Kaspersky® Security for Mail Server

Protection nouvelle génération des e-mails professionnels

Le courrier électronique est le premier vecteur des 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 de nouvelle génération pour protéger les e-mails des ransomwares, des pièces jointes malveillantes, des courriers indésirables, du phishing et des menaces inconnues.

Protégez votre entreprise des dommages financiers, opérationnels et réputationnels causés par les attaques contre les systèmes de messagerie électronique grâce à la solution de sécurité la plus primée et la plus testée au monde.

Avantages

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

L'Anti-Spam dans le Cloud nouvelle génération de Kaspersky Lab détecte les courriers indésirables inconnus, même les plus sophistiqués, en réduisant au minimum les messages perdus en raison de faux positifs. La possibilité de réduire le temps perdu, ainsi que les risques liés aux courriers indésirables en les stoppant 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.

Assurez la conformité de votre entreprise en protégeant les données sensibles

Kaspersky Security for Mail Server, avec option de prévention des pertes de données (DLP), identifie les données commerciales, financières, personnelles ainsi que les autres informations sensibles contenues dans les e-mails sortants ou dans les pièces jointes sur les serveurs Microsoft Exchange. Cette solution garantit la confidentialité de vos données d'entreprise, de celles de vos associés et de vos clients, conformément à la législation sur la protection des données. Des techniques analytiques sophistiquées, y compris les recherches de données structurées et les glossaires spécifiques à l'entreprise, permettent d'identifier et de bloquer les e-mails suspects tout en avertissant la personne concernée de l'incident (p. ex. le ou la Data Protection Officer).

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

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

Avantages pour les fournisseurs de services gérés (MSP)

Les MSP sont de plus en plus nombreux à proposer la cybersécurité dans leur offre de services. Kaspersky Security for Mail Server prend en charge des fonctionnalités de gestion multi-clients, des méthodes souples de licence et la surveillance de l'état général des systèmes dont a besoin l'assistance de premier niveau d'un fournisseur de services gérés.

Points forts

- Protection contre les programmes malveillants nouvelle génération en temps réel et à la demande
- Intégration bidirectionnelle de Kaspersky Anti Targeted Attack Platform
- La gestion de l'authentification des e-mails contribue à la lutte contre les e-mails professionnels compromis
- Disponible sous forme de licence mensuelle pour les utilisateurs et les MSP
- Protection contre les menaces de type « zero-hour »
- Adossé à la veille stratégique mondiale sur les menaces issue de Kaspersky Security Network
- Prend en charge Microsoft Active Directory et le serveur LDAP
- Gestion de la quarantaine pour les e-mails et les pièces jointes
- Traitement des macros malveillantes intégrées ainsi que d'autres objets malveillants
- Blocage des ransomwares distribués par e-mail
- Protection contre les fuites de données (pour les utilisateurs de MS Exchange)

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

Fonctionnalités

HuMachine™, protection multi-niveaux contre les programmes malveillants

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, associés à des e-mails entrants. Des analyses en temps réel et sur demande sont disponibles, la deuxième catégorie étant particulièrement utile dans le cadre de scénarios de migration.

- **Threat Intelligence mondiale :**
  Kaspersky Security for Mail Server exploite des données du monde entier pour obtenir la vision la plus récente de l'environnement à risques, alors même que celui-ci évolue.
- **Machine learning (ou apprentissage automatique) :**
  Le « big data » issu de la Threat Intelligence mondiale est traité grâce à la puissance des algorithmes de machine learning combinée à l'expertise humaine, assurant par là même des niveaux de détection élevés en minorant les faux positifs.
- **Sandboxing imitatif :**
  Pour une protection sûre contre les programmes malveillants les plus sophistiqués et les plus habilement dissimulés, les pièces jointes sont exécutées dans un environnement imitatif 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 exploite largement les 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™.

Système anti-phishing avancé

Pour la détection efficace des modèles, le système anti-phishing avancé de Kaspersky Lab est fondé sur une analyse issue de réseaux de neurones artificiels. Utilisant plus de 1 000 critères, dont des images, des contrôles linguistiques et des scripts particuliers, cette approche dans le Cloud est alimentée par les données mondiales portant sur les URL malveillantes ou de phishing pour fournir une protection contre les e-mails de phishing « zero-hour », connus ou non.

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 de pièces jointes de Kaspersky Lab permet de configurer de façon très souple la politique relative à la livraison des pièces jointes et détecte plusieurs modes de dissimulation de fichier couramment utilisés par les cybercriminels. Ces fonctionnalités contribuent à réduire les risques de fuite de données.

Prévention des fuites de données

Les utilisateurs de Microsoft Exchange sont en mesure de gérer les informations confidentielles contenues dans des e-mails ou dans des pièces jointes par catégories (y compris les informations personnelles et les données de carte de paiement), par glossaires (y compris les packs conformité prêts à l'emploi) et en fonction de l'analyse approfondie effectuée au moyen de données structurées (la prévention des fuites de donnée est limitée aux serveurs Microsoft Exchange).

Sauvegarde intégrée

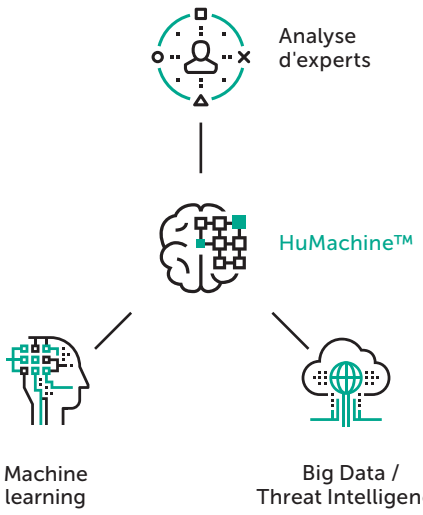
Pour s'assurer qu'aucune donnée critique n'est perdue en raison d'actions de désinfection ou de suppression, les messages d'origine sont enregistrés dans un stockage de sauvegarde pour être traités par l'administrateur au moment opportun. La sauvegarde conditionnelle des données peut être configurée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

Intégration de Kaspersky Anti Targeted Attack

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, les capacités de machine learning et l'expertise humaine, Kaspersky HuMachine™ offre 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.



2 La fonction optionnelle de prévention des fuites de données de Kaspersky Security pour les serveurs Microsoft Exchange est vendue séparément.

Applications incluses

- Kaspersky Security for Linux Mail Server
- Kaspersky Security for Microsoft Exchange Server
- Kaspersky Anti-Virus for Lotus Notes/Domino
- Kaspersky Security Center

Comment acheter

Kaspersky Security for Mail Server est disponible en souscrivant à une licence annuelle ou à un abonnement mensuel.
Le produit peut être acheté séparément ou comme une composante de Kaspersky Total Security for Business.[2]
Pour vous aider à choisir le produit le plus adapté, veuillez consulter un revendeur Kaspersky Lab ou un distributeur agréé.

www.kaspersky.fr
#truecybersecurity