kaspersky BRING ON THE FUTURE*

Kaspersky® Security for Mail Server

Protection nouvelle génération des e-mails professionnels

Le courrier électronique est le premier vecteur de programmes malveillants menaçant la sécurité informatique des entreprises.[1]
Kaspersky Security for Mail Server utilise des méthodes heuristiques avancées, le sandboxing, le Machine Learning ainsi que d'autres technologies nouvelle génération pour protéger les emails des pièces jointes malveillantes, du spam, du phishing et des menaces inconnues.

Protégez votre entreprise des dommages sur vos finances, vos opérations et votre réputation, causés par les attaques visant les systèmes de messagerie électronique, grâce à la solution de sécurité la plus testée et la plus récompensée au monde.

Plus de la moitié des e-mails envoyés sont du spam. Augmentez votre productivité et réduisez les menaces grâce à une protection contre le spam de nouvelle génération, hébergée dans le Cloud.

Le système anti-spam nouvelle génération de Kaspersky Lab, hébergé dans le Cloud, détecte les emails indésirables inconnus, même les plus sophistiqués, en réduisant au minimum la perte de messages importants due aux faux positifs. La possibilité de réduire le temps perdu ainsi que les risques liés aux spams en les bloquant, permet d'économiser les ressources système et humaines.

Diminution du coût de possession

Kaspersky Security for Mail Server est très simple d'utilisation. Les scénarios de configuration du filtrage étant très souples, l'adéquation à vos processus d'entreprise est parfaitement assurée, ce qui réduit les ressources nécessaires.

Souplesse dans le choix des licences pour les petites et moyennes entreprises

Kaspersky Security for Mail Server est disponible en souscrivant à une licence annuelle ou à un abonnement mensuel.

Avantageux pour les fournisseurs de services managés (MSP)

Les MSP sont de plus en plus nombreux à intégrer la cybersécurité à leur offre de services. Kaspersky Security for Mail Server prend donc en charge des fonctionnalités de gestion multi-clients, propose des licences flexibles, et la surveillance de l'état général des systèmes dont a besoin le support de premier niveau d'un fournisseur de services managés.

Avantages

- Protection contre les programmes malveillants nouvelle génération en temps réel et à la demande
- Intégration bidirectionnelle de Kaspersky Anti Targeted Attack Platform
- Protection spécialisée contre les menaces sophistiquées par phishing, y compris les attaques de la messagerie d'entreprise
- Disponible sous forme de licence mensuelle pour les utilisateurs finaux et les MSP
- Protection contre les menaces de type « zero-hour »
- Associé à la Threat Intelligence mondiale issue de Kaspersky Security Network
- Prend en charge Microsoft Active Directory et lLDAP
- Gestion de la quarantaine pour les e-mails et les pièces jointes
- Traitement des macros malveillantes intégrées ainsi que d'autres objets malveillants
- Bloque les ransomwares délivrés par email et les logiciels malveillants de type Trojan miner

1 Verizon : rapport d'enquêtes sur la violation des données, 2017.

*Bienvenue dans le futur

Fonctionnalités

Protection multi-niveaux contre les programmes malveillants grâce à la surveillance HuMachine™

La protection nouvelle génération de Kaspersky Lab contre les programmes malveillants intègre plusieurs niveaux de sécurité proactive, y compris le Machine Learning et la Threat Intelligence dans le Cloud, pour filtrer les pièces jointes et les programmes malveillants, que ces derniers soient connus ou non. Des analyses en temps réel et à la demande sont disponibles, la deuxième catégorie étant particulièrement utile dans le cadre de scénarios de migration.

Threat Intelligence de niveau mondial
Kaspersky Security for Mail Server analyse des données du monde entier pour établir le panorama des menaces le plus récent, alors même que celui-ci évolue en permanence.

- **Machine Learning**
  Le « Big Data » issu de la Threat Intelligence mondiale est traité grâce à la puissance des algorithmes du Machine Learning conjuguée à l'expertise humaine, assurant par là même des niveaux de détection élevés avec un minimum de faux positifs.
- **Sandboxing émulatif**
  Pour une protection sûre contre les programmes malveillants les plus sophistiqués et les plus habilement dissimulés, les pièces jointes sont exécutées dans un environnement émulé sécurisé, au sein duquel elles sont analysées pour s'assurer qu'aucune instance dangereuse n'infecte le système de l'entreprise.

Système anti-spam robotisé (avec contenu réputationnel)

Le système anti-spam de Kaspersky Lab utilise des modèles de détection issus du Machine Learning. Pour minimiser le risque de faux positifs et s'adapter aux changements dans l'environnement à risques, le traitement robotisé des spams est supervisé par les experts de Kaspersky Lab, partie intégrante de la structure Kaspersky HuMachine™.

Protection avancée contre le phishing et les attaques de la messagerie d'entreprise

Pour des modèles de détection efficaces, le système anti-phishing avancé de Kaspersky Lab est fondé sur une analyse issue de réseaux de neurones artificiels. S'appuyant sur plus de 1 000 critères, incluant images, contrôles linguistiques et scripts particuliers, cette méthode hébergée dans le Cloud est alimentée par les données mondiales relatives aux URL malveillantes ou de phishing, pour fournir une protection contre les emails de phishing « zero-hour », connus ou non. Des algorithmes spécialisés ciblent les menaces d'attaque de la messagerie d'entreprise.

Gestion de l'authentification des e-mails

Des mécanismes d'authentification fiables des expéditeurs tels que SPF, DKIM et DMARC contribuent à la protection contre l'usurpation des sources. Cela est particulièrement utile dans le cas d'e-mails professionnels compromis.

Filtrage des pièces jointes

Certains types de pièces jointes représentent un trop gros risque pour être admis dans le périmètre de sécurité de l'entreprise. Le système de filtrage des pièces jointes Kaspersky Lab permet de configurer de façon très souple la politique relative à la livraison des dites pièces et détecte plusieurs modes de dissimulation de fichier couramment utilisés par les cybercriminels. Ces fonctionnalités contribuent à réduire les risques de fuite de données.

Sauvegarde intégrée

Pour s'assurer qu'aucune donnée critique n'est perdue en raison d'actions de désinfection ou de suppression, les messages d'origine sont enregistrés dans un stockage de sauvegarde pour être traités par l'administrateur au moment opportun. La sauvegarde conditionnelle des données peut être configurée selon des règles spécifiques.

Intégration de Kaspersky Anti Targeted Attack (KATA)

L'intégration bidirectionnelle de la solution puissante Anti-APT et EDR de Kaspersky Lab permet d'utiliser les systèmes de messagerie comme sources d'informations supplémentaires pour détecter les attaques ciblées et peut également bloquer d'autres messages comportant des contenus dangereux sur la base de l'analyse en profondeur effectuée par la solution Kaspersky Lab.

Approche Kaspersky HuMachine™
Basé sur la Threat Intelligence à partir du Big Data, le Machine Learning et l'expertise humaine, Kaspersky HuMachine™ présente de nombreux avantages et assure une protection plus efficace. En combinant chaque élément, les composants individuels gagnent en puissance pour proposer une solution encore plus efficace.

Applications incluses
- Kaspersky Security for Linux Mail Server
- Kaspersky Secure Mail Gateway
- Kaspersky Security for Microsoft Exchange Server
- Kaspersky Security Center

Comment acheter
Kaspersky Security for Mail Server est disponible en souscrivant à une licence annuelle ou à un abonnement mensuel. Il est inclus dans Kaspersky Total Security for Business, mais il est également possible de l'acheter séparément. N'hésitez pas à contacter votre revendeur Kaspersky Lab ou votre distributeur agréé ; il vous aidera à choisir le produit le plus adapté à votre situation.

www.kaspersky.fr
#truecybersecurity