

Kaspersky® Anti-Spam

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

When a user opens a new email account, it is almost inevitable that at some point their address will be added to a spam database and targeted with anonymous spam messages. As a result, companies find that a significant amount of time is lost during the work day, as employees have to delete tens, if not hundreds, of unwanted messages from their mailboxes. Other side effects include over-payments for excess Internet traffic, overloaded mail systems and an increased risk of viruses and phishing attacks penetrating networks.

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

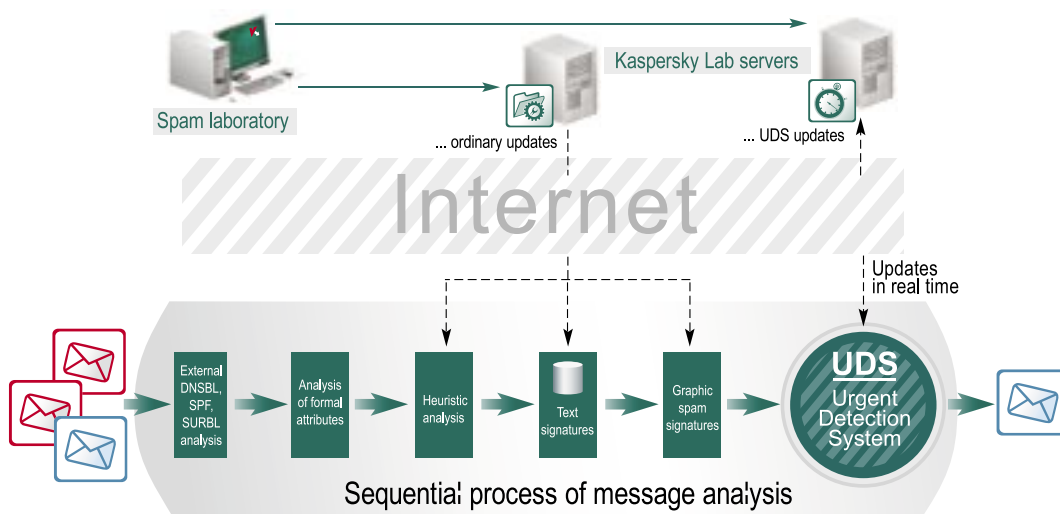
Main advantages

Advanced antispam technologies. The application uses SpamTest™ intelligent technology to detect spam, which includes the following methods: DNS blacklist plugin, analysis of formal attributes, linguistic heuristics, signature databases that are updated in real time and signatures for graphic spam.

Rapid reaction to new spam mailings. Kaspersky Lab spam analysts work round-the-clock to keep databases up-to-date with the latest spam templates and techniques used by spammers to evade spam filters. The UDS (Urgent Detection System) provides data on newly discovered spam mailings within seconds of their detection, while generating a minimal amount of Internet traffic.

Convenience for administrators. With the new Kaspersky Anti-Spam interface, system administrators can administer and configure the product from any location. Administrators will find that the highly intuitive and ergonomic administration tools help them quickly master the application. Meanwhile, the new reporting module simplifies and accelerates the process of analyzing mail traffic and ascertaining the ratio of spam-to-legitimate mail.

Efficiency and scalability. The new filtration engine in Kaspersky Anti-Spam uses four to five times fewer resources than the previous version, and the size of downloadable updates has been reduced 3.5 times. Kaspersky Anti-Spam offers effective protection both for small businesses and for large-scale mail systems such as Mail.Ru, which processes up to 70 million messages daily, totalling as much as 500 GB.



Functions

Protection from spam

Lists. Messages are checked against blacklists of email addresses and sender IP addresses (known as DNSBL or DNS-based Blackhole Lists), which are maintained by service providers and public organizations. Administrators can also compile their own whitelists (e.g., friends lists) of users, whose messages will automatically be delivered without undergoing analysis.

Analysis of formal attributes. Attributes that are typical of spam messages include modifications of sender addresses, no recipients specified or an excessive number of recipients, and the absence of an IP address in the DNS system. The size and format of messages are also taken into consideration during analysis.

Linguistic heuristic analysis. Both messages and attachments are filtered according to their content, which is scanned for specific word combinations and their distribution within messages.

Signature analysis. When a new spam message is detected, it can be automatically assigned a lexical signature, which is added to the signature database. From this signature, Kaspersky Anti-Spam can recognize the message or modified versions of the message.

Detection of graphic spam. Graphic signatures are created and added to the signature database in the same way as for ordinary spam. Using graphic spam analysis, images rather than words are analyzed in messages that can include both images and text.

UDS (Urgent Detection System) requests in real time. If the application cannot decide whether a message is legitimate mail or spam, it sends a request to the UDS server. The UDS server contains information on newly discovered spam messages, which is added to the database the minute Kaspersky Lab spam analysts discover a new spam message.

Administration

Flexible settings. System Administrators can adjust the stringency level of filtration, maintain sender blacklists and whitelists, enable or disable individual filtration rules and set the application to block mail encoded for East-Asian languages.

Administration of user groups. Administrators can create user groups by defining address lists or lists of domain masks (such as *@???.domain.com). Each group can be assigned its own settings, filtration rules and processing rules.

Configurable processing rules. The processing rules for spam can be configured to best suit the needs of each individual customer. The application can automatically delete each spam message, send notification of refusal to the sender or redirect a message (or copy of the message) to the quarantine folder. Administrators can also add a marker to the letter's subject line or headers, so that the message can be sent to the recipient and filtered at the level of the mail client.

Updates to databases. Administrators have the option of setting their own schedule for receiving updates (by default, updates are downloaded every 20 minutes). The application will also make real-time requests to the UDS update server when it identifies any suspicious messages.

Detailed reports. Administrators can view graphic HTML reports or Linux log files to maintain control over the day-to-day operation of the application, the status of antispam protection and product licenses. Reports can be exported to CSV or Excel files. The application can also create reports on mail traffic and the proportion of spam to non-spam in any given period.

System requirements

Hardware requirements

- Intel Pentium III 500 MHz or faster
- At least 512 MB free RAM (1 GB recommended)
- 100 MB free HDD space for installation of the application (does not include the disk space required for backup storage and temporary files)

Software requirements

Mail servers:

- Sendmail 8.13.5 with support for Milter API
- Postfix 2.2.2
- Qmail 1.03
- Exim 4.52
- Communicate 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

bzip2, which utilities and a Perl interpreter are required for program operation.

Languages: English & Russian (documentation only)

Version: 3.0

Contact information:

Kaspersky Lab HQ
10, bld. 1, 1st Volokolamskii Proyezd
Moscow 123060
Russian Federation

Phone: +7 495 797 8700
sales@kaspersky.com

See www.kaspersky.com for details.

Kaspersky Lab products are available from our partners at www.kaspersky.com/partners

©2006 Kaspersky Lab Ltd.
Kaspersky® Security is a registered trademark of Kaspersky Lab Ltd.
All other names and trademarks are the copyrighted work of their respective owners.