KASPERSKY LAB

Kaspersky™ Anti-Virus Business Optimal

ANTI-VIRUS SOLUTION

KASPERSKY ANTI-VIRUS
BUSINESS OPTIMAL

Anti-Virus Solution

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

Contents

Chapter 1

1. Kaspersky™ Anti-Virus Business Optimal

1.1. Main function of the software package

Real protection for the virtual space. What is Kaspersky™ Anti-Virus Business Optimal?

Kaspersky™ Anti-Virus Business Optimal is one of the latest technological achievements of Kaspersky Lab. The package is developed to provide the full-scale data-protection for small and medium size corporate networks containing up to 100 workstations and mostly using uniform operation systems.

Kaspersky™ Anti-Virus Business Optimal is an optimal set of anti-virus tools that can be configured to meet your specific requirements. Depending on your network configuration and the operating systems you use the package may be supplied with various components. It means that with Kaspersky™ Anti-Virus Business Optimal every customer may choose anti-virus *solution* that ideally meets his (her) specific system requirements while at the same time significantly decreases costs of implementation and use of the anti-virus system.

Anti-virus software products in the Business Optimal package 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, Solaris), file servers (Windows NT Server, Linux, Novell NetWare, FreeBSD, OpenBSD, BSDi) and e-mail gateways (MS Exchange Server, Lotus Notes, Sendmail, Qmail, Postfix, Exim). Powerful and easy-to-use protection management tools allow for centralized deployment and administration of your data-protection system.

Regardless of the components you choose, we provide you with round-the-clock anti-virus technical support by phone and e-mail.

1.2. Components

What components the Kaspersky™ Anti-Virus Business Optimal package includes?

Kaspersky™ Anti-Virus Business Optimal includes the following main components[1]:

- Protection for workstations — Kaspersky™ Anti-Virus for Windows 95/98/Me, Windows 2000/NT/XP Workstation, OS/2[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, Postfix, Exim, Sendmail and Qmail.
- Centralized deployment and management of the package components - Kaspersky™ Administration Kit

The customer is free to order any of the Kaspersky™ Anti-Virus Business Optimal components that will provide comprehensive anti-virus protection of all main elements of his (her) network: workstations, file servers and mail systems.

---

[1] depending on the type of supplied package

[2] Kaspersky™ Anti-Virus for OS/2 is not included in the standard Business Optimal package and may be supplied on additional customer request.

The supplied package may include separate components for the selected operational environments as well as any combination of those three components for different operating systems.

If later you decide to transfer your network to some other platforms or to add new network elements, you may order (*for an extra payment*) corresponding components that will be integrated (*guaranteed*) into your existing copy of Kaspersky™ Anti-Virus Business Optimal[3].

From our retail dealers you may buy the following standard packages of Kaspersky™ Anti-Virus Business Optimal:

1) Kaspersky™ Anti-Virus Business Optimal: Protection for workstations running Windows 95/98/Me, Windows 2000/NT/XP, 5 and 10 licenses.

2) Kaspersky™ Anti-Virus Business Optimal: Protection for file servers running Windows 2000/NT, 1 license.

3) Kaspersky™ Anti-Virus Business Optimal: Protection for file servers running Novell Netware, 1 license.

4) Kaspersky™ Anti-Virus Business Optimal: Protection for file servers running FreeBSD/BSDi/OpenBSD/Solaris, 1 license.

5) Kaspersky™ Anti-Virus Business Optimal: Protection for file servers running Linux, 1 license.

1.3. Information in this book

Issues that we discuss in this documentation.

This book is divided into the following chapters:

[3] For details about how to purchase new components for your existing copy of Kaspersky™ Anti-Virus Business Optimal refer to the local partner of Kaspersky Lab or directly to our company.

Kaspersky™ Anti-Virus Business Optimal	General information about the product, its main function, main components and the description of the book structure
Kaspersky™ Anti-Virus Business Optimal: Protecting Workstations	The list of Kaspersky™ Anti-Virus components that are developed to protect from viruses on workstations: • Kaspersky™ Anti-Virus for workstations running Windows 95/98/Me and Windows 2000/NT/XP (Wintel) • Kaspersky™ Anti-Virus for OS/2. Main features and function.
Kaspersky™ Anti-Virus Business Optimal: Protecting File Servers	The list of Kaspersky™ Anti-Virus components that are developed to protect from viruses on file servers: • Kaspersky™ Anti-Virus for Windows 2000/NT Server, • Kaspersky™ Anti-Virus for Novell NetWare. Main features and function.
Kaspersky™ Anti-Virus Business Optimal: Protecting Mail Systems	The list of Kaspersky™ Anti-Virus components that are developed to protect from viruses in mail systems: • Kaspersky™ Anti-Virus for MS Exchange Server, • Kaspersky™ Anti-Virus™ for Lotus Notes/Domino. Main features and function.

Kaspersky™ Anti-Virus Business Optimal: Protecting Linux and UNIX Operating Systems	The list of the Kaspersky™ Anti-Virus components that are developed to protect from viruses in Linux and UNIX operating systems: • Kaspersky™ Anti-Virus for Linux, • Kaspersky™ Anti-Virus for FreeBSD/BSDi/OpenBSD, • Kaspersky™ Anti-Virus for Sendmail/Qmail, Postfix, Exim. Main features and function.
Appendix. Kaspersky Lab JSC	About Kaspersky Lab. Contact information

Chapter

2

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 Client, 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 in MS Outlook, MS Exchange Client, 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. 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.

2.1.6. 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.

2.1.7. Centralized deployment and management

Kaspersky™ Anti-Virus for Wintel is completely integrated in the unique system of anti-virus protection management. Kaspersky™ Administration Kit (network subsystem) 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.

2.1.8. 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.

2.1.9. 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/XP), 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.

Chapter

3

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.

Chapter

4

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.

Chapter

5

5. Protecting Linux and UNIX Operating Systems

5.1. Kaspersky™ Anti-Virus for Linux/UNIX Operating Systems. Main features

Kaspersky™ Business Optimal 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. Compliancy with the most popular Linux and UNIX versions

These Kaspersky™ Business Optimal 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), Solaris operating systems.

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

Kaspersky™ Business Optimal 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** [4] – anti-virus scanner with optimized loading into the system memory. Filters data from viruses in real-time mode.
- **Anti-virus monitor** [5] – 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.

[4] full versions of modules are available in the server version only.

[5] full versions of modules are available in the server version only.

5.1.4. Centralized protection of your e-mail systems[6]

Kaspersky™ Business Optimal 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.

---

[6] available in the server version only.

Chapter

6

6. Management of anti-virus protection

6.1. 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.

6.1.1. 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.

6.1.2. 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.

6.1.3. 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.

6.1.4. 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.

Technical support	Please find the technical support information at www.kaspersky.com.buyoffline.asp
General information	WWW: http://www.kaspersky.com http://www.viruslist.com E-mail: sales@kaspersky.com