaspersky™ Anti-Virus for Exchange prohibits infected e-mail from entering the Internet-connected workstations within your corporate network. You may

set the program to delete, block or disinfect the infected messages. Furthermore, if a virus has infected one of your workstations, it is unable to distribute itself, since the program suppresses any attempts of the kind and informs the system administrator about this event.

### **4.1.3.    Comprehensive control over e-mail messages**

Kaspersky™ Anti-Virus for Exchange controls all elements of an e-mail message: the message body, embedded OLE objects, attached files (including archived and compressed files) and other messages of any nesting level.

### **4.1.4.    Flexible configuration for personal and public e-mail accounts**

Kaspersky™ Anti-Virus for Exchange protects all types of mailboxes – personal and public. You may set specific preferences for each separate mailbox or folder.

### **4.1.5.    Reliable quarantine of dangerous objects and alert broadcasting**

You can define your quarantine address where the program will transfer all infected and suspicious objects that have been detected in e-mail traffic. If Kaspersky™ Anti-Virus detects a virus attempting to enter your network, it informs the system administrator(s) by sending a user-defined alert message to the pre-set address(es), reporting the details of the source and current location of the infected object.

### **4.1.6.    Real-time configuration update**

To change the configuration (to update your anti-virus databases, to edit the list of protected mailboxes) you do not need to restart your Kaspersky™ Anti-Virus for Exchange. All changes will be activated right after the system administrator has confirmed them.

### **4.1.7. Centralized management**

The product is completely integrated in MS Exchange Administrator (included in MS Exchange). It enables you to centrally perform full control over Kaspersky™ Anti-Virus for Exchange from any computer; to perform on-demand scan for protected objects and schedule program operating; to control access rights to change the program configuration; and update the list of protected mailboxes. Kaspersky™ AV Control Centre (included in the package) allows you to automatically retrieve and enable anti-virus database updates via the Internet.

### **4.1.8. Support for an unlimited number of e-mail accounts**

Kaspersky™ Anti-Virus for Exchange allows you to protect any number of mailboxes (according to the number of the product licenses you bought).

### **4.1.9. User-friendly**

Kaspersky™ Anti-Virus for Exchange logs all the program activity and virus attack statistics.

## **4.2. Kaspersky™ Anti-Virus for Lotus Notes/Domino. Main features**

Kaspersky™ Anti-Virus for Lotus Notes/Domino is a centralized anti-virus system for Lotus Notes/Domino mail systems operating under Linux and Windows NT.

### **4.2.1. Constant protection of e-mail-traffic**

Kaspersky™ Anti-Virus for Lotus Notes/Domino integrates itself into the mail server as a supplemental module and permanently checks for viruses in the incoming and outgoing e-mail traffic.

## **4.2.2.   Comprehensive control over e-mail messages**

Kaspersky™ Anti-Virus for Lotus Notes/Domino controls all elements of an e-mail message: the message body, embedded OLE objects, attached files (including archived and compressed files) and other messages of any nesting level.

## **4.2.3.   Virus alerts broadcasting**

The program utilizes built-in functions preventing infected messages from being sent with simultaneous broadcasting of alerts to the recipient and the sender of infected message.

## **4.2.4.   Real-time virus neutralization**

Due to the flexible configuration the program allows you to efficiently delete, block, isolate (quarantine) or disinfect malicious codes so the end user will receive only an absolutely virus-free correspondence. Furthermore, if a virus has infected one of your workstations by some other ways except for email, it is unable to distribute itself, since the program suppresses any attempts of the kind and notifies the system administrator about this event.

## **4.2.5.   User-friendly**

The program contains the simple and user-friendly graphic interface that is fully integrated into the Lotus Notes control system. Centralized installation and control over Kaspersky™ Anti-Virus can be performed from the network administrator console using the Lotus Notes/Domino standard features.

## **4.2.6.   Automated updating**

The Kaspersky™ AV Updater module allows for automated updating of anti-virus databases containing virus and remedy definitions, and of the software package components.

# **5. Protecting Linux/UNIX Operating Systems**

## **5.1. Kaspersky™ Anti-Virus for Linux/UNIX Operating Systems.**

### **Main features**

Kaspersky™ Corporate Suite provides anti-virus protection for workstations, file and application servers and mailing systems running Linux and UNIX (FreeBSD, OpenBSD, BSDi, Solaris) operating systems against all types of malicious code.

#### **5.1.1. Full-scale anti-virus protection**

Kaspersky Lab anti-virus programs for Linux/UNIX operating systems allows detection and prevention of malicious programs of all types from entering your network: Internet-worms, Trojans, Java and ActiveX applets and computer viruses including those specially developed for Linux and UNIX platforms.

### 5.1.2. **Compliance with the most popular Linux and UNIX versions**

These Kaspersky™ Corporate Suite components can be used with the most popular versions of Linux for the Intel platform, which uses the NSS library version 1.x. The list includes Red Hat Linux, S.u.S.E. Linux, Linux-Mandrake, Debian GNU/Linux, Black Cat Linux etc. It is also compatible with FreeBSD/BSDi 3.xx and 4.xx. The programs also support FreeBSD (versions 2.x, 3.x, 4.x), OpenBSD (version 2.8), BSDi (versions 3.x, 4.x) and Solaris operating systems.

### 5.1.3. **Unique combination of the most advanced anti-virus tools for Linux and UNIX**

Kaspersky™ Corporate Suite includes a unique set of anti-virus tools for Linux and UNIX operating systems:

- **Anti-virus scanner** – on-demand checks for viruses on hard disks (local and network).
- **Anti-virus daemon**<sup>1</sup> – anti-virus scanner with optimized loading into the system memory. Filters data from viruses in real-time mode.
- **Anti-virus monitor**<sup>2</sup> – client program for anti-virus daemon. In real-time mode, it intercepts file operations (start, opening and initialization of modules) and checks for viruses.

Combined use of these modules allows you to create an anti-virus defense structure, which ideally meets your specific system requirements.

---

<sup>1</sup> full versions of modules are available in the server version only.

<sup>2</sup> full versions of modules are available in the server version only.

### **5.1.4. Centralized protection of your e-mail systems<sup>3</sup>**

Kaspersky™ Corporate Suite includes a ready-made solution to integrate the product into the popular Sendmail, Qmail, Exim and Postfix email systems under Linux, FreeBSD and BSDi operating systems. This is a perfect solution to create your own centralized system that filters e-mail traffic.

### **5.1.5. Easy integration into third-party applications**

The client part of the program is supplied in open source code. It enables you to easily integrate the product into your own applications (for example, into other e-mail or application servers) to perform your specific tasks.

### **5.1.6. Automated retrieve of updates via the Internet**

Kaspersky™ Anti-Virus for Linux includes the Updater module allowing for download and automated installation of the latest anti-virus database updates via the Internet. The function can be performed on demand or fully automatically by means of the built-in event scheduler.

### **5.1.7. Interactive management system**

Kaspersky™ Anti-Virus for Linux has a simple and friendly Tuner-interface that is easy-to-use even for the beginners. It allows definition and editing of all the main settings in Scanner and Daemon profiles.

---

<sup>3</sup> available in the server version only.

## **6. Protecting WEB Servers**

### **6.1. Kaspersky™ WEB Inspector**

Kaspersky™ WEB Inspector is installed directly on the physical Web server. The program checks the integrity of data on the server and traces all changes in real-time and in background. If the program detects any unauthorized changes, it sends notification to a pre-set address(es) and allows for the complete recovery of the original content of your Web server.

#### **6.1.1. Monitoring changes**

Kaspersky™ WEB Inspector is installed on a Web server as a system service and constantly (as a background process) monitors all changes to files that have been created, deleted, or processed etc. The program controls these changes by saving the original file imprints (CRC sums) and subsequently checking files on the server against these imprints.

### **6.1.2. Improved file analysis**

Kaspersky™ WEB Inspector allows for the fastest and the most effective check of your Web server while requiring minimum system resources. Since the program supports most popular formats of executable files (PE EXE (Win32), NE EXE (Win16), MZ EXE (DOS), SYS, COM, OLE2 (Word, Excel и Access), ELF (Linux)), it creates Fast-CRC sums for these files. It increases productivity **by five times** while keeping the highest reliability of data control.

### **6.1.3. Back up**

Kaspersky™ WEB Inspector is able to back up the Web server on a user demand. Contents of the server may be copied onto any data media, including tape, magneto-optical and other storage devices, remote recourses located on the Web server as well as on a remote PC. If your files have been illegally changed, it allows you to perform a full recovery of the originals.

### **6.1.4. Recovery of original content**

If the program detects any changes, it, according to the defined settings (automatically or on demand), recovers the original contents of your Web server.

### **6.1.5. Real-time configuration update**

To update the configuration Kaspersky™ WEB Inspector requires no additional restart. All changes will be activated right after you have confirmed them.

### **6.1.6. Immediate broadcast of warnings**

If the program detects any unauthorized changes to your Web-server content, it immediately sends notification with a detailed report to a pre-set e-mail address (address group).

### **6.1.7.   User-friendly**

Kaspersky™ WEB Inspector logs all program activity and virus attack statistics. The user-friendly interface makes your work with this program simple and easy. All the main actions are performed by a step-by-step method, offering a user recommendations for the next step. Main functions of the program (processing of the contents of server, updating CRC database, creation of report) can be activated by the touch of a single key.

## **7. Protecting Data Traffic Passing through Firewalls**

### **7.1. Kaspersky™ Anti-Virus for Firewall**

Kaspersky™ Anti-Virus for Firewall is a special plug-in module for the centralized filtering of data traffic passing through firewalls supporting Content Vectoring Protocol (CVP).

#### **7.1.1. Anti-virus solution for the Internet**

The major concept of your corporate network anti-virus protection is effective control of the external data traffic. Mostly, the program concentrates on files that are received by users via the Internet and from other networks. In real-time, Kaspersky™ Anti-Virus for Firewall checks for and deletes all types of malicious code from data passing through the firewall and received by HTTP, FTP, SMTP and other protocols.

### **7.1.2.    Compliance with all the most popular firewalls**

Kaspersky™ Anti-Virus for Firewall may be used in any firewall supporting Content Vectoring Protocol (CVP). For example, Check Point Firewall-1 and others.

### **7.1.3.    Advanced anti-virus technology**

Kaspersky™ Anti-Virus for Firewall is based on the world's famous anti-virus kernel used in other Kaspersky Lab products. The program searches for viruses in archived and packed files and e-mail. A powerful heuristic code analyzer and redundant scan feature will protect your network from even unknown viruses.

### **7.1.4.    Transparency of data traffic**

Kaspersky™ Anti-Virus for Firewall provides a user-configurable system of batch communication between the anti-virus plug-in, your firewall, and a client computer. This system allows high transparency of data communication with the highest possible level of protection. In this way, the program excludes unexpected breaks in communication when downloading large files via the firewall.

### **7.1.5.    Reliable quarantine of dangerous objects and alert broadcasting**

You can define the quarantine directory where the program will transfer all infected and suspicious objects that have been detected in the Internet traffic. All detected virus attacks are immediately reported by Kaspersky™ Anti-Virus to the pre-defined e-mail addresses.

## **7.1.6. Centralized management**

The product is completely integrated into Kaspersky™ Administration Kit (included in the package). It enables you to centrally install and control Kaspersky™ Anti-Virus for Firewall from any (including the remote) computer; to schedule starts of the program modules; and to automatically retrieve and enable updates of anti-virus database via the Internet.

## **7.1.7. User-friendly**

Kaspersky™ Anti-Virus for Firewall logs all the program activity and the virus attack statistics. You may change any program setting without needing to restart it. All changes will be activated right after you have confirmed them.

You may install the program on any computer in your corporate network and then integrate it into your firewall. To do this, you just need to add Kaspersky™ Anti-Virus for Firewall to the list of your firewall services.

# 8. Management of anti-virus protection

## 8.1. Kaspersky™ Administration Kit

Kaspersky™ Administration Kit is developed specially for administrators of corporate networks or anti-virus security officers. This is a network toolkit allowing a network administrator to install, to configure and to update the anti-virus software, and also to efficiently and timely deal with virus-outbreaks simultaneously on all the workstations of a corporate network directly from the administrating station.

### 8.1.1. Remote management of the anti-virus tools

The software package allows a network administrator to manage every tool of the corporate anti-virus system without leaving the administrator's station. The remote management is especially important for administrators of large networks covering more than one building or office. Kaspersky™ Administration Kit allows the administrator to

- scan workstations on-demand or at the predefined time. The administrator is able to remotely launch scanning on workstations of the cor-

porate network and to schedule the scanning procedure to be automatically started at a certain point of time.

- automatically update anti-virus databases on workstations. The updating procedure may be performed centrally, in this case you do not need every workstation to connect to the Kaspersky Lab web server. The updating procedure also may be scheduled to start automatically on a regular basis.
- change settings of any workstation on the corporate network in advance. In this program we implemented the so-called Pending application of the new settings. Now, while defining new settings for a workstation the administrator doesn't have to worry whether the workstation is available on the network. It may be simply disconnected at the moment. The settings are defined using their copy stored on the primary server, and are actually applied immediately after the network connection to the workstation is restored.
- detect a virus-outbreak (simultaneous infection of several computers on the network) immediately after it happened. The administrator can customize the anti-virus software to repulse the outbreak.
- remotely install (deploy) anti-virus software on the workstations.



To remotely deploy anti-virus software on the corporate network workstations, the administrator has to download the Kaspersky™ Anti-Virus software on the administrating station (or a dedicated server) only once, and then remotely install it on the corporate network workstations.

### **8.1.2. Alerts broadcasting**

The special notification subsystem allows the administrator to define the list of events to be notified about via email. For example, you may want to be notified about a virus on your network, or about the failure to update virus-definition databases on a workstation.

### **8.1.3. Cumulative reporting**

The network report describes events detected by the anti-virus software on all the protected workstations. You can also request separate reports from workstations, and to be reported on the integrity of the logic network itself.

### **8.1.4. Isolating infected and suspicious objects**

The administrator can centrally store suspicious files, encode them and move to the server quarantine. This enables the administrator to establish the highest level of anti-virus protection for computers, since even if you simply place the infected file into the quarantine location there is still a possibility that it can be restored.

# Appendix.

## KASPERSKY LAB Ltd.

Kaspersky Lab Ltd. is a privately-owned, international, data-security software-development group of companies with offices in Moscow (Russia), Cambridge (United Kingdom) and Pleasanton (United States). Founded in 1997, Kaspersky Lab concentrates its efforts on the development, marketing and distribution of leading-edge information security technologies and computer software.

Kaspersky Lab is one the world leaders in data-security and anti-virus technologies. The Company was the first to develop many features that are now an essential part of all modern anti-virus protection: an external anti-virus database with embedded specialized modules, a search capability within archived and compressed files, integrated anti-virus protection for Linux, etc. In addition to anti-virus software, Kaspersky Lab is committed to the development of general data-security software. Our current product line includes Kaspersky Inspector and Kaspersky WEB Inspector, whose unique capabilities allow users full control over any unauthorized alteration to the file system and content of a Web server.

Upcoming add-on features include Kaspersky Personal Firewall for general workplace defence against any hacker attacks, and Kaspersky Access Control for reliable regulation of user access rights to a computer. Kaspersky Lab's flagship product, known as Kaspersky Anti-Virus (AVP), has been in constant development since 1989, and has been rated consistently by numerous computer magazines and virus research centres as the best anti-virus product on the market.

Kaspersky Anti-Virus covers all reliable methods of anti-virus protection: anti-virus scanners, resident "on-the-fly" virus interceptors, integrity checkers and behavior blockers. Kaspersky Anti-Virus supports all of the most popular operating systems and applications. It provides strong anti-virus defence for mail gateways (MS Exchange Server, Lotus Notes/ Domino, Sendmail, Qmail, and Postfix), firewalls and WEB servers. All Kaspersky Anti-Virus products rely on Kaspersky's own database of over 55,000 known viruses and types of malicious code. The product is also powered by a unique technology combating even future threats: the built-in heuristic code analyzer is able to detect up to 92% of unknown viruses and the world's

only behavior blocker for MS Office 2000 provides 100% guaranteed protection against any macro-viruses.

If you have any questions, comments or suggestions please refer them to our distributors or directly to Kaspersky Lab. We will be glad to advise you on any matters related to our product by phone or e-mail and all your recommendations and suggestions will be thoroughly reviewed and considered.

Technical support	Please find the technical support information at <a href="http://www.kaspersky.com.buyoffline.asp">www.kaspersky.com.buyoffline.asp</a>
General information	WWW: <a href="http://www.kaspersky.com">http://www.kaspersky.com</a> <a href="http://www.viruslist.com">http://www.viruslist.com</a> E-mail: <a href="mailto:sales@kaspersky.com">sales@kaspersky.com</a>