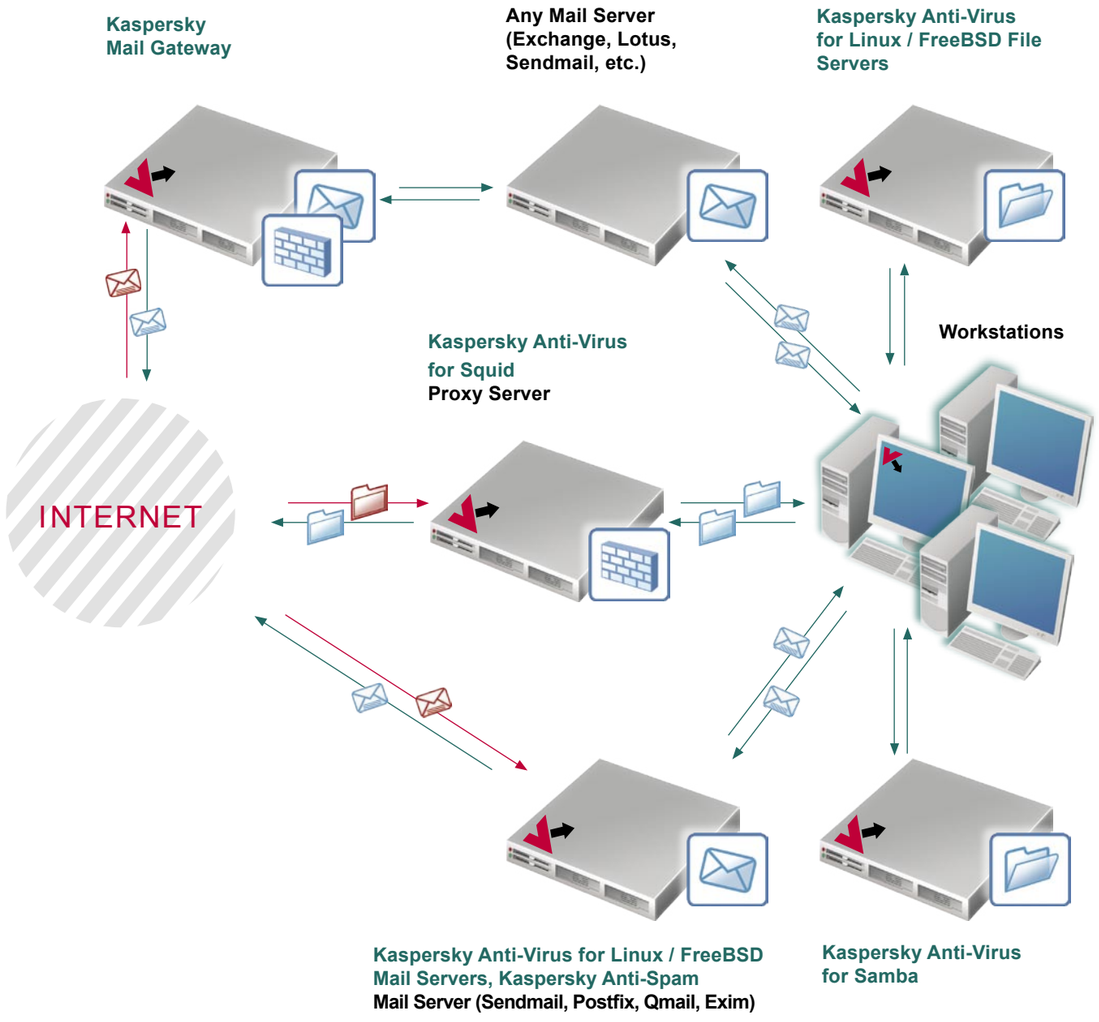
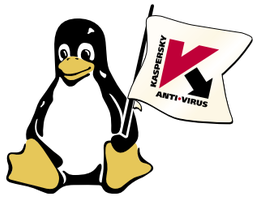
for Linux / FreeBSD

Kaspersky Lab Corporate Products

KASPERSKY lab

Kaspersky Lab Corporate Products for Linux / FreeBSD





CONTENTS

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 systems. 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

Today most computer networks are heterogeneous, with Linux platforms frequently used for servers. Linux and FreeBSD are more secure and very few viruses exist for these operating systems. However, most workstations run under the Microsoft Windows family of operating systems, which is under constant attack from virus writers. Information in the form of emails and files is exchanged between Windows users. Since Linux mail, file and proxy servers act as transit corridors for this information flow, they need to be protected as carefully as workstations and servers running under Windows.

In 1999 Kaspersky Lab was the first to develop antivirus protection for workstations, file servers and application servers running Linux / FreeBSD. By 2000, Kaspersky Lab was again the first to provide protection for Sendmail and Qmail. For the past six years, we have supplied effective data protection solutions for both open-source and commercial Linux / FreeBSD distributions.

Currently, Kaspersky Lab offers companies a complete line of products that provide full-scale protection of all nodes in a corporate network: antivirus scanning solutions for mail and web traffic, as well as solutions designed to protect file storage and that prevent spam. This catalog presents an overview of Kaspersky Lab's products for Linux / FreeBSD platforms. You can find more detailed information about our products and the nearest retailer on our corporate website (www.kaspersky.com).

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 then protects against 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 of new and existing malware. All antivirus vendors declare a high level of malware detection, but this characteristic can be objectively evaluated only through independent comparative tests. In such tests, Kaspersky Anti-Virus invariably takes one of the top places.

Virus Bulletin — Providing virus information since 1989, this UK-based publication regularly tests antivirus programs on detection rates, performance and false positives rates. In April 2005, Kaspersky Anti-Virus received the VB100% award for detecting 100% of malicious programs on the Red Hat Linux 9 platform.

AV-Test.Org — This independent German laboratory tests antivirus programs for response speed and the time it takes to release updates in response to new malicious programs. Kaspersky Anti-Virus achieved top results in May 2005 tests.

AV-comparatives.org — This Austrian project independently evaluates antivirus programs through various tests, including evaluation of heuristic analyzers. In February 2005, Kaspersky Anti-Virus took first place for malware detection.

Heuristic analysis

A heuristic analyzer is responsible for detecting unknown malicious programs. The heuristic analyzer used in the Kaspersky Anti-Virus engine was designed to be multi-faceted from the start, unlike most first-generation heuristic analyzers, which were designed to detect only specific types of malicious code.

Currently, Kaspersky Lab's heuristic analyzer is capable of detecting almost any type of malicious code in executable files, all sectors and memory, as well as new script viruses and malicious programs for Microsoft Office and, finally, malicious code written in high-level languages, such as Microsoft Visual Basic and Delphi.

False positive rates

This parameter is crucial for the evaluation of the quality of an antivirus program's performance, given that mistakenly identifying a virus can lead to serious consequences, such as data loss, blocked access to applications or the Internet, etc. Currently, the Kaspersky Anti-Virus engine is an acknowledged leader in terms of detection rate is, while the false positive rate is close to zero.

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 a large number of packers. The Kaspersky Anti-Virus engine supports over 1,200 archival formats (as of February 2006). Support for such a large number of formats reduces the time required to analyze new viruses, resulting in faster response times to new threats. This is especially important for protecting mail systems, given that a significant number of viruses are sent by email as compressed attachments.

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.

KASPERSKY lab

MAIL PROTECTION

Kaspersky® Anti-Virus for Linux / FreeBSD Mail Servers

Kaspersky® Anti-Virus for Linux / FreeBSD Mail Servers 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. It also scans the server's file systems on demand. Kaspersky Anti-Virus for Linux/FreeBSD Mail Servers supports the most widely used email solutions, namely Sendmail, Qmail, Postfix, Exim, and Sendmail with Milter API.

FEATURES

Detection and disinfection of 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, and 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/or recipient 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 a quarantine folder, where they will be disinfected, 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 them if necessary.

File server scanning
In addition to scanning mail traffic, Kaspersky Anti-Virus for Linux / FreeBSD Mail Servers offers on-demand scanning of the server's file systems. 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/FreeBSD Mail Servers can be configured either traditionally, via the application's configuration file, or using the Webmin interface. The Webmin administration system also provides the capability of regulating access privileges for different user groups.

Optimizing 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 work queue and limiting the number of objects scanned simultaneously in the background mode.

Configuring database updates
Antivirus databases can be updated from Kaspersky Lab's servers via the Internet or from local update servers on demand or automatically. 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 including spyware, adware, etc.). Kaspersky Lab's antivirus databases are updated hourly.

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

SYSTEM REQUIREMENTS

Hardware requirements:
- Pentium-class CPU
- At least 32 MB RAM
- At least 100 MB HDD space

Software requirements:
One of 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 9.2
- Mandrake (Mandriva) Linux 10.1
- Debian GNU/Linux (updated (r4))
- FreeBSD 4.10 / 5.3
- 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 which utility
- Webmin program (www.webmin.com)
- Perl 5.0 or higher (www.perl.org) – for installation of Kaspersky Anti-Virus using install.pl

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). When installed between the corporate network and the Internet, the application scans email messages for viruses, performs centralized filtering of spam of all mail traffic and protects the company's mail server from unauthorized use. As a stand alone solution, the application fits neatly into any environment and combines easily with other vendors' programs installed on other network nodes.

FEATURES

Integrated protection against 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 graphical signatures that detect spam in image format.

User notification — If a suspicious or infected object is detected, the system administrator, sender and/or recipient receive a message, 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 capabilities

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.

*Product launch is scheduled for the second quarter of 2006.

Protection of the server from unauthorized access

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

Flexible management and administration

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

Flexible configuration — 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's queue and limit the number of objects that can be scanned simultaneously in the background.

Automatic 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.

Graphic reports — The program includes the option to view virus activity for a given period of time in graphic form. Information regarding the types of viruses detected during antivirus scans can also be viewed. Furthermore, 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 HDD space for application installation.
- At least 500 MB available in the /tmp file system.

Software requirements
- Kaspersky Mail Gateway is compatible with the following operating systems:
  - Red Hat Enterprise Linux Advanced Server 4.
  - Red Hat Linux 9.0.
  - Fedora Core 3.
  - SuSE Linux Enterprise Server 9.0.
  - SuSE Linux Professional 10.0.
  - Debian GNU/Linux 3.1 updated (r1).
  - Mandriva 2006.
  - FreeBSD 4.11, 5.4, 6.0.
- Interpreter of the Perl language version 5.0 or higher (www.perl.org), the which utility – for program installation
- Webmin program (www.webmin.com) version 1.070 or higher is necessary for remote administration.

Product version: 5.5

Kaspersky® Anti-Spam*

Kaspersky® Anti-Spam is a solution that protects users of corporate mail systems from spam (that is, unsolicited mass mailings). Kaspersky Anti-Spam performs the function of a spam filter on the mail server, identifying and blocking spam messages in incoming and outgoing mail traffic.

Intelligent technology is used to analyze mail messages. Regular updates, released by the antispam laboratory every 20 minutes, enable blocking of nearly all spam messages.

Kaspersky Anti-Spam is recommended as a specialist solution for ISPs, since the specific requirements of Internet providers were incorporated into the product at the development stage.

FEATURES

Protection from Spam

Filtration by white and blacklists
When processing messages, the program checks for mail and IP addresses against those that are in the blacklists (DNSBL – a DNS-based Blackhole List) of providers and non-profit organizations. Administrators can also maintain their own whitelists of addresses (Friends Lists), which will always be allowed.

Analysis of formal attributes
Common attributes of spam that are, for example, modifications of sender's addresses, omission of the recipient's name or a large number of recipient names, and absence of an IP address in the DNS system are take into consideration when processing messages. Messages are also analyzed according to their size and format.

Linguistic heuristics
The application checks for the distribution of certain phrases in messages that are typical of spam. The filtration server analyzes not only the text of the messages but also any attachments.

Signature analysis
A lexical signature can be automatically created for each spam message, so that even modifications to spam messages will be detected. Every day, the Linguistic Laboratory adds tens of thousands of new signatures to its databases.

Detection of graphic spam
Signatures are created and cataloged for graphic spam similarly to the procedures for non-graphic spam. The only difference is that the main body of the message or attachments is in the form of images.

*Product launch is scheduled for the second quarter of 2006.

UDS requests in real time mode
Sometimes, a message cannot be given a spam rating on the basis of the initial analysis, in which case the program sends a request to the UDS server. This contains a database of the very latest spam mailings. Information about a new spam mailing is added to the database as soon as it has been identified by our analysts.

Administration

Flexible settings
System administrators can set the stringency of filtration and create white and blacklists of sender addresses. They can also enable/disable any of the filtration rules and enable filtration of mail that is encoded for East Asian languages.

Management of user groups
Administrators can create different user groups, in the form of lists of addresses and according to domain name (for example, *@???.domain.com). Each group can be assigned its own settings, filtration rules and message processing rules.

Filtration policy
There is now a wide range of options for possible responses to spam messages. Messages can be automatically deleted, a refusal notification can be sent to the sender and messages (or copies of messages) can be stored in quarantine. Administrators also have the option of adding notes to the message heading, in which case the letter is delivered to the recipient and filtered at the level of the mail client.

Updating databases
Databases are updated according to the schedule set by the administrator (every 20 minutes by default). The application also sends requests to the UDS update server in real time about any suspicious objects.

Detailed reports
System administrators can control the application's operation and status of the antispam protection using graphic reports and by viewing the Linux log files. Reports can be formatted in CSV and Excel. Administrators can also access reports about mail traffic in general and the proportion of spam during a specified time period.

SYSTEM REQUIREMENTS

Hardware requirements
- Intel Pentium III processor 500 MHz 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 servers:
- Sendmail 8.13.5 with Milter API.
- Postfix 2.2.2.
- Qmail 1.03.
- Exim 4.52.
- 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 Squid*

Kaspersky® Anti-Virus for Squid is an antivirus solution designed to protect web traffic (http/ftp) passing through the Squid web proxy server, one of the most popular proxy servers today. The application helps make web surfing safe and protects users against most worms distributed via IM (instant messaging) applications.

FEATURES

Detection and disinfection of viruses, spyware and other malware

Real time web traffic protection
The application integrates with the Squid Web Proxy Cache using the ICAP protocol (Internet Content Adaptation Protocol) and scans all web traffic passing through the proxy server in real time.

Customizable notifications
Administrators can define the format and contents for notification messages sent to users as .html pages.

Quarantine
Infected, suspicious and damaged objects detected during the antivirus scan can be moved to quarantine folders pending further analysis and action, such as treatment, deletion, etc.

Backup storage
Infected objects can be saved in a backup storage area before they are treated and/or deleted, making it possible to restore them if the object is damaged during treatment.

*Product launch is scheduled for the second quarter of 2006.

Flexible management and administration

Remote administration
Kaspersky Anti-Virus for Squid can be configured either traditionally, via the application's configuration file, or using the Webmin interface. The Webmin administration system also provides the option of regulating access privileges for different user groups.

Antivirus database updates
Antivirus database updates can be downloaded from Kaspersky Lab servers via the Internet or from local update servers on demand or automatically. 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's antivirus databases are updated hourly.

SYSTEM REQUIREMENTS

Hardware requirements:
- x86-32 architecture with a Pentium-class CPU.
- At least 32 MB of RAM.
- At least 100 MB HDD available.

Software requirements:
- One of 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
- Squid Proxy server with support for ICAP protocol
- The which utility
- Webmin package (optional) – for the remote administration of Kaspersky Anti-Virus.
- Perl version 5.0 or higher

KASPERSKY lab

FILE SERVER PROTECTION

Kaspersky® Anti-Virus for Linux / FreeBSD File Servers and Workstations

Kaspersky® Anti-Virus for Linux / FreeBSD File Servers and Workstations 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 file modifications (file creation and modification), thereby ensuring real time protection of the system without significantly increasing the 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

Detection and disinfection of 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 and 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/or 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 if treatment results in damage to the original file.

Easy administration

Remote administration
Kaspersky Anti-Virus for Linux / FreeBSD File Servers and Workstations can be configured either traditionally, via the application's configuration file, or using the Webmin interface. The Webmin administration system also provides the option of setting access privileges for different user groups.

Antivirus database updates
Antivirus database updates can be downloaded from Kaspersky Lab servers via the Internet or from local update servers on demand or automatically. 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's antivirus databases are updated hourly.

SYSTEM REQUIREMENTS

Hardware requirements:
- x86-32 architecture with a Pentium-class CPU.
- At least 32 MB of RAM.
- At least 100 MB HDD available.

Software requirements:
- One of 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 which utility.
- Perl version 5.0 or higher.
- Webmin package (optional) – for the remote administration of Kaspersky Anti-Virus.

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 a Windows file server under the Linux / FreeBSD operating system. Windows-based users within a heterogeneous network are provided with safe and transparent access to data stored on Linux / FreeBSD file servers. Kaspersky Anti-Virus is easily integrated with the Samba Server and does not require recompilation of the Samba Server or parts of the operating system.

FEATURES

Detection and disinfection of viruses, spyware and other malware

Real time protection for file storage — The application intercepts requests for access to Samba file servers, 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 user defined 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 eliminating the need to scan all files and only scanning those that have been modified since the last 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 if 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 Webmin interface. The Webmin administration system also provides the option to regulate access privileges for different user groups.

Antivirus database updates — Antivirus database updates can be downloaded from Kaspersky Lab servers via the Internet or from local update servers on demand or automatically. 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's antivirus databases are updated hourly.

SYSTEM REQUIREMENTS

Hardware requirements:
- x86-32 architecture with a Pentium-class CPU
- At least 32 MB of RAM
- At least 100 MB HDD available

Software requirements:
- One of the following operating systems:
  - Red Hat Linux 9.0
  - Linux RedHat 7.3, 8.0, 9.0
  - Linux SuSE 8.1, 8.2
  - Linux Debian 3.0
- Samba Server version 2.2.6 or higher
- The which utility
- Perl version 5.0 or higher
- Webmin package (optional) – for the remote administration of Kaspersky Anti-Virus

Product version: 5.5

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.

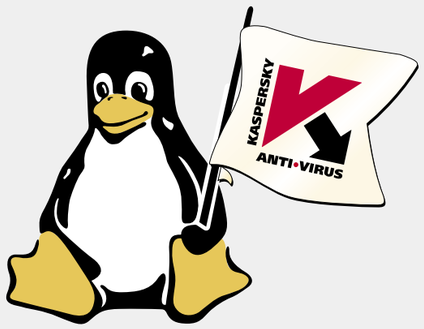
Regular database updates are crucial for ensuring the effective operation of Kaspersky Lab products. Currently, antivirus database updates are released hourly and antispam databases are updated every 20 minutes. During virus outbreaks or epidemics, Kaspersky Lab issues more frequent updates and disinfection 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
1st Volokolamsky Proezd, 10/1
Moscow 123060
Russian Federation
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
Czestochowa 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 Qu 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