KASPERSKY lab

SOLUTION DE PROTECTION DE NOUVELLE GÉNÉRATION POUR MESSAGERIES

d'e-mails sont envoyés chaque seconde.

Il suffit d'un seul e-mail pour compromettre votre entreprise.

Microsoft Office 365 est confronté aux cybermenaces 24 h/24 et 7 jours/7

La plupart des entreprises ont consacré du temps et de l'énergie à la formation des utilisateurs face aux e-mails suspects. Mais que pouvez-vous faire quand les cybercriminels et les spammeurs modifient constamment leur stratégie ?

Lorsque le courrier électronique est le premier vecteur des programmes malveillants menaçant les entreprises[1], s'appuyer sur des paramètres de sécurité intégrés ou par défaut pour vous protéger présente un risque.

Kaspersky Security for Microsoft Office 365 aide votre entreprise à détecter et bloquer les spams et les e-mails malveillants avant qu'ils ne deviennent un problème, sans impact négatif sur la productivité, ni suppression accidentelle de trafic légitime.

Comme Microsoft Office 365, il est hébergé dans le Cloud. Et comme toutes les autres solutions de Kaspersky Lab, il repose sur les produits de sécurité les plus testés et les plus récompensés au monde.

1 : Rapport d'enquêtes sur la violation des données de Verizon, 2017

Courriers indésirables : bien plus qu'une simple nuisance

De la bande passante à la perte de productivité, le spam représente bien plus qu'une simple nuisance pour l'entreprise : les salariés consacrent en moyenne 13 heures chaque année à l'analyse et à la suppression des spams.[2]

Et que dire du temps perdu à rechercher les e-mails professionnels légitimes pris à tort pour du spam ? Les e-mails bloqués sont une chose, mais c'est encore pire lorsque les messages sont automatiquement supprimés : un problème courant avec les paramètres de sécurité intégrés des messageries dans le Cloud.

Et tout cela avant même de prendre en compte le fait que de nombreux spams contiennent un programme malveillant. 58 % de l'ensemble des messages électroniques sont du spam. Pourquoi perdre le temps, les ressources et l'argent que vous avez économisés pour migrer vers le Cloud à traiter des messages indésirables dont personne ne veut ?

2 : Atlassian : Time Wasting At Work (Perte de temps au travail)

Technologies de protection contre les courriers indésirables

Kaspersky Security for Microsoft Office 365 utilise une technologie de détection et d'analyse des spams de nouvelle génération qui repose sur le machine learning ainsi que sur la surveillance en temps réel, basée dans le Cloud, assurée par Kaspersky Security Network. Cette technologie vise à détecter et bloquer les attaques de spam en constante évolution.

Système anti-spam robotisé avec contenu réputationnel

Le système anti-spam de Kaspersky Lab est basé sur les modèles de détection issus du machine learning. Le traitement robotisé des spams, qui est supervisé par les experts de Kaspersky Lab, permet de détecter efficacement les courriers indésirables inconnus, même les plus sophistiqués, et de réduire au minimum les messages importants perdus en raison de faux positifs.

Prise en charge de l'authentification des e-mails

Le spoofing/usurpation est l'un des principaux outils qu'utilisent les spams d'ingénierie sociale malveillants et frauduleux. Sender Policy Framework (SPF) vérifie que les e-mails entrants qui semblent provenir de sources dignes de confiance sont authentiques, ce qui réduit ainsi considérablement le risque d'usurpation.

Kaspersky Security Network

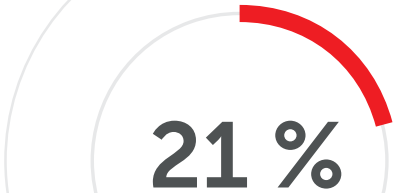
Kaspersky Security Network recueille des informations quasiment en temps réel sur les nouveaux spams provenant du monde entier, ce qui permet de réagir immédiatement à tout courrier indésirable inconnu, y compris les courriers indésirables « zero hour » et les nouvelles épidémies. La collecte s'effectue automatiquement, sans nécessiter l'intervention de personnel informatique, et permet de prévenir les infections et les « inondations » de messages.

MassMail

Les messages provenant d'une source de confiance peuvent présenter certains attributs caractéristiques du spam, sans pour autant être de vrais courriers indésirables, et peuvent même être utilisés à des fins professionnelles. Pour garantir la productivité des salariés, ces messages peuvent être identifiés comme des messages MassMail (courrier de masse) ou transférés dans un dossier spécial, plutôt que de les supprimer purement et simplement.

Phishing : la menace est dans le courrier

Les cybercriminels utilisent les e-mails pour lancer leurs attaques car c'est le moyen le plus rapide et le plus direct pour atteindre le cœur de toutes les entreprises.



21 % des cyberincidents signalés impliquent une certaine forme de phishing[3]

Ils savent également que, malgré tous vos efforts pour former les utilisateurs, un courrier bien « camouflé » suffit généralement pour inciter un utilisateur, même prudent, à cliquer sur une pièce jointe ou un lien malveillant. Les attaques de phishing se présentent généralement sous la forme d'e-mails ayant l'apparence de communications légitimes, conçus pour inciter les utilisateurs à cliquer sur une pièce jointe ou un lien malveillant. Nous les avons tous déjà vus : OFFRE SPÉCIALE ! RETARD DE PAIEMENT ! LA LIVRAISON DE VOTRE COLIS EST RETARDÉE ! Ils ne sont pas simplement conçus pour inciter les utilisateurs à cliquer sans réfléchir, ils utilisent délibérément des techniques et un langage persuasifs qui les rendent convaincants.

Le phishing ciblé va encore plus loin. Beaucoup plus ciblé, il vise généralement des collaborateurs bien spécifiques d'une entreprise, avec des e-mails et des pièces jointes qui ressemblent à s'y méprendre à des communications légitimes : un mail de candidature à un poste, transmis au responsable de recrutement spécifiquement nommé, qui se réfère à une annonce d'emploi légitime, ou bien une facture envoyée à la personne adéquate du service de comptabilité, provenant d'une société qui fait effectivement affaire avec vous.

Plus récemment, nous avons assisté à l'apparition des « e-mails professionnels compromis » : des messages qui semblent provenir de collaborateurs au sein de votre propre entreprise, par exemple le PDG. Il s'agit généralement « d'autoriser » un transfert d'argent ou de solliciter des données sensibles. Parce qu'elles sont très finement conçues, ces attaques réussissent souvent à passer malgré les spam traps. Ils ne sont pas envoyés en grand nombre et ne sont habituellement transmis qu'à quelques salariés bien choisis.

En masquant une extension de fichier ou en « maquillant » une adresse e-mails pour que le message semble provenir du PDG, les cybercriminels peuvent facilement exploiter une faille de sécurité.

3 : Rapport d'enquêtes sur la violation des données de Verizon, 2017

Technologies antiphishing

Kaspersky Security for Microsoft Office 365 utilise le sandboxing et le machine learning pour filtrer les menaces, même inconnues, avant que les utilisateurs ne puissent commettre une erreur. Même lorsqu'une extension de fichier est masquée, la reconnaissance des types de fichiers authentiques détecte et bloque l'attaque.

Les technologies antiphishing nouvelle génération de Kaspersky Security for Microsoft Office 365 protègent les e-mails des menaces inconnues et avancées, sans impact sur la productivité :

Moteur antiphishing basé sur les réseaux de neurones artificiels

Fournit une protection contre les e-mails de phishing inconnus et de type « zero-hour » en utilisant plus de 1 000 critères pour établir les modèles de détection. Nos bases de données sur les menaces, constamment mises à jour et prises en charge par Kaspersky Security Network, fournissent une protection contre les URL malveillantes et autres menaces liées au phishing.

Threat Intelligence liée aux URL de phishing et malveillantes

Prises en charge par Kaspersky Security Network (notre réseau de veille stratégique dans le Cloud), les bases de données continuellement mises à jour sont alimentées par des données détectées automatiquement ainsi que par des recherches sur les menaces menées par des experts.
Cela permet d'empêcher les attaques de point d'eau et les infections par téléchargement « drive-by », ainsi que la fraude via les sites Web malveillants.

Supprimer, déplacer ou identifier des messages de phishing :

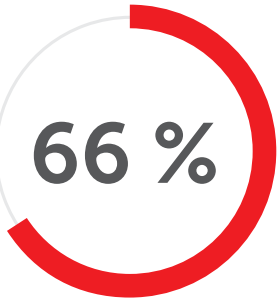
Les messages non sollicités ne sont pas tous des courriers indésirables ; leur suppression automatique peut entraîner des problèmes de productivité ou avoir un impact sur des communications potentiellement utiles. La solution anti-phishing de Kaspersky Lab facilite le filtrage basé sur les balises et utilise des balises personnalisées pour signaler des courriers de masse potentiellement utiles. Ces messages sont alors déplacés vers le dossier Courrier indésirable, mais ne sont pas supprimés.

Analyse des pièces jointes prévisualisées :

Grâce à ce système unique, protégez-vous contre les attaques par phishing avancées. Cette fonction analyse les pièces jointes qui peuvent être prévisualisées, y compris les fichiers PDF, RTF et MSOffice, pour détecter du contenu de phishing.

Programmes malveillants : ransomwares, failles de type « zero-hour » et pièces jointes suspectes

66 % des programmes malveillants sont installés à partir de pièces jointes malveillantes.[4] Les attaques de type « zero-hour » ou « zero-day » sont souvent dissimulées dans des fichiers Word, Excel, PowerPoint et autres applications d'entreprise, attendant simplement que l'utilisateur clique dessus.

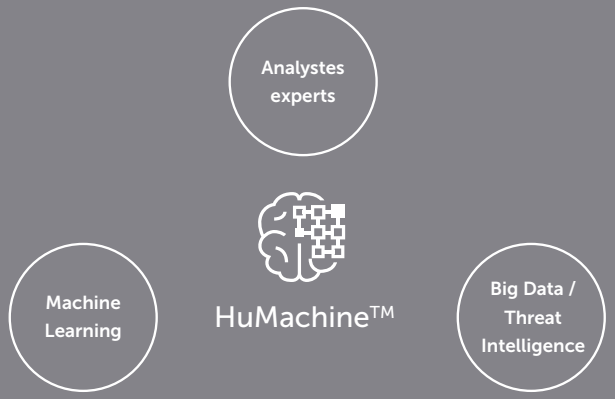


des programmes malveillants sont installés à partir de pièces jointes malveillantes

Dans de nombreux cas, les pièces jointes malveillantes contiennent des programmes malveillants conçus pour dérober des données d'authentification ou des identifiants de connexion à l'aide de logiciels espions ; le programme malveillant est installé à l'insu de l'utilisateur. Parmi les autres attaques courantes liées aux pièces jointes, figure le ransomware : une fois le programme lancé, les données de l'utilisateur sont chiffrées et une rançon est demandée.

Qu'est-ce que HuMachine™ ?

HuMachine© de Kaspersky Lab combine le meilleur de l'expertise humaine au machine learning et à la Threat Intelligence à partir du big data pour défendre une entreprise contre tous les types de menaces auxquels elle est confrontée.



4 : Rapport d'enquêtes sur la violation des données de Verizon, 2017.

Technologies de défense contre les programmes malveillants

Kaspersky Security for Microsoft Office 365 utilise le sandboxing et le machine learning pour déterminer la véritable nature d'une pièce jointe ou d'un fichier avant d'en autoriser la réception. Les fichiers suspects peuvent être exécutés dans un espace sûr pour déterminer s'il s'agit ou non d'un programme malveillant avant d'en autoriser la réception.

Détection multi-niveau des menaces grâce à la surveillance HuMachine

Les capacités de détection éprouvées de Kaspersky Lab intègrent plusieurs niveaux de sécurité proactive qui filtrent les pièces jointes malveillantes associées aux e-mails. Les modèles de détection issus du machine learning filtrent les programmes malveillants « zero-hour » jusque-là inconnus.

Kaspersky Security Network

Basé dans le Cloud, notre réseau mondial de veille stratégique sur les menaces utilise des données réelles anonymisées provenant de plus de 60 millions de sondes de terminaux dans le monde. Nous garantissons ainsi des délais d'intervention très rapides et des niveaux de protection maximum, alors même que le paysage des menaces évolue.

Filtrage des pièces jointes

Bloquez les fichiers dangereux avant qu'ils ne deviennent un problème et gérez les messages indésirables. La reconnaissance du type de fichier réel empêche la réception des fichiers malveillants qui se font passer pour des fichiers sains. Le filtrage des pièces jointes par extension permet de bloquer ou d'identifier des types de fichiers indésirables, tandis que la détection des virus macro permet de prendre les mesures qui s'imposent sur les fichiers Office potentiellement dangereux contenant des macros activées. Les exclusions flexibles et le marquage permettent de réduire la perte de messages légitimes pris en compte par les critères de filtrage.

Protection de nouvelle génération économique et facile à gérer

Vous avez choisi le Cloud pour plus de commodité, d'efficacité des ressources et de rentabilité. Avec Kaspersky Security for Microsoft Office 365, vous n'avez besoin de sacrifier aucun de ces éléments au détriment de la sécurité du courrier électronique. Une seule et même console d'administration intuitive vous permet de tout gérer et offre une vue unique des menaces détectées et des statistiques. Vous n'aurez pas à acheter de matériel supplémentaire et votre personnel n'aura pas besoin d'une formation spéciale. Vous n'aurez même pas besoin d'installer un programme de distribution.

Cette console est conçue pour vous permettre de vous protéger sans ralentir ou sans supprimer accidentellement le trafic de messagerie légitime :

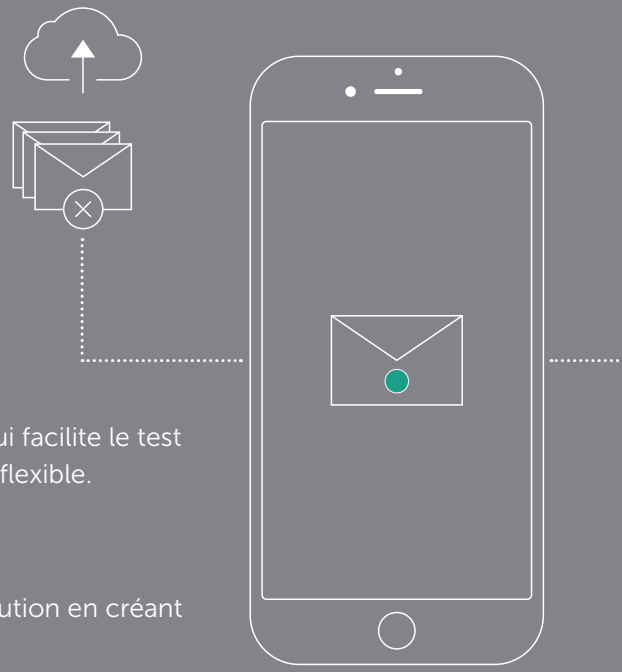
Gestion, administration et intégration simplifiées

Tableau de bord « en un clin d'œil » :

Un seul écran pour la surveillance quotidienne, hebdomadaire ou mensuelle et le statut des menaces, les statistiques, les détections, etc.

Configuration simplifiée :

Tous les paramètres sont regroupés sur un seul et même écran pour simplifier au maximum la configuration et le contrôle.



Test avant le déploiement :

Choisissez les boîtes aux lettres à protéger, ce qui facilite le test de configuration ou l'application d'une stratégie flexible.

Solution multi-clients :

Autorisez plusieurs administrateurs à gérer la solution en créant différents comptes.

Sauvegarde :

De nombreux utilisateurs ont déjà subi la détection comme spam d'e-mails tout à fait légitimes. Grâce à un nombre moins important de faux positifs et à un contrôle administrateur du traitement des e-mails suspects, Kaspersky Security for Microsoft Office 365 réduit considérablement les risques d'erreur en matière d'identification des e-mails. Les messages supprimés sont sauvegardés et peuvent être recherchés et restaurés : finie la disparition d'e-mails !

Notification :

Assurez une intervention rapide suite à un incident via des notifications à l'administrateur en cas de spams, de phishing, d'attaques de virus ou de violations de la politique liée aux pièces jointes.

Authentification unique :

Une seule console et une option d'authentification unique pour gérer la sécurité des différents terminaux, appareils et Exchange Online.

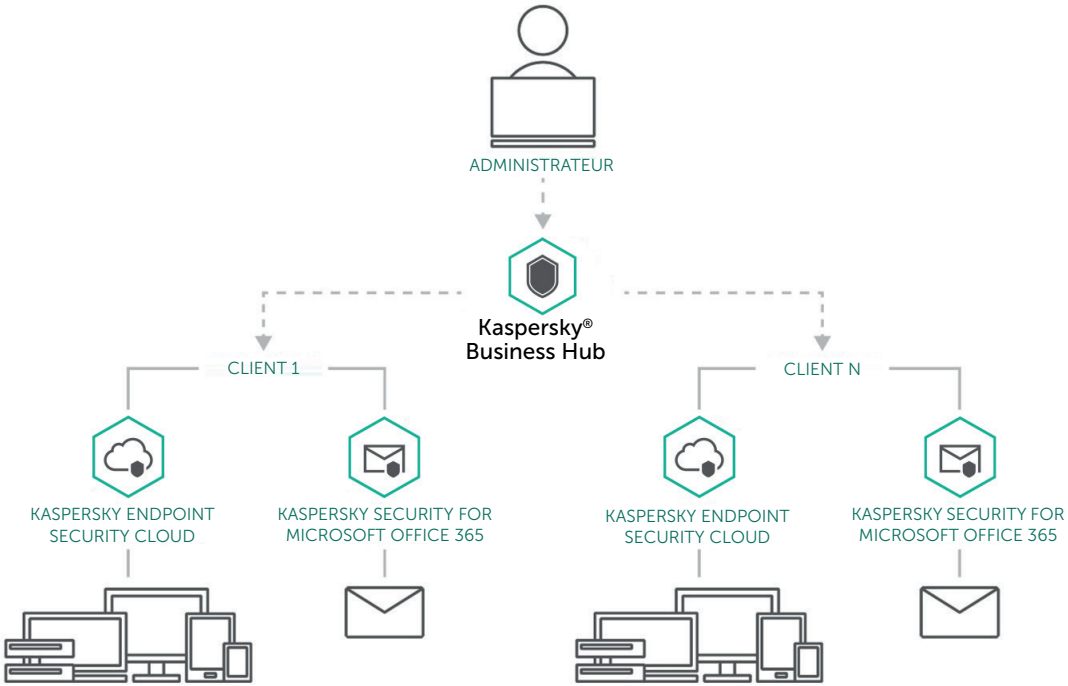
Kaspersky® Business Hub

Kaspersky Business Hub : une console unique pour gérer la protection de votre société.

Testez notre interface intuitive, notre gestion simplifiée et notre protection de qualité supérieure, pour différents appareils et outils. Il suffit de vous connecter à partir de l'appareil de votre choix : vous maîtrisez la situation partout et à tout moment.

Les produits suivants sont gérés depuis le Kaspersky Business Hub :

- Kaspersky Endpoint Security Cloud
- Kaspersky Security for Microsoft Office 365



Kaspersky® Security for Microsoft Office 365

Quand il s'agit de protéger votre messagerie Microsoft Office 365, la meilleure stratégie est de s'assurer que les menaces sont détectées et bloquées avant qu'elles ne deviennent un problème.

Kaspersky Security for Microsoft Office 365 est conçu pour vous permettre de vous protéger sans ralentir ou sans supprimer accidentellement le trafic de messagerie légitime.

Découvrez comment nos technologies de sécurité nouvelle génération peuvent rendre votre messagerie Microsoft Office 365 encore plus facile à sécuriser et à gérer.

Testez la solution gratuitement sur cloud.kaspersky.com