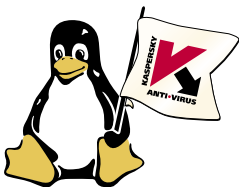
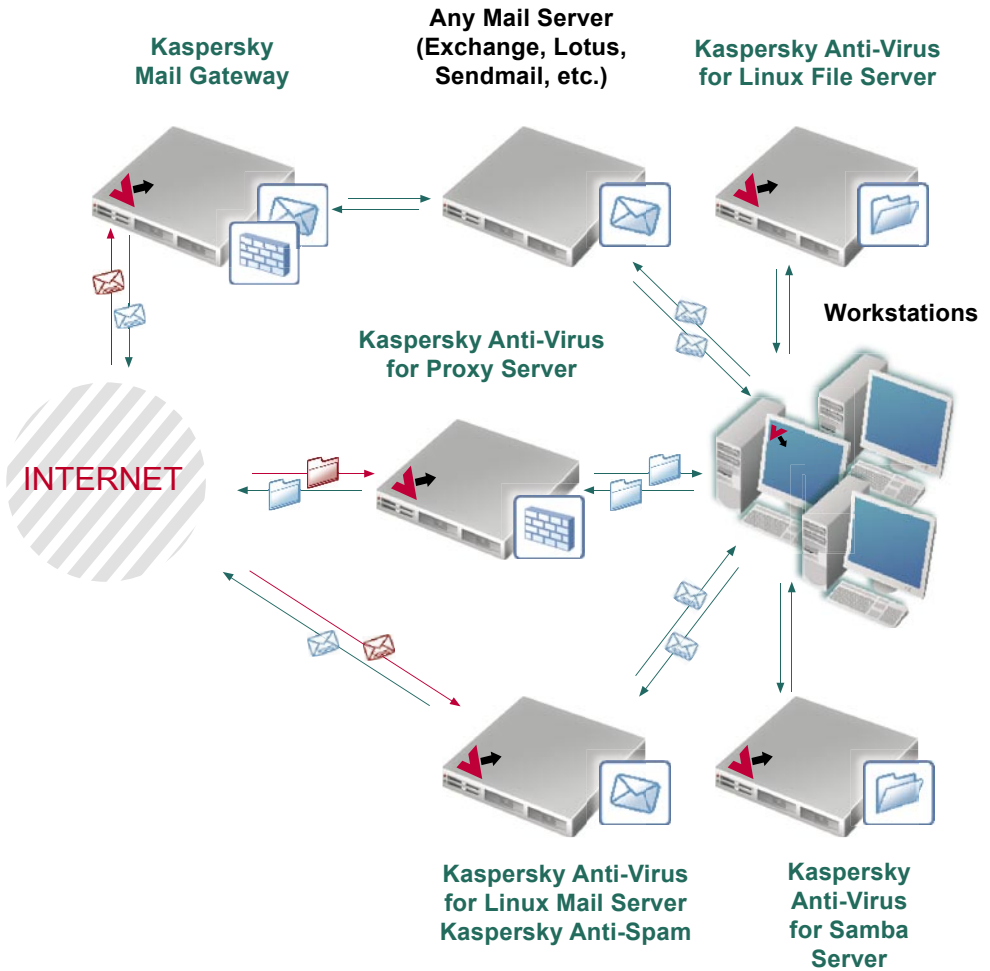


Kaspersky® Linux Security

PRODUCTS

KASPERSKY Lab

Kaspersky Lab Products for Linux



CONTENTS

Kaspersky Lab: an expert in data security	2
Kaspersky Lab in the Linux data security market	3
The Kaspersky® Anti-Virus Engine	4
MAIL PROTECTION	6
Kaspersky® Anti-Virus for Linux Mail Server	8
Kaspersky® Mail Gateway	10
Kaspersky® Anti-Spam	12
WEB PROTECTION	14
Kaspersky® Anti-Virus for Proxy Server	16
FILE SERVER PROTECTION	18
Kaspersky® Anti-Virus for Linux File Server and Workstation	20
Kaspersky® Anti-Virus for Samba Server	22
Services	24
Contact Information	25

Kaspersky Lab: an expert in data security

Kaspersky Lab is an acknowledged leader in developing protection against viruses, spyware, adware, spam and hacker attacks. The company is headquartered in the Russian Federation, with a global network of regional offices and partners.

With more than 16 years' experience in fighting viruses and other IT threats, we at Kaspersky Lab have amassed knowledge and experience that allows us to predict trends in malware development. This is the main advantage we bring to our services and products, and helps us to remain one step ahead of our competitors in offering our customers the best protection possible.

Kaspersky Lab developed many of the technologies which are in place in contemporary antivirus solutions. These technologies are available in our own products, and in those produced by our technology partners F-Secure (Finland), G-Data (Germany), Sybari (US), Blue Coat (US), Clearswift (UK), Astaro (Germany), Alcatel (France), ZyXEL (Taiwan), and BlackSpider (UK).

Kaspersky Lab customers have access to a wide range of additional services guaranteeing complete conformity with all business requirements. We design, implement and support enterprise-wide antivirus solutions. Our customers receive hourly antivirus database updates and we offer our users round-the-clock technical support in several languages.

Kaspersky Lab in the Linux data security market

Most IT networks today are heterogeneous. Linux platforms are frequently used for servers, while most workstations on a company network run under the Microsoft Windows family of operating systems. Linux is one of the most widely recognized operating systems, and its use is becoming the rule rather than the exception.

In early 1999, Kaspersky Lab was one of the first developers to introduce integrated antivirus software for Linux. Today, Kaspersky Lab continues to lead the industry in the development of mail and file server, and workstation protection for Linux platforms, including solutions designed for FreeBSD.

Currently, Kaspersky Lab offers companies a complete line of products that provide full-scale protection of all nodes on a corporate network: antivirus scanning solutions for mail and web traffic, as well as solutions designed to protect file storage areas and that prevent spam. You can find more detailed information about Kaspersky Lab products for Linux at <http://www.kaspersky.com/linux>.

The Kaspersky® Anti-Virus Engine

The heart of any antivirus program is its engine, i.e., the module responsible for scanning objects and detecting malicious programs. How well an antivirus solution detects malicious software and users from new infections depends on the way the antivirus engine is designed and implemented. What makes an antivirus engine effective?

Detection rates

Detection rates measure the thoroughness and speed of detection for new and existing malware. All antivirus vendors declare a high level of malware detection, but this can be objectively evaluated only through independent comparative tests. The Kaspersky® Anti-Virus Engine is an acknowledged leader in terms of detection rates, while false positive rates are close to zero. The independent Austrian antivirus testing lab AV-Comparatives.org, *Virus Bulletin* – a popular UK publication – and the independent German publication *Computerbild* have all confirmed the high quality detection rate of the Kaspersky Anti-Virus Engine.

Coverage

In recent years, spyware, adware, dialers and other malicious programs have grown at an alarming rate. Protection from these programs is essential since they can create significant security and legal risks. Currently, in addition to the award winning detection of viruses, Trojans, backdoors, rootkits and worms, the Kaspersky Anti-Virus Engine provides superior detection of spyware, adware, dialers, key loggers, password stealers and even mobile malicious code.

Response to new threats

Today, when viruses and worms can achieve 100% penetration in less than a few hours, response time to new threats is crucial for effective malware protection. Kaspersky Anti-Virus employs the right level of heuristics to ensure the fastest response to new malware with minimum false positives. Proactive technologies are supported by industry leading signature based technologies that ensure accurate detection and the quickest release of emergency updates. Kaspersky Anti-Virus invariably occupies one of the top places in the industry's most comprehensive response time tests from organizations such as AV-Test.Org, an independent project at the Otto-von-Guericke University, in Magdeburg, Germany.

Antivirus database update frequency and size

To reduce the period during which users are unprotected, antivirus database updates should be released as often as possible and be small enough to ensure convenience and speed. Kaspersky Lab releases database updates hourly - the most frequent in the world with over 700 updates released monthly. During outbreaks, urgent updates are released immediately after a signature has been added to the antivirus databases. Moreover, the average update size is around 30 KB.

Antivirus engine updates

Sometimes it is necessary to update not only the antivirus database, but also parts of the antivirus engine. If an antivirus program does not support quick engine updates, users might be unprotected from new viruses. Kaspersky Anti-Virus database updates can be used to update about 70% of the functionality of the antivirus engine. Support for a new compression or archiving utility can be added in any antivirus update. Therefore, by updating the antivirus databases daily, users receive not only new malware detection signatures, but also updates to the antivirus engine.

Support for compression and archiving utilities

Quite often, virus writers compress malware using several different packers and then release numerous versions of the malware which are essentially the same virus. Antivirus vendors can either spend time on unpacking each variant and releasing numerous updates that require additional end user resources or support for a large number of packers. The Kaspersky Anti-Virus Engine supports more than 1,800 archival and packing formats (as of June 2006). Support for such a large number of formats reduces the time required for analyzing new viruses, resulting in faster response time to new threats. This is especially important for the protection of mail systems, given that a significant number of viruses are sent by email as compressed attachments.

KASPERSKY Lab



MAIL PROTECTION

Kaspersky® Anti-Virus for Linux Mail Server

Kaspersky® Anti-Virus for Linux Mail Server provides effective antivirus protection for corporate mail traffic. The application is integrated as an additional module into the existing mail system and provides real-time scanning of SMTP mail traffic for malicious code.

Kaspersky Anti-Virus for Linux Mail Server scans the server's file systems on demand, and supports the most widely used email solutions, namely Sendmail, Qmail, Postfix and Exim.

FEATURES

Detects and disinfects viruses, spyware and other malware

- Antivirus scanning** All elements of email messages are scanned for malicious code. The application scans for and removes all types of viruses, Trojans, spyware, malicious and potentially hostile programs from incoming and outgoing mail messages and attachments in most formats.
- Customizable notifications** When a suspicious or infected object is detected, the system administrator, sender and recipient of the message receive a message, the contents and format of which are defined by the system administrator. System messages can be sent in any language.
- Quarantine** Infected, suspicious and damaged objects detected in a server's file system or in email traffic can be moved to the quarantine folder, where they will be disinfecting, deleted or stored according to predefined settings.
- Backup copies** Backup storage can be created to store copies of infected objects before they are treated, making it possible to restore if necessary.
- File server scanning** In addition to scanning mail traffic, Kaspersky Anti-Virus for Linux Mail Server offers on demand scanning of the server's file systems. The scanning is performed with the help of iChecker, a check summing technology which significantly reduces the amount of time required for additional scans of each object.

Additional message filtering

By attachment type The application can be configured to filter mail traffic by attachment name and file type and to apply specified processing rules for each category.

By user group Administrators can create user groups, assign individual message processing rules to each group and define user privileges for each group.

Flexible management and administration

Remote administration Kaspersky Anti-Virus for Linux Mail Server can be configured either traditionally, via the application's configuration file, or using the Web interface.

Optimized performance Administrators can monitor mail server load and configure operating parameters to avoid problems in the event of virus or hacker attacks and load peaks. This includes defining timeouts for message receipt or sending, managing the application's queue and limiting the number of objects scanned simultaneously in background mode.

Configuration of updates Antivirus databases can be updated from Kaspersky Lab's servers via the Internet or from local update servers on demand or on schedule. Administrators can choose the type of antivirus databases to be used: standard (detection of true malware only) or extended (databases used to detect potentially hostile software such as spyware, adware and more). Kaspersky Lab antivirus databases are updated hourly.

Graphical reports Administrators can use the Webmin interface to view graphical information on virus activity for selected time periods, as well as data on the types of viruses detected during antivirus scans. Additionally, administrators can receive detailed information about the program's performance using a broad range of reports with predefined levels of detail.

SYSTEM REQUIREMENTS

Hardware requirements

- Intel Pentium class CPU
- At least 32 MB of RAM
- At least 100 MB available space for installation

Software requirements

This program is compatible with the following operating systems:

- Red Hat Enterprise Linux Advanced Server 3
- Red Hat Linux 9.0
- Fedora Core 3
- SuSE Linux Enterprise Server 9.0

- SuSE Linux Professional 9.20
- Debian GNU/Linux 3.0 updated (r4)
- FreeBSD 4.10, 5.3
- Mandrake (Mandriva) Linux 10.1
- OpenBSD 3.6

One of the following mail systems:

- Sendmail 8.x
- Qmail 1.03
- Postfix version not lower than snapshot_20000529
- Exim 4.0

The following additional software is required:

- The which utility – for program installation.
- Webmin program (www.webmin.com); optional version 1.070 or higher is necessary for remote administration of the application.
- Perl version 5.0 or higher (www.perl.org) for Kaspersky Anti-Virus program installation using install.sh

Product version: 5.5

Kaspersky® Mail Gateway

Kaspersky® Mail Gateway is a versatile solution that provides full-scale protection for mail system users against viruses and unsolicited emails (e.g., spam).

Kaspersky Mail Gateway can be installed on a separate server and does not require integration into the existing mail system. The solution significantly increases the level of protection against today's computer threats, making it possible to combine different vendors' antivirus solutions on the same network.

Because it is designed to operate autonomously, the application fits neatly into any environment and combines easily with other vendors' programs installed on other network nodes. Its installation and configuration do not require extensive experience with Linux systems.

FEATURES

Integrated protection from viruses and spam

- Antivirus scanning** The program scans for and removes all types of viruses, and malicious and potentially hostile programs in all elements of incoming and outgoing email messages including attachments.
- Spam filtering** The application scans mail traffic for spam based on formal attributes and analysis of message contents and their attachments using intelligent technologies, including special graphic signatures for detecting spam in the form of images.
- User notification** If a suspicious or infected object is detected, the system administrator, sender and recipient of the message receive a notice, the contents and format of which are defined by the system administrator. If a message is categorized as spam, it can be blocked, sent to a quarantine folder or delivered to the recipient with a special tag in the subject field.
- Quarantine** Infected and suspicious objects and messages identified as spam can be moved to a quarantine folder, where the administrator can view or delete them, or forward them to the end user.

Additional message filtering

- By attachment type** The application can be configured to filter mail traffic by attachment name and file type, helping to immediately identify objects that are likely to contain viruses.
- By user group** The administrator can define separate message processing rules for each group of mail system users by defining limitations in accordance with the security policy and employee needs.

Protection from unauthorized access

The application can be configured to prevent DoS (Denial of Service) attacks and third party attempts to use the server for launching unauthorized mass mailings. In some cases, this helps reduce the server load and increases the processing speed of mail traffic.

Flexible management and administration

Remote administration Kaspersky Mail Gateway can be managed remotely using a web interface, as well as traditionally using the configuration file.

Configuration and optimization of the application Depending upon mail traffic volume and the stringency of the company's security policy, the administrator can change the application's operating parameters from maximum system performance to maximum user protection. The administrator can also configure various timeouts for sending and/or receiving messages, manage the application queue and limit the number of objects that can be scanned simultaneously in the background mode.

Configuration of updates The antivirus database can be updated on demand or automatically according to a predefined schedule from Kaspersky Lab servers on the Internet or from local servers specified by the system administrator. Some modules of the antivirus engine and the linguistic analyzer can be updated as well.

Graphical reports The program includes the capability of viewing virus activity for a given period of time in graphical form. Information regarding the types of viruses detected during antivirus scans can also be viewed. Additionally, the administrator can receive detailed information on the program's status and operation by using a broad range of reports with the desired level of detail.

SYSTEM REQUIREMENTS

Hardware requirements

- Intel Pentium class CPU (Pentium III or Pentium IV recommended)
- At least 256 MB of RAM
- At least 100 MB available HDD space for installation
- At least 500 MB available in the /tmp file system.

Software requirements

This program is compatible with the following operating systems:

- Red Hat Enterprise Linux Advanced Server 4
- Red Hat Linux 9
- Fedora Core 4
- SuSE Linux Enterprise Server 9.0 (SP3)
- SuSE Linux Professional 10.0
- Debian GNU/Linux 3.1r1
- FreeBSD 4.11, 5.4, 6.0
- Mandriva 2006

The following additional software is required:

- Interpreter of the Perl language version 5.0 or higher (www.perl.org)
- The which utility – for program installation
- Webmin version 1.070 or higher (www.webmin.com) to install the remote administration module (optional)

Product version: 5.5

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam protects both users of company mail systems and Internet providers from unsolicited mass mailing or spam.

Kaspersky Anti-Spam helps mail system users eliminate unwanted mail. It employs intelligent spam detection technology, which was developed using Kaspersky Lab's extensive experience in protecting large scale mail systems.

FEATURES

Protection from spam

- List-based filtration** Sender IP addresses are checked against blacklists of spammers, which are maintained by Internet service providers and public organizations (DNS-based Blackhole Lists). System administrators can add addresses of trusted correspondents to a safe list, ensuring that their messages are always delivered without undergoing filtration.
- SPF and SURBL technologies** The filtration process also involves verifying senders using the Sender Policy Framework. Detection of spammer IP addresses using DNSBL is supplemented by SURBL technology (Spam URL Real-time Block List), which can identify spam URLs in the message body.
- Analysis of formal attributes** The program recognizes spam by such typical characteristics as distorted sender addresses or the absence of the sender's IP address in DNS, an excessive number of intended recipients or hidden addresses. The size and format of messages are also taken into consideration.
- Signature analysis** Lexical signature databases are updated around the clock. Using spam signatures, the program can even recognize modified versions of spam messages that have been altered to evade spam filters.
- Linguistic heuristics** The program scans messages for words and phrases that are typical of spam messages. Both the content of the message itself and any attachments are analyzed.
- Graphic spam** A database of signatures for graphic spam equips the program to block messages containing spam images, a type of spam that has become increasingly common in recent years.
- Real-time UDS requests** The Urgent Detection System is updated with information on spam messages literally seconds after they first appear on the Internet. Messages that could not be assigned a definitive status (e.g., spam, not spam) can be scanned using UDS.

Administration

Flexible management Our web interface allows system administrators to manage the application both locally and remotely. The filtration level is easily configurable, as are blacklists and safe lists. It is also possible to disable/enable individual filtration rules and automatically block mail encoded in Asian language sets.

Management of user groups The administrator can create user groups either using lists of addresses or domain masks (for example, XXX@domain.com) or by applying individual settings and filtration rules to each group.

Options for processing spam The program can be configured to process spam by either automatically deleting it, redirecting it to the quarantine folder with a note to the user or sending it for further filtration to the mail client.

Detailed reports Administrators can easily monitor the application, protection status and license status using HTML reports or alternatively, by viewing log files. Data can be exported in CSV and Excel formats.

Updating databases on schedule Updates to antivirus databases can be downloaded on a schedule set by the administrator (by default they update every 20 minutes). When undecided about the status of a suspicious message, the program also makes requests to the UDS server.

SYSTEM REQUIREMENTS

Hardware requirements

- Intel Pentium III 500 MHz processor or higher
- At least 256 MB RAM (1 GB recommended)
- 100 MB available HDD space for program installation (with additional space for the quarantine folder and temporary files)

Software requirements

Mail systems:

- Sendmail 8.13.5 with support for Milter API

- Postfix 2.2.2
- Qmail 1.03
- Exim 4.50
- Communigate Pro 4.3.7

Operating systems:

- Red Hat Linux 9.0
- Red Hat Fedora Core 3
- Red Hat Enterprise Linux Advanced Server 3
- SuSE Linux Enterprise Server 9.0
- SuSE Linux Professional 9.2

- Mandrake Linux version 10.1
- Debian GNU/Linux version 3.1
- FreeBSD version 4.10
- FreeBSD version 5.4

For the program to function properly, the following utilities need to be installed:

- bzip2
- The which utility
- Perl language interpreter

Product version: 3.0

KASPERSKY Lab



WEB PROTECTION

Kaspersky® Anti-Virus for Proxy Server

Kaspersky® Anti-Virus for Proxy Server protects all HTTP and FTP Internet traffic that passes through the proxy server.

The application provides security for users when working online and removes malicious programs and worms that spread via instant messaging programs.

FEATURES

Protection from viruses, Trojans and spyware

- | | |
|--|---|
| Real-time scanning of Internet traffic | The program detects and deletes all types of viruses, worms, Trojans and other malicious programs in traffic that passes through the proxy server. |
| Choice of filtration parameters | The program includes a wide choice of filtration parameters (IP and URL addresses, MIME types and file size), which can be used to create individual scanning rules for different user groups. |
| Scanning of archived files | Kaspersky Anti-Virus for Proxy Server provides the highest quality detection and treatment of viruses in any type of file or attachment. Kaspersky Anti-Virus Engine supports more than 1,800 archival and packing formats (as of June 2006). |
| Detection of potentially harmful programs | Using the extended protection option, the application can detect and delete not only known malicious programs, but also potentially harmful programs (such as spyware). |

Flexible administration

- Remote administration** The application can be administered remotely via the web interface or via a single configuration file.
- Group security policies** The administrator can set individual traffic filtration rules for each user group, which defines permission rules in line with the corporate security policy and employee requirements.
- User notifications** The program automatically blocks any infected objects and sends the user a notification in the form of an HTML page. The system administrator can configure the content, format and language of notifications.
- Reports and statistics** The application can compile statistical reports to help administrators track virus activity and monitor the application's performance.
- Configurable update modes** Updates to antivirus databases and program modules are available on demand, automatically or on schedule. They can be downloaded directly from Kaspersky Lab servers via the Internet or from a local corporate server.
- High reliability** Protection from memory leaks, hardware conflicts, input/output errors and critical system conflicts ensure fast and stable application performance.

SYSTEM REQUIREMENTS

Hardware requirements

- x86-32 architecture with a Pentium class processor
- At least 32 MB RAM
- At least 100 MB available HDD space

Software requirements

One of the following operating systems:

- Red Hat Enterprise Linux Advanced Server 4

- Red Hat Linux 9
- Fedora Core 5
- SuSE Linux Enterprise Server 9
- SuSE Linux Professional 10.1
- Debian GNU/Linux 3.1 updated (r2)
- Mandriva Linux 2006
- FreeBSD 4.11, 5.4, 6.1

The following additional programs are required:

- Squid Proxy Server with support for ICAP protocol
- The which utility
- The Webmin package (preferable) – for remote administration of the application
- Perl 5.0 or higher

Product version: 5.5

KASPERSKY Lab



FILE SERVER PROTECTION

Kaspersky® Anti-Virus for Linux File Server and Workstation

Kaspersky® Anti-Virus for Linux File Server and Workstation is a two-part solution designed to protect file servers and workstations. The first module, the on access protection, is integrated with the operating system and checks modified files (either new or amended files), thereby ensuring real-time protection of the system without significantly increasing server load. The second module, the on demand scanner, scans the file system, removable media devices and individual files either on schedule or on demand.

FEATURES

Detects and disinfects viruses, spyware and other malware

- Real-time protection of the system** The application intercepts file system requests, scans the files being accessed for malicious code and cures or deletes infected objects or isolates suspicious objects for further analysis.
- On demand file system scanning** The application scans specified areas for infected and suspicious objects at the time specified (or upon the administrator's request). It analyzes objects and disinfects, deletes or isolates objects for further analysis.
- Quarantine** Infected, suspicious and damaged objects detected in the server's file system can be moved to the quarantine folder, where they may undergo further actions, such as disinfection, deletion, etc.
- Backup storage** The solution incorporates support for saving copies of infected objects in a backup storage area before they are treated and/or deleted, making it possible to restore them on demand if treatment results in damage to the original file.

Easy administration

Remote administration Kaspersky Anti-Virus for Linux File Server and Workstation can be configured either traditionally, via the application's configuration file, or using the web interface.

Antivirus database updates Antivirus database updates can be downloaded from Kaspersky Lab's servers via the Internet or from local update servers on demand or on schedule. Administrators can choose the type of antivirus databases to be used: standard (detection of true malware only) or extended (databases used to detect potentially hostile software such as spyware, adware, etc.). Kaspersky Lab antivirus databases are updated hourly.

SYSTEM REQUIREMENTS

Hardware requirements

- x86-32 architecture with a Intel Pentium class CPU
- At least 32 MB of RAM
- At least 100 MB available HDD space for installation

Software requirements

This program is compatible with the following operating systems:

- Red Hat Linux 9.0
- Red Hat Fedora Core 3
- Red Hat Enterprise Linux Advanced Server 3

- SuSE Linux Enterprise Server 9.0
- SuSE Linux Professional 9.2
- Mandrake (Mandriva) Linux version 10.1
- Debian GNU/Linux version 3.0 updated (r4)
- FreeBSD version 4.10
- FreeBSD version 5.3
- OpenBSD version 3.6

The following additional software is required:

- Interpreter of the Perl language version 5.0 or higher (www.perl.org) for program installation using `install.pl`
- The `which` utility – for program installation
- `Webmin` program (www.webmin.com; optional) version 1.070 or higher is necessary for remote administration of the application.

Product version: 5.5

Kaspersky® Anti-Virus for Samba Server

Kaspersky® Anti-Virus for Samba Server is designed to protect file storage areas on Samba Servers, which emulate Windows file servers under the Linux operating system. Thus, Windows users within a heterogeneous network are provided with safe and transparent access to data stored on Linux file servers. The solution is easily integrated with the Samba Server and does not require the Samba Server or parts of the operating system to be recompiled.

FEATURES

Detects and disinfects viruses, spyware and other malware

- | | |
|--|---|
| Real-time protection for file storage | The application intercepts requests for access to Samba file storage areas, analyzes the files being accessed for malicious code and disinfects or deletes infected objects. Suspicious objects are quarantined pending further analysis. |
| On demand file system scanning | The application scans specified areas for infected and suspicious objects at the specified times (or on demand). It analyzes objects and disinfects, deletes or quarantines objects for further analysis. |
| Antivirus scanning optimization | The iChecker technology significantly reduces the time required for duplicate scans of each object by only scanning those files that have been modified since the latest scan. |
| Quarantine | Infected, suspicious and damaged objects detected in the file system can be moved to the quarantine folder, where they are processed according to administrator defined rules. |
| Backup storage | The solution saves copies of infected objects in a backup storage area before they are treated and/or deleted, making it possible to restore an object on demand in the event that disinfection fails. |

Easy administration

Remote administration Kaspersky Anti-Virus for Samba Server can be configured either traditionally via the application's configuration file or using the Web interface.

Antivirus database updates Antivirus database updates can be downloaded from Kaspersky Lab's servers via the Internet or from local update servers on demand or on schedule. Administrators can choose the type of antivirus databases to be used: standard (detection of true malware only) or extended (databases used to detect potentially hostile software such as spyware, adware, etc.). Kaspersky Lab antivirus databases are updated hourly.

SYSTEM REQUIREMENTS

Hardware requirements:

- Pentium class CPU
- At least 32MB of RAM
- At least 100MB available HDD space for installation

Software requirements:

This program is compatible with the following operating systems:

- Red Hat Enterprise Linux Advanced Server 4

- Red Hat Linux 9.0
- SuSE Linux Enterprise Server 9.0
- SuSE Linux Professional 9.2
- Debian 3.1
- Mandrake Linux 10.1
- FreeBSD 4.10, 5.4
- Samba Server Version 2.2.6 or higher

The following additional software is required:

- Interpreter of the Perl language version 5.0 or higher (www.perl.org) for program installation using `install.pl`

Product version: 5.0

Services

Support services comprise an essential component of Kaspersky Lab's products and solutions. Registered users are provided with hourly antivirus database updates, free product updates and round-the-clock technical support. A range of additional services are available to corporate customers.

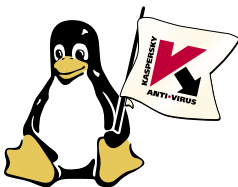
Regular database updates are crucial for ensuring the effective operation of Kaspersky Lab products. Currently, antivirus database updates are released hourly and antispam databases are updated every 20 minutes. During virus outbreaks or epidemics, Kaspersky Lab issues more frequent updates and disinfection tools to help users prevent infection.

Additionally, users of Kaspersky Lab products can contact the company's 24-hour technical support service. Support is available via telephone and email in English, French, German and Russian.

Anyone visiting the Kaspersky Lab website can scan any file on their computer for viruses online. Before purchasing any program, users can download a free trial version and try it on their computers. During global virus outbreaks, the company releases free disinfection utilities which are available to the general public.

In addition to software, Kaspersky Lab offers information support. The Virus Encyclopedia contains detailed descriptions of malicious programs of all kinds and the company's newsletter keeps users updated on the latest virus outbreaks.

Kaspersky Lab supports its enterprise level information security products with a range of additional services. Each corporate client's needs are addressed on an individual basis. Services provided to such customers include examining and analyzing the corporate network, installation of an antivirus system, training of the company's staff and maintenance of the security system installed.



Contact Information



● **Kaspersky Lab HQ**
Science and Technology Park
10/1 1st Volokolamsky Proezd
Moscow 123060 Russia
www.kaspersky.com
Email: sales@kaspersky.com
Tel. +7 495 797 8700

● **Kaspersky Lab USA**
300 Unicorn Park
Woburn MA 01801 USA
www.kaspersky.com
Email: info@us.kaspersky.com
Tel. +1 781 503 1800

● **Kaspersky Lab Japan**
Iwamoto Bldg. 4F 3-2-3
Iwamoto-cho 101-0032
Chiyoda-ku Tokyo Japan
www.kaspersky.co.jp
Email: sales@kaspersky.co.jp
Tel. +81 3 5687 7839

● **Kaspersky Lab UK**
Culham Innovation Centre
D5 Culham Science Centre
Abingdon OX14 3DB
United Kingdom
www.kaspersky.co.uk
Email: sales@kasperskylab.co.uk
Tel. +44 (0) 870 0113461

● **Kaspersky Lab Germany**
Steinheilstraße 13
85053 Ingolstadt
Germany
www.kaspersky.de
Email: info@kaspersky.de
Tel. +49 (0) 841 98 18 90

● **Kaspersky Lab France**
Immeuble l'Européen
ZAC Rueil 2000
2 Rue Joseph MONIER
92 500 Rueil Malmaison
France
www.kaspersky.fr
Email: info@fr.kaspersky.com
Tel. +33 8205 888 612

● **Kaspersky Lab Benelux**
Havensingel 1A
5211 TX's-Hertogenbosh
The Netherlands
www.kasperskylab.nl
Email: sales@bnl.kaspersky.com
Tel. +31 (0) 73 615 4860

● **Kaspersky Lab Poland**
Ul. Krotka 27A 42-200
Czesochowa Poland
www.kaspersky.pl
Email: info@kaspersky.pl
Tel. +48 34 368 18 14

● **Kaspersky Lab China**
Suite A504-505
U-Space Mall, No. 8
Guang Ou Men Wai Street
Chaoyang District
Beijing 100022 China
www.kaspersky.cn
Email: sales@kaspersky.com.cn
Tel. +86 10 5861 2570

● **Kaspersky Lab Korea**
Flour 8, Plaza 654 Building
654-3 Yuksam-dong
Kangnam-ku Seoul 135-080
South Korea
www.kasperskylab.co.kr
Email: sales@kasperskylab.co.kr
Tel. +82 2 508 8789

Kaspersky® Anti-Virus and Kaspersky® are registered trademarks of Kaspersky Lab Ltd.
Other brands and products are trademarks of their respective holder(s).
Copyright © 2006 Kaspersky Lab Ltd. All rights reserved.