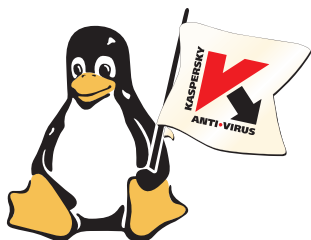
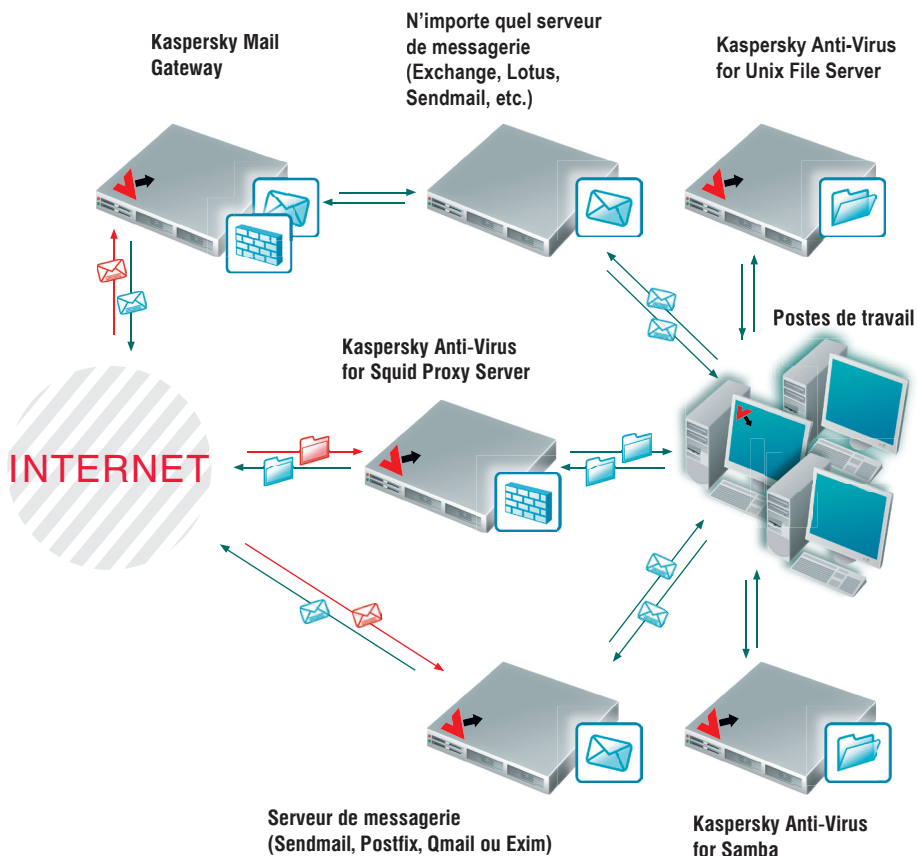


Kaspersky Lab
LOGICIELS
pour Linux / Unix



Logiciels de Kaspersky Lab pour Linux / Unix



Sommaire

Kaspersky Lab, spécialiste de la protection des données 4

Position de Kaspersky Lab sur le marché de la protection des données sous Linux/Unix 5

Le moteur antivirus de Kaspersky 6-7

Protection du courrier
• Kaspersky Anti-Virus® for Linux/Unix Mail Servers 10-11

• Kaspersky® Mail Gateway 12-13

• Kaspersky® Anti-Spam 14-15

Protection du trafic HTTP/FTP
• Kaspersky Anti-Virus® for Squid (Disponible courant 2006) 18-19

Protection des entrepôts de fichiers
• Kaspersky Anti-Virus® for Linux/Unix File Servers and Workstations 22-23

• Kaspersky Anti-Virus® for Samba Server 24-25

Services 26

Coordonnées 27

Kaspersky Lab, spécialiste de la protection des données

Kaspersky Lab est l'éditeur de logiciels de sécurité informatique le plus connu en Russie et jouit également d'une reconnaissance internationale. Ses différents logiciels offrent une protection contre les virus informatiques, le courrier non sollicité et les attaques de pirates informatiques.

Depuis quinze ans, nous menons une lutte impitoyable contre les virus et les autres menaces informatiques et cela nous a permis d'acquérir des connaissances et des compétences qui sont notre bien le plus estimable. Nous analysons en permanence l'activité sur le front des virus et nous avons appris à prévoir les tendances au niveau du développement des programmes malveillants. Cet avantage est à la base des produits et des services proposés par Kaspersky Lab. Nous avons toujours une longueur d'avance sur la concurrence et nous fournissons à nos clients la meilleure protection possible.

Kaspersky Lab a été le premier à développer de nombreuses technologies qui occupent désormais une place incontournable dans la lutte contre les virus. Ce n'est pas un hasard si de nombreux autres éditeurs ont adopté, pour leur propre produit, le moteur antivirus de Kaspersky Lab : Nokia ICG (Etats-Unis), F-Secure (Finlande), Aladdin (Israël), Sybari (Etats-Unis), G Data (Allemagne), Deerfield (Etats-Unis), Alt-N (Etats-Unis), Microworld (Inde), BorderWare (Canada), MailWatcher (France) et NetAsq (France).

Les clients de Kaspersky Lab bénéficient d'un large éventail de services qui garantissent le fonctionnement ininterrompu des logiciels et qui répondent à la moindre de leurs attentes. Nous étudions, déployons et offrons une assistance technique pour les solutions antivirus destinées aux entreprises. Nos clients ont accès à l'une des bases antivirus les plus importantes au monde, renouvelée toutes les heures. Nous proposons à nos utilisateurs un service d'assistance technique en français, en anglais, en allemand, en espagnol et en russe.

Position de Kaspersky Lab sur le marché de la protection des données sous Linux/Unix

Comme vous le savez, la majorité des réseaux informatiques modernes sont hétérogènes. Les systèmes d'exploitation Linux et Unix, extrêmement bien protégés et si peu vulnérables aux virus, sont installés en règle générale sur les serveurs qui remplissent des fonctions multiples. Mais la majorité des postes de travail tournent sous Windows, un système d'exploitation connu pour les failles qu'il offre aux virus, aux programmes malveillants et aux programmes potentiellement dangereux. Ainsi, l'échange d'informations, sous la forme de fichiers ou de messages électroniques, a lieu en fin de compte entre des utilisateurs Windows. Une telle situation oblige les responsables informatiques à assurer la protection des serveurs Linux/Unix via lesquels transitent ces informations.

Kaspersky Lab fut le premier éditeur au monde à proposer en 1999 une solution antivirus pour les postes de travail, les serveurs de fichiers et les serveurs d'applications tournant sous Linux/FreeBSD. Vinrent ensuite les premiers filtres antivirus pour les systèmes de messagerie Sendmail et Qmail. Voici déjà cinq ans que nous proposons des solutions efficaces de protection antivirus pour les versions les plus populaires de Linux/Unix. A l'occasion du salon Linux World Expo cet été à San Francisco, trois des cinq nominés au titre de Best Security Solution (Meilleure solution de sécurité) employaient le moteur antivirus de Kaspersky Lab dans leurs produits.

Kaspersky Lab propose une gamme de produits complète pour une protection avancée de l'ensemble des nœuds d'un réseau d'entreprise : analyse antivirus du trafic de messagerie et du trafic Internet, analyse des entrepôts de fichiers et solution de lutte contre le courrier indésirable.

Le présent catalogue a été conçu dans le but de vous offrir une vue d'ensemble de la gamme de logiciels développés par Kaspersky Lab pour les systèmes Linux/Unix. Si vous souhaitez obtenir de plus amples informations sur notre société, nous vous invitons à consulter notre site à l'adresse www.kaspersky.com/fr.

Le moteur antivirus de Kaspersky

Au sein de tout logiciel antivirus, on trouve un “moteur”, à savoir un module responsable de l’analyse des objets et de la découverte des programmes malveillants. Le taux de détection des programmes malveillants et l’efficacité de la protection contre ces derniers dépendent en grande partie de la conception et de la fabrication de ce module. Il existe plusieurs critères fondamentaux qui permettent de juger de la qualité d’un “moteur” antivirus.

Qualité de la détection

Ce paramètre définit le niveau d’identification des virus. Tous les logiciels antivirus disponibles sur le marché vantent leur taux de détection élevé, toutefois seuls les tests réalisés par des laboratoires indépendants sont capables de donner une évaluation objective. Kaspersky Lab finit régulièrement en tête des tests organisés. Parmi les organisations de renommée internationale qui ont soumis des logiciels antivirus à des tests indépendants, nous pouvons citer:

Virus Bulletin. Ce magazine britannique, qui traite des virus depuis 1989, met régulièrement sur pied des essais afin d’évaluer le taux de détection, la vitesse de traitement et le nombre de fausses alertes caractéristiques de différents logiciels. En avril 2005, Kaspersky Anti-Virus a décroché une fois de plus le titre VB100%, ce qui confirme l’excellence de la détection des programmes malveillants sous Red Hat Linux 9.

AV-Test.org. Ce laboratoire indépendant allemand teste les logiciels sur la vitesse de réaction et la publication des mises à jour en cas d’apparition d’un nouveau code malicieux. Suite à un test réalisé en mai 2005, Kaspersky Lab a décroché, à son habitude, l’une des premières places.

Av-Comparatives.org. Laboratoire autrichien qui réalise divers tests, dont plusieurs vérifiant l’efficacité des analyseurs heuristiques. En février 2005, Kaspersky Anti-Virus a décroché la première place en termes de programmes malveillants identifiés.

Niveau de détection des analyseurs heuristiques

Un analyseur heuristique a pour but d’identifier les programmes malveillants encore inconnus du logiciel antivirus qui ne possède pas les signatures (exemples) correspondantes. L’analyseur heuristique intégré au “moteur” antivirus de Kaspersky Lab a dès le début de sa conception montré de grandes différences par rapport à la majorité des autres analyseurs. A l’heure actuelle, l’analyseur heuristique du moteur antivirus de Kaspersky Lab permet d’identifier quasiment tout type de code malveillant (vers de réseau et de messagerie, virus, chevaux de Troie divers, majorité des logiciels espions) dans les fichiers exécutables, ainsi que dans les secteurs et la mémoire.

Niveau de fausses alertes

Un fichier sain qui est classé par erreur comme un fichier infecté est une situation qui peut entraîner de fâcheuses conséquences: perte de données suite à la suppression du fichier, blocage de l'utilisation de certains logiciels et d'Internet, par exemple, impossibilité de lancer le navigateur Internet, de consulter certains sites ou de charger certains modules logiciels, etc. A l'heure actuelle, Kaspersky Anti-Virus est le leader en matière de détection de programmes malveillants avec un pourcentage de fausses alertes pratiquement nul. Ce fait a été confirmé à maintes reprises dans le cadre de tests indépendants mais aussi par les utilisateurs de nos logiciels.

Prise en charge d'un grand nombre de logiciels d'archivage et de compactage

Les créateurs de programmes malveillants dissimulent très souvent les virus qu'ils produisent à l'aide de différents utilitaires. Cette technique permet de modifier certains des paramètres utilisés en général par les logiciels antivirus pour identifier les programmes malveillants. Afin de pouvoir identifier les modifications d'un seul et même virus, de nombreux logiciels antivirus doivent mettre à jour leur base antivirus. Kaspersky Anti-Virus prend en charge plus de 450 utilitaires de compactage de fichiers exécutables, de logiciels d'installation et d'utilitaires d'archivage (plus de 1 200 modifications en juin 2005). Le décompactage des objets a lieu quel que soit le niveau de complexité des archives. La prise en charge d'un aussi grand nombre d'utilitaires de compactage et d'archivage est particulièrement importante pour la protection des systèmes de messagerie dans la mesure où les virus qui sont diffusés par courrier électronique sont bien souvent archivés.

Fréquence et taille de la mise à jour des bases antivirus

Les bases antivirus de Kaspersky Lab sont actualisées toutes les heures, ce qui représente une fréquence unique au monde. En cas d'épidémie, ces bases sont diffusées dès que la procédure d'identification du nouveau virus a été ajoutée. Ainsi, on compte en moyenne plus de 700 mises à jour par mois.

Possibilité d'actualiser le moteur sans mettre à jour les bases antivirus

Bien souvent, l'identification des virus requiert non seulement la mise à jour des bases antivirus mais également l'actualisation de certains modules du "moteur". Un logiciel antivirus qui ne permet pas la mise à jour opérationnelle de son "moteur" prive son utilisateur de protection face aux nouveaux virus. De plus, cette procédure permet d'améliorer le fonctionnement du "moteur" et de rectifier les erreurs. Les utilisateurs de Kaspersky Anti-Virus peuvent actualiser environ 70% des fonctions du moteur lors de la mise à jour des bases antivirus. Par exemple, la mise à jour peut contenir un nouveau logiciel d'archivage ou de compactage pris en charge. Ainsi, en procédant à la mise à jour quotidienne des bases antivirus, l'utilisateur s'assure que le moteur du logiciel antivirus est toujours d'actualité.



PROTECTION DU COURRIER

Kaspersky Anti-Virus® for Linux/Unix Mail Servers

Kaspersky Anti-Virus for Linux/Unix Mail Servers est une solution efficace pour la protection antivirus du flux de messagerie des entreprises.

L'application s'intègre au système de messagerie déjà en place sous la forme d'un module supplémentaire et recherche, en temps réel, la présence d'éventuels virus dans les messages électroniques transmis via le protocole SMTP. Elle peut également analyser à la demande le système de fichiers du serveur.

Kaspersky Anti-Virus for Linux/Unix Mail Servers a été développé pour les serveurs de messagerie les plus répandus : Sendmail, Qmail, Postfix, Exim et Sendmail avec Milter API.

FONCTIONS

Analyse antivirus avancée et réparation

- **Analyse antivirus avancée.** Kaspersky Anti-Virus for Linux/Unix Mail Servers recherche la présence d'éventuels virus dans tous les composants du message électronique. L'application recherche et supprime tous les types de virus, de programmes malveillants et de riskwares dans le courrier entrant et sortant ainsi que dans les pièces jointes de n'importe quel format.
- **Notifications.** En cas de découverte d'un objet suspect ou infecté, l'administrateur système, l'expéditeur et le destinataire du message reçoivent un avertissement dont le contenu et le format sont définis par l'administrateur. Ces notifications peuvent être rédigées dans n'importe quelle langue.
- **Quarantaine.** Les fichiers infectés, suspects et corrompus découverts dans le système de fichiers du serveur ou dans le flux de messagerie peuvent être placés en quarantaine. Ils pourront y être soumis à n'importe quelle action (réparation, suppression, etc.).
- **Copies de sauvegarde.** Il est possible de créer un dossier de sauvegarde afin de conserver les copies des objets infectés avant qu'ils ne soient réparés. Cette mesure permettra, le cas échéant, de les restaurer en cas d'échec de la réparation de l'objet.
- **Analyse du système de fichiers du serveur.** En plus du trafic de messagerie, Kaspersky Anti-Virus for Linux/Unix Mail Servers peut réaliser l'analyse à la demande du système de fichiers du serveur. L'analyse est réalisée à l'aide de la technologie unique iChecker qui permet de réduire sensiblement la durée des analyses ultérieures d'un même objet.

Filtrage complémentaire des messages

- **Selon le type de pièce jointe.** Les paramètres de l'application permettent de filtrer le courrier en fonction du nom et du type de fichier en pièce jointe et d'appliquer aux messages ainsi filtrés des règles de traitement particulières.
- **Selon les groupes d'utilisateurs.** L'administrateur peut créer des groupes d'utilisateurs du système de messagerie et définir pour chacun d'entre eux des règles individuelles de traitement des messages ainsi que différentes restrictions.

Souplesse de l'administration

- **Administration à distance.** La configuration de Kaspersky Anti-Virus for Linux/Unix Mail Servers peut s'opérer de manière traditionnelle via le fichier de configuration ou via l'interface Web du logiciel Webmin.
- **Optimisation du fonctionnement de l'application.** Les paramètres de l'application permettent à l'administrateur de contrôler la charge du serveur de messagerie et de modifier en temps opportuns le fonctionnement du système afin d'éviter des pics de charge en cas d'épidémie de virus ou d'attaque par déni de service (DoS). Citons par exemple la configuration de différents délais de connexion pour l'envoi et/ou la réception de messages, la gestion de la file de travail de l'application et la restriction du nombre d'objets analysés simultanément en arrière plan.
- **Configuration du mode de mise à jour.** Les mises à jour des bases antivirus peuvent être réalisées à la demande ou automatiquement selon un horaire défini depuis les serveurs de Kaspersky Lab (Internet) ou des serveurs locaux définis. L'administrateur peut choisir le type de mise à jour utilisée : standard ou étendue (pour l'identification des programmes qui présentent un risque potentiel tels que les logiciels espions).
- **Rapports clairs.** Webmin permet d'afficher sous forme de graphique l'activité virale pour une période donnée. De plus, l'administrateur peut obtenir des informations détaillées sur l'état et le fonctionnement du logiciel grâce à un large éventail de rapports dont le niveau de détail a été prédéfini.

CONFIGURATION REQUISE

Configuration matérielle :

Processeur de classe
Pentium
Au moins 32 Mo de RAM
Au moins 100 Mo d'espace
disque

Configuration logicielle :

Un des systèmes d'exploitation
suivants :
RedHat Enterprise Linux Advanced
Server 3
RedHat 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

Un des programmes de messagerie électronique suivants :

Sendmail 8.x,
Qmail 1.03
Postfix, au moins la version snapshot_
20000529
Exim 4.0
Utilitaire which
Programme Webmin (www.webmin.com)
Perl 5.0 et suivante (www.perl.org) – pour
l'installation de Kaspersky Anti-Virus à l'aide
d'install.pl

Version du logiciel : 5.5

Kaspersky® Mail Gateway

Kaspersky Mail Gateway est une solution universelle pour la protection avancée des utilisateurs des services de messagerie contre les virus et le courrier indésirable.

L'application, qui est installée entre le pare-feu de l'entreprise et Internet, recherche la présence d'éventuels virus dans le courrier, assure un filtrage centralisé du flux de messagerie pour identifier le courrier indésirable et protège les serveurs de messagerie des entreprises contre les utilisations non autorisées.

De par son autonomie, cette application peut s'intégrer à pratiquement n'importe quel milieu. Elle est compatible avec les logiciels antivirus d'autres éditeurs installés sur les autres ordinateurs du réseau et son installation et sa configuration ne requièrent pas une grande connaissance de Linux/Unix.

FONCTIONS

Protection avancée contre les virus et le courrier indésirable

- **Analyse antivirus.** Le programme identifie et supprime tout type de virus dans tous les éléments du courrier entrant et sortant, y compris les pièces jointes.
- **Filtrage du courrier indésirable.** L'application recherche la présence de courrier indésirable dans les flux de messagerie sur la base d'un filtrage selon les signes formels, et en analysant le contenu des messages et des pièces jointes grâce à des technologies intelligentes qui contiennent des signatures graphiques spéciales pour l'identification du courrier indésirable sous forme d'image.
- **Notifications de l'utilisateur.** En cas de découverte d'un objet suspect ou infecté, l'administrateur système, l'expéditeur et le destinataire du message reçoivent un avertissement dont le contenu, le format et la langue sont définis par l'administrateur. Tout message classé comme courrier indésirable peut être bloqué, envoyé en quarantaine ou délivré au destinataire avec un signe spécial dans l'objet du message.
- **Quarantaine.** Les objets infectés et suspects, de même que les messages classés comme courrier indésirable peuvent être placés en quarantaine. L'administrateur pourra les examiner, les supprimer ou les envoyer au destinataire final.

Fonctions complémentaires au niveau du filtrage des messages

- **Selon le type de pièce jointe.** Le filtrage du flux de messagerie peut être organisé en fonction du nom et du type de fichier en pièce jointe. Il est possible ainsi d'isoler directement les objets qui sont à même de contenir des virus.
- **Selon les groupes d'utilisateurs.** L'administrateur peut définir des règles de traitement particulières pour les messages destinés à chaque groupe d'utilisateurs du système de messagerie en fonction de la politique de sécurité et des besoins des employés.

Protection du serveur contre les accès non autorisés

Les paramètres de l'application permettent de résister aux attaques DoS et d'empêcher l'utilisation du serveur par un tiers dans le cadre de la diffusion massive et non autorisée de messages. Dans certains cas, ces mesures accélèrent la vitesse de traitement du flux de messagerie.

Souplesse de l'administration

- **Administration à distance.** Il est possible d'administrer Kaspersky Mail Gateway à distance via un navigateur Internet en utilisant Webmin ou de manière traditionnelle, via le fichier de configuration.
- **Configuration et optimisation du fonctionnement de l'application.** L'administrateur peut modifier le mode de fonctionnement de l'application et passer du niveau de performances maximales du système à la sécurité maximale des utilisateurs. Il est possible également de configurer plus de délais de connexion pour l'envoi et/ou la réception de messages, de gérer la file de travail de l'application et de limiter le nombre d'objets analysés simultanément en arrière plan.
- **Configuration du mode de mise à jour.** Les mises à jour des bases antivirus peuvent être réalisées à la demande ou selon un horaire défini depuis les serveurs de Kaspersky Lab (Internet) ou des serveurs locaux définis. La mise à jour de certains modules du moteur antivirus et du dispositif d'analyse linguistique est également réalisée à ce stade.
- **Rapports clairs.** Webmin permet de consulter les statistiques de l'activité virale sous forme graphique pour une période déterminée, de même que les données relatives aux virus identifiés lors de l'analyse antivirus.

CONFIGURATION REQUISE

Configuration matérielle:

Processeur Intel Pentium (Pentium III ou Pentium IV recommandé)
Au moins 256 Mo de RAM disponible
Au moins 100 Mo d'espace disque disponible pour l'installation de l'application
Au moins 500 Mo d'espace disponible dans le système de fichiers /tmp

Configuration logicielle minimale requise:

Un des systèmes d'exploitation suivants :
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
Debian GNU/Linux 3.0r3
Mandrake Linux (Mandriva) 10.1
FreeBSD 4.10, 5.3

Interprète du langage Perl version 5.0 ou suivante (www.perl.org), utilitaire which pour l'installation de l'application
Programme Webmin (www.webmin.com) version 1.070 ou suivante pour l'administration à distance de l'application

Version du logiciel : 5.5

Kaspersky® Anti-Spam

Kaspersky Anti-Spam est un système intelligent qui met l'utilisateur des messageries électroniques des entreprises à l'abri du courrier indésirable. Le programme est intégré au système de messagerie existant en tant que module complémentaire et réalise le filtrage des messages qui transitent via le protocole STMP avant que ceux-ci ne soient livrés au destinataire final. L'intégration de Kaspersky Anti-Spam à l'infrastructure de réseau existante est simple, quel que soit le système d'exploitation utilisé.

La technologie SpamTest™ est à la base du fonctionnement de Kaspersky Anti-Spam. Cette technologie identifie le courrier indésirable en comparant chaque message à des exemples tirés de la base de données de Kaspersky Lab actualisée toutes les 20 minutes. La comparaison s'opère sur la base de plus de 10 000 descriptions de messages non sollicités, plus de 50 000 expressions uniques en différentes langues (français, anglais, allemand, espagnol, russe) ainsi que des éléments graphiques.

Kaspersky Anti-Spam a été développé pour les entreprises de toute taille, y compris les fournisseurs d'accès Internet.

FONCTIONS

Identification du courrier indésirable à plusieurs niveaux

Kaspersky Anti-Spam intègre un système de filtrage et d'analyse des messages électroniques à plusieurs niveaux :

- Filtrage en fonction des attributs formels : adresse électronique, adresse IP, taille et format du message. Le filtrage s'opère sur la base des listes d'adresses RBL qui regroupent les sources de courrier indésirable ainsi que sur la base des listes "noire" ou "blanche" constituées par l'administrateur.
- Analyse à l'aide du moteur linguistique unique SpamTest™ qui identifie les messages sur la base des exemples repris dans la base de données de Kaspersky Lab qui est actualisée en permanence.
- Les mots ou expressions caractéristiques de tout courrier indésirable sont également analysés.

Lutte contre les formes inhabituelles de courrier indésirable

Kaspersky Anti-Spam permet d'identifier les messages non sollicités qui sont ignorés par les méthodes habituelles. Par exemple, les redoublements de lettres, le remplacement de certains caractères cyrilliques par des caractères latins, l'insertion d'espace ou de point dans les mots. La technique utilisée par Kaspersky Lab permet d'identifier les trucs et astuces HTML (texte invisible, caractères de taille différente, etc.) Kaspersky Anti-Spam fonctionne également avec des signatures graphiques spéciales qui permettent d'analyser les images contenues dans les messages.

Analyse des pièces jointes

Kaspersky Anti-Spam analyse non seulement le texte du message mais également celui de la pièce jointe, notamment les fichiers au format ASCII, HTML, MS Word ou RTF.

Souplesse de la configuration du traitement du courrier

Kaspersky Anti-Spam propose plusieurs profils de filtrage. Il est possible de modifier les profils standards ou de créer des règles de traitement des messages propres aux utilisateurs. Le profil permet à l'administrateur système de régler la sévérité des critères d'évaluation des messages et de choisir diverses variantes pour leur traitement ultérieur.

Tout message non sollicité ainsi découvert, en fonction de sa catégorie, des règles de traitement et des paramètres utilisateur, peut être envoyé au destinataire (sous sa forme originale ou avec des modifications), supprimé ou réorienté vers une autre adresse.

Convivialité de l'administration

La configuration de tous les paramètres du logiciel est réalisée via une interface Web conviviale. L'administrateur est en mesure d'administrer le logiciel depuis n'importe quel point du réseau, de configurer la mise à jour des bases de signatures lexicales et d'y ajouter ses propres exemples de messages non sollicités.

Mises à jour fréquentes

Kaspersky Anti-Spam doit son excellente efficacité à la fréquence des mises à jour, comprises dans le prix du logiciel. Lors de la mise à jour, l'utilisateur obtient les exemples les plus récents de courrier indésirable et d'expressions préparés par les experts du laboratoire linguistique. La diffusion de nouvelles versions du logiciel s'accompagne toujours d'une mise à jour de l'analyseur linguistique.

CONFIGURATION REQUISE

Configuration logicielle:

Linux ou FreeBSD 4.x
Wget et bzip2
Un des programmes de messagerie électronique suivants : Sendmail, Postfix, Exim, Qmail, Communicate Pro

Configuration matérielle:

Processeur Intel Pentium III, 500 Mhz
256 Mo de RAM

Version du logiciel : 2.0

PROTECTION DU TRAFIC HTTP/FTP



Kaspersky Anti-Virus® for Squid

(Disponible courant 2006)

Kaspersky Anti-Virus for Squid est une solution antivirus conçue pour la protection du trafic Internet (HTTP/FTP) sur la base du serveur proxy le plus populaire, à savoir Squid. L'application rend la navigation et le téléchargement de fichiers inoffensifs et protège également l'utilisateur contre la majorité des vers qui se propagent via les systèmes de messagerie instantanée.

FONCTIONS

Protection antivirus et réparation

- **Protection du trafic Internet en temps réel.** L'application s'intègre à Squid Web Proxy Cache grâce au protocole ICAP (Internet Content Adaptation Protocol) et elle assure, en temps réel, l'analyse antivirus de tout le trafic Internet qui transite via le serveur proxy.
- **Notifications.** En cas de découverte d'objets infectés, l'utilisateur est averti par un message HTML dont le format et le contenu sont définis par l'administrateur.
- **Quarantaine.** Les fichiers infectés, suspects et corrompus découverts suite à l'analyse antivirus peuvent être placés en quarantaine. Ils pourront y être soumis à n'importe quelle procédure (réparation, suppression, etc.).
- **Dossier de sauvegarde.** L'application permet de créer une copie de l'objet infecté dans le dossier de sauvegarde avant la réparation et/ou la suppression afin de pouvoir éventuellement le restaurer à la demande au cas où il contiendrait des données importantes.

Administration

- **Administration à distance.** La configuration de Kaspersky Anti-Virus for Squid peut s'opérer de manière traditionnelle via le fichier de configuration ou via l'interface Web du logiciel Webmin. Le système d'administration Webmin permet de régir les privilèges d'accès à l'application.
- **Mise à jour des bases antivirus.** Les mises à jour des bases antivirus peuvent être réalisées à la demande ou automatiquement selon un horaire défini depuis les serveurs de Kaspersky Lab (Internet) ou des serveurs locaux définis. L'administrateur peut choisir le type de mise à jour utilisée : standard ou étendue (pour l'identification des programmes qui présentent un risque potentiel tels que les logiciels espions).

CONFIGURATION REQUISE

Configuration matérielle :

Architecture x86-32 avec processeur Pentium
Au moins 32 Mo de RAM
Au moins 100 Mo d'espace disque

Configuration logicielle :

Un des systèmes d'exploitation suivants :
RedHat Linux 9.0
RedHat Fedora Core 3
RedHat 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
Serveur proxy Squid, version 3.0, avec prise en charge du protocole ICAP
Utilitaire which
Programme Webmin (facultatif) – pour l'administration à distance de Kaspersky Anti-Virus
Perl version 5.0 ou suivante

PROTECTION DES ENTREPÔTS DE FICHIERS



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

Kaspersky Anti-Virus for Linux/Unix File Servers and Workstations est une solution antivirus à deux niveaux conçue pour la protection des serveurs de fichiers de n'importe quel type et des postes de travail. Grâce à l'intégration au système d'exploitation, l'analyse des opérations qui entraînent une modification des fichiers est réalisée en temps réel. Il est possible également de soumettre à l'analyse antivirus le système de fichiers, les disques amovibles ou des fichiers individuels, à la demande ou selon un horaire défini.

FONCTIONS

Protection antivirus et réparation

- **Protection du système en temps réel.** L'application intercepte les requêtes adressées au système de fichiers, recherche la présence de code malveillant dans les fichiers auxquels l'utilisateur accède, répare ou supprime les objets infectés ou isole les objets suspects en vue d'une analyse ultérieure.
- **Analyse à la demande du système de fichiers.** L'application permet également de rechercher les objets suspects ou infectés dans les zones d'analyse spécifiées à une heure définie (ou à la demande de l'administrateur). Ces objets sont analysés, réparés, supprimés ou isolés en vue d'une analyse ultérieure.
- **Quarantaine.** Les fichiers infectés, suspects et corrompus découverts dans le système de fichiers du serveur peuvent être placés en quarantaine. Ils pourront y être soumis à n'importe quelle action (réparation, suppression, etc.).
- **Dossier de sauvegarde.** L'application permet de créer une copie de l'objet infecté dans le dossier de sauvegarde avant la réparation et/ou la suppression afin de pouvoir éventuellement le restaurer à la demande au cas où il contiendrait des données importantes.

Administration

- **Administration à distance.** La configuration de Kaspersky Anti-Virus for Linux/Unix File Servers and Workstations peut s'opérer de manière traditionnelle via le fichier de configuration ou via l'interface Web du logiciel Webmin. Le système d'administration Webmin permet de régir les privilèges d'accès à l'application.
- **Les mises à jour des bases antivirus.** Les mises à jour des bases antivirus peuvent être réalisées à la demande ou automatiquement selon un horaire défini depuis les serveurs de Kaspersky Lab (Internet) ou des serveurs locaux définis. L'administrateur peut choisir le type de mise à jour utilisée : standard ou étendue (pour l'identification des programmes qui présentent un risque potentiel tels que les logiciels espions).

CONFIGURATION REQUISE

Configuration matérielle :

Architecture x86-32 avec processeur Pentium
Au moins 32 Mo de RAM
Au moins 100 Mo d'espace disque

Configuration logicielle :

Un des systèmes d'exploitation suivants :
RedHat Linux 9.0
RedHat Fedora Core 3
RedHat 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
Utilitaire which
Perl version 5.0 ou suivante
Progiciel Webmin (facultatif) pour l'administration à distance de Kaspersky Anti-Virus

Version du logiciel : 5.5

Kaspersky Anti-Virus® for Samba Server

Kaspersky Anti-Virus for Samba Server est une solution qui a été développée pour protéger les entrepôts de fichiers du serveur Samba contre les virus. Samba est un programme qui émule un serveur de fichier Windows sous Linux et qui permet de donner aux clients Windows (utilisateurs) un accès transparent aux données sauvegardées sur le serveur de fichiers Linux. Kaspersky Anti-Virus s'intègre facilement au serveur Samba et ne nécessite pas de réorganisation au niveau du serveur Samba ou d'une partie du système d'exploitation.

FONCTIONS

Protection antivirus et réparation

- **Protection des entrepôts de fichiers du serveur Samba en temps réel.** L'application intercepte les requêtes adressées aux entrepôts de fichiers Samba, recherche la présence de code malveillant dans les fichiers auxquels l'utilisateur accède, répare ou supprime les objets infectés ou isole les objets suspects en vue d'une analyse ultérieure.
- **Analyse à la demande du système de fichiers.** L'application permet également de rechercher les objets suspects ou infectés dans les zones d'analyse spécifiées à une heure définie (ou à la demande de l'administrateur). Ces objets sont analysés, réparés, supprimés ou isolés en vue d'une analyse ultérieure.
- **Technologie d'optimisation de l'analyse antivirus.** L'utilisation de la technologie unique iChecker permet de réduire sensiblement la durée des analyses ultérieures d'un même objet car seuls les objets qui ont été modifiés depuis la dernière analyse sont analysés.
- **Quarantaine.** Les fichiers infectés, suspects et corrompus découverts dans le système de fichiers du serveur peuvent être placés en quarantaine. Ils pourront y être soumis à n'importe quelle action (réparation, suppression, etc.).
- **Dossier de sauvegarde.** L'application permet de créer une copie de l'objet infecté dans le dossier de sauvegarde avant la réparation et/ou la suppression afin de pouvoir éventuellement le restaurer à la demande, au cas où il contiendrait des données importantes.

Administration

- **Administration à distance.** La configuration de Kaspersky Anti-Virus for Samba server peut s'opérer de manière traditionnelle via le fichier de configuration ou via l'interface Web du logiciel Webmin. Le système d'administration Webmin permet de régir les privilèges d'accès à l'application.
- **Mise à jour des bases antivirus.** Les mises à jour des bases antivirus peuvent être réalisées à la demande ou automatiquement selon un horaire défini depuis les serveurs de Kaspersky Lab (Internet) ou des serveurs locaux définis. L'administrateur peut choisir le type de mise à jour utilisée : standard ou étendue (pour l'identification des programmes qui présentent un risque potentiel tels que les logiciels espions).

CONFIGURATION REQUISE

Configuration matérielle :

Architecture x86-32 avec processeur Pentium
Au moins 32 Mo de RAM
Au moins 100 Mo d'espace disque

Configuration logicielle :

Un des systèmes d'exploitation suivants :
RedHat 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 ou suivante
Utilitaire which
Perl version 5.0 ou suivante
Progiciel Webmin (facultatif) pour
l'administration à distance de Kaspersky
Anti-Virus

Version du logiciel : 5.0

Services

Les services qui accompagnent chacun de nos logiciels constituent l'une des principales caractéristiques de Kaspersky Lab. Les utilisateurs enregistrés reçoivent les mises à jour des bases antivirus toutes les heures, ils peuvent télécharger gratuitement les mises à jour des logiciels installés et contacter le service d'assistance technique. Des services complémentaires sont prévus pour les entreprises.

Mise à jour des bases et version

La fréquence de la mise à jour des bases est le garant de l'excellence des logiciels édités par "Kaspersky Lab". A l'heure actuelle, les bases antivirus sont actualisées toutes les heures, tandis que les bases antispam sont mises à jour toutes les 20 minutes.

Assistance technique

En cas de situation d'urgence, les utilisateurs des logiciels de Kaspersky Lab peuvent compter sur notre service d'assistance technique. Nos opérateurs peuvent être contactés par téléphone ou par courrier électronique. Les services sont offerts en français, en anglais, en allemand et en russe.

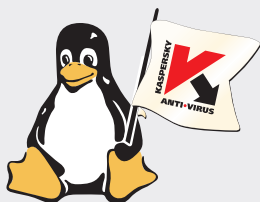
Services gratuits pour tous

Tout internaute qui visite notre site peut rechercher en ligne la présence éventuelle de virus dans n'importe quel fichier. Nous offrons à nos clients potentiels des versions d'évaluation qui permettent de tester nos produits en conditions réelles. Lorsqu'une épidémie mondiale éclate, nous diffusons des utilitaires de réparation gratuits accessibles à tous.

Kaspersky Lab propose non seulement des logiciels mais également des informations par le biais de l'Encyclopédie des virus qui propose une description détaillée des programmes malveillants de tout type. Les communiqués de presse que nous publions permettent aux utilisateurs d'être toujours au courant des dernières épidémies.

Services complémentaires offerts aux entreprises

Kaspersky Lab a mis sur pied un ensemble de services complémentaires pour nos clients professionnels. La relation avec les grands comptes est individuelle. Nous étudions et analysons le réseau, installons le système antivirus, assurons la formation du personnel et le déploiement du système de sécurité.





● Kaspersky Lab

Russie, Moscou 125363
ul. Geroev Panfilovtsev, 10;
www.kaspersky.ru
Courrier électronique :
sales@kaspersky.com
Tél. : +7 095 797 8700

● Kaspersky Lab France

Immeuble l'Européen
ZAC Rueil 2000
2, Rue Joseph MONIER
92 500 Rueil Malmaison
www.kaspersky.fr
Courrier électronique: info@fr.kaspersky.com
Tél. : +33 825 888 612

● Kaspersky Lab USA

300 Unicorn Park
Woburn, MA 01801, USA
www.kaspersky.com
Courrier électronique: info@us.kaspersky.com
Tél. : +1 781 503 1800

● Kaspersky Lab UK

Culham Innovation Centre
D5 Culham Science Centre
Abingdon OX14 3DB
Royaume-Uni
www.kaspersky.co.uk
Courrier électronique:
sales@kasperskylab.co.uk
Tél. : +44 0 870 0113461

● Kaspersky Lab Germany

Neuburger Str.57
S-85057, Ingolstadt
Allemagne
www.kaspersky.de
Courrier électronique:
info@kaspersky.de
Tél. : +49 841 98189 0

● Kaspersky Lab Benelux

Havensingel 1A
5211 TX's-Hertogenbosh
Pays-Bas
www.kasperskylab.nl
Courrier électronique:
sales@bnl.kaspersky.com
Tél. : +31 0 73 6154860

● Kaspersky Lab Poland

Ul. Krotka 27A, 42-200
Czestochowa, Pologne
www.kaspersky.pl
Courrier électronique:
info@kaspersky.pl
Tél. : +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, Chine
www.kaspersky.cn
Courrier électronique:
sales@kaspersky.com.cn
Tél. : +86 10 5861 2570

● Kaspersky Lab Japan

Iwamoto Bldg. 4F 3-2-3
Iwamoto-cho, 101-0032
Chiyoda-ku, Tokyo, Japon
www.kaspersky.co.jp
Courrier électronique:
sales@kaspersky.co.jp
Tél. : +81 3 5687 7839

Kaspersky® Anti-Virus est une marque déposée de Kaspersky Lab Ltd.
Toutes les autres marques citées sont déposées par leurs propriétaires respectifs.

Copyright © 2005 Kaspersky Lab Ltd.

Novembre 2005