Kaspersky® Web Traffic Security

Une défense stratégique pour l'ensemble de votre réseau

Le serveur proxy est un entonnoir naturel pour le trafic Web entre l'infrastructure de l'entreprise et le monde extérieur. Ce positionnement stratégique permet de contenir les menaces dès leur apparition et presque sans efforts.

Kaspersky Web Traffic Security est une application qui s'intègre aux serveurs proxy pour protéger le réseau informatique de l'entreprise des dangers d'Internet et augmenter la productivité en régulant son utilisation. Elle traite le trafic Web et bloque tout ce qui est dangereux, conformément aux politiques de sécurité de l'entreprise. Malgré son approche standard en matière de sécurité périmétrique, l'étendue des fonctionnalités et la qualité inégalée de la protection contre les menaces permettent à Kaspersky Web Traffic Security de se démarquer des autres offres sur le marché.

Points forts

- Protection anti-phishing et contre les programmes malveillants de nouvelle génération en temps réel
- Filtrage de contenu pour bloquer les types de fichiers à risque et éviter les fuites de données
- Évolutif pour s'adapter aux réseaux à forte charge
- Disponible sous forme de licence mensuelle pour les utilisateurs finaux et les MSP
- Protection contre les menaces de type « zero-hour »
- Sécurisé par la Threat Intelligence mondiale de Kaspersky Security Network
- Compatible Microsoft Active Directory
- Accès basé sur les rôles à l'administration et à l'utilisation du Web
- Contrôle Web régissant l'utilisation des ressources Web
- Blocage des ransomwares avant leur entrée dans le réseau
- Location multiple pour les MSP et les entreprises diversifiées

Avantages

Réduction considérable du risque d'infection empêchant l'interruption des activités.

En bloquant la majorité des menaces entrantes au niveau de la passerelle et en les empêchant d'atteindre les terminaux, Kaspersky Web Traffic Security réduit considérablement leur impact potentiel sur les utilisateurs finaux et leur poste de travail.

Renforce l'efficacité de la protection des passerelles d'entreprise

Dotée des technologies de protection les plus puissantes du secteur avec un taux de détection supérieur et un taux de faux positifs proche de zéro, l'application Kaspersky Web Traffic Security est le compagnon idéal pour vos contre-mesures de passerelle Web existantes et améliore sensiblement la protection. Cette qualité est particulièrement importante pour les entreprises et les institutions gérant des données hautement sensibles et/ou avec une faible tolérance aux incidents de sécurité.

Réduit les frais généraux pour l'informatique et le personnel de sécurité informatique

Même si la protection des terminaux est adéquate, un nombre réduit d'alarmes les concernant signifie moins d'utilisateurs paniqués et moins de temps passé à enquêter sur les incidents.

Augmente la productivité

En régissant l'utilisation des ressources Internet, Kaspersky Web Traffic Security réduit non seulement le risque de cyberattaques, mais évite également les distractions, limitant l'impact de l'informatique parallèle, surtout lorsque des terminaux non Windows sont concernés.

Configuration matérielle requise pour les serveurs servant à l'installation de Kaspersky Web Traffic Security

Serveur esclave :

- Processeur : Intel Xeon E5606 (4 cœurs) 1,86 GHz ou plus ;
- 8 Go de RAM ;
- partition swap d'au moins 4 Go ;
- 100 Go d'espace sur le disque dur, y compris :
- 25 Go pour le stockage de fichiers temporaires ;
- 25 Go pour le stockage de fichiers journaux.

Serveur maître :

- Processeur : Intel Xeon E5606 (4 cœurs) 1,86 GHz ou plus ;
- 8 Go de RAM ;
- partition swap d'au moins 4 Go ;
- 100 Go d'espace sur le disque dur.

Si vous installez le serveur maître et un serveur esclave sur le même serveur physique :

- Processeur : 2 x Intel Xeon E5606 (8 cœurs) 1,86 GHz ou plus ;
- 16 Go de RAM ;
- partition swap d'au moins 4 Go ;
- 200 Go d'espace sur le disque dur, y compris :
- 25 Go pour le stockage de fichiers temporaires ;
- 25 Go pour le stockage de fichiers journaux.

Configuration logicielle requise pour les serveurs servant à l'installation de Kaspersky Web Traffic Security

- Red Hat Enterprise Linux version 7.5 x64.
- Ubuntu 18.04.1 LTS.
- Debian 9.5.
- SUSE Linux Enterprise Server 12 SP3.
- CentOS version 7.5 x64.

Configuration supplémentaire requise

- Ngnix versions 1.10.3, 1.12.2 et 1.14.0.
- Équilibrage de charge HAProxy version 1.5.
- Squid 3.5.20 si vous installez le service Squid sur le serveur esclave.

Pour que Kaspersky Web Traffic Security traite le trafic de votre réseau, vous devez installer et configurer un serveur proxy HTTP(S) intégrant le protocole ICAP, les services Request Modification (REQMOD) et Response Modification (RESPMOD). Vous pouvez utiliser un serveur proxy distinct ou, par exemple, installer le service Squid sur un serveur esclave de Kaspersky Web Traffic Security.

Configuration logicielle requise pour la gestion de Kaspersky Web Traffic Security via l'interface Web

Pour exécuter l'interface Web, un des navigateurs suivants doit être installé sur l'ordinateur :

- Mozilla Firefox version 39.
- Internet Explorer version 11.
- Google Chrome version 43.
- Microsoft Edge version 40.

S'adapte à la taille de votre entreprise

En fonction de la charge du système, la solution peut être évolutive, offrant gestion multi-nœuds et déploiement hiérarchique.

Réduit les risques associés à la transmission de certains types de fichiers, dans les deux sens

Kaspersky Web Traffic Security renforce la sécurité en limitant la transmission de certains types de fichiers. Cela permet d'éviter les infections dues à l'utilisation de contenu malveillant intégré dans les documents et réduit également le risque de fuite de données. Par ailleurs, en empêchant les utilisateurs d'accéder aux fichiers multimédia dont ils n'ont pas besoin pour travailler, vous augmentez leur productivité.

Avantages pour les fournisseurs de services gérés (MSP)

Comme les MSP ajoutent la cybersécurité à leur proposition de valeur, Kaspersky Web Traffic Security prend en charge les capacités de gestion multi-client et les licences flexibles et permet de déléguer le bon degré de contrôle aux administrateurs des clients.

Fonctionnalités

Protection multi-niveaux contre les menaces avec HuMachine™

La nouvelle génération de protection contre les programmes malveillants de Kaspersky Lab intègre de multiples couches de sécurité proactive, y compris celles basées sur des algorithmes de machine learning et assistées par de puissants mécanismes basés dans le cloud. Elle filtre les logiciels malveillants, les ransomwares et les programmes potentiellement indésirables dans le trafic entrant et sortant.

Threat Intelligence mondiale : Kaspersky Web Traffic Security exploite des données du monde entier pour obtenir le dernier aperçu 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 sur les menaces 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 et un minimum de 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 ne pénètre le système de l'entreprise.

Détection de script

Selon les analystes de la cybersécurité, les scripts sont de plus en plus utilisés à la fois pour les attaques sur le Web et pour l'intégration de logiciels malveillants dans des fichiers de bureau apparemment inoffensifs. Kaspersky Web Traffic Security sait traiter ces deux problèmes, en empêchant les attaques éclair et l'exécution de logiciels malveillants mortels avant même qu'ils n'atteignent le terminal demandé.

Base de données sur les hôtes liés aux cyberattaques

Pour éviter le moindre risque d'interaction avec des ressources dangereuses, ce service basé sur le cloud compare la ressource demandée à une vaste base de données de serveurs de commandement et de contrôle de cyberattaquants actifs, d'objets avec des exploits « zero-day », de sites Web toxiques et de points de distribution de programmes malveillants identifiés comme source de violation. Cette base de données est continuellement mise à jour en temps réel grâce aux informations de la célèbre équipe GReAT de Kaspersky Lab, pour bloquer les dernières ressources dangereuses émergentes avant même que la requête ne soit exécutée.

Filtrage basé sur la réputation

Kaspersky Web Traffic Security peut demander des réputations de fichiers et d'adresses à partir des bases de données dans le cloud constamment renouvelées de Kaspersky Security Network. Cela permet de bloquer instantanément les fichiers et les ressources Internet suspectes ou indésirables sans recourir à une analyse plus approfondie.

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.

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 hébergée dans le cloud est alimentée par les données mondiales portant sur les URL malveillantes ou de phishing. Elle fournit une protection contre les URL de phishing « zero-hour », connues ou non, contenues dans les fichiers téléchargés.

Filtrage des contenus

La transmission de certains types de fichiers peut être interdite. Le filtrage est basé sur différents paramètres, tels que le nom, l'extension/le type (la reconnaissance de format est utilisée pour les fichiers avec de fausses extensions), la taille, le type MIME et le hachage. Cela permet de remplir plusieurs objectifs, comme la réduction du risque de cyberattaque, la prévention des fuites de données, la réduction du trafic et l'amélioration de la productivité

Contrôle Web avec les catégories Kaspersky Lab

Les ressources Web ne sont pas toutes nécessaires aux activités professionnelles des salariés et bon nombre d'entre elles peuvent représenter un danger considérable pour la sécurité et la réputation de l'entreprise si elles hébergent des programmes malveillants ou proposent des produits piratés. Le contrôle Web restreint certaines catégories de ressources Web afin de réduire les risques et d'assurer un travail ininterrompu sans distractions indésirables. Si nécessaire, un scénario de blocage par défaut peut être implémenté, limitant l'utilisation de toutes les ressources Web à l'exception de celles absolument nécessaires au travail d'un utilisateur ou d'un groupe particulier.

Surveillance du trafic chiffré SSL sécurisée

L'architecture de la solution permet une mise en œuvre facile de la surveillance du trafic d'entreprise (« man-in-the-middle » ou « homme du milieu de l'entreprise »). Le trafic Web chiffré SSL devenant de facto la norme pour les communications Internet, il s'agit d'une fonctionnalité indispensable.

Sécurité des systèmes équipés de la technologie ICAP

En plus des serveurs proxy, la solution de Kaspersky Lab peut sécuriser le trafic sur tout autre appareil compatible avec le protocole ICAP. Il peut s'agir, par exemple, de NAS ou d'autres systèmes qui ne peuvent être protégés par une solution de sécurité interne.

Intégration SIEM

Si votre entreprise utilise un système de gestion des événements et des informations de sécurité (SIEM) pour assurer le suivi des activités sur le réseau d'entreprise, Kaspersky Web Traffic Security enrichira votre environnement sécurité en exportant les informations au format Common Event Format (CEF) et syslog (format largement utilisé).

Gestion pratique

Kaspersky Web Traffic Security offre un système de gestion flexible et facile à utiliser.

Console centralisée : contrôlez la sécurité de tous vos systèmes compatibles ICAP, y compris les proxys et les périphériques de stockage, grâce à une interface Web centralisée offrant à vos responsables de la sécurité une excellente visibilité et une facilité de gestion incomparable.

Tableau de bord pratique : tout ce qui est nécessaire pour évaluer l'état actuel de la sécurité de l'entreprise au niveau des passerelles est centralisé dans un seul tableau de bord. Vous obtenez ainsi une vue d'ensemble instantanée et complète de la situation, événements urgents inclus.

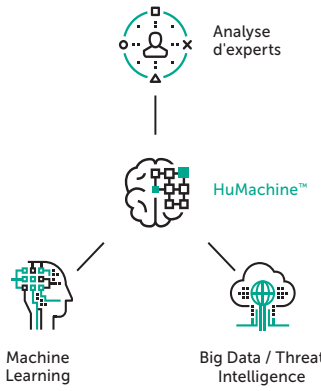
Gestion des événements : Les résultats d'analyse des menaces sont présentés à l'aide d'une approche centrée sur l'événement et affichent l'activité en temps réel. Le comportement des utilisateurs sur Internet peut également être analysé.

Système flexible de configuration de règles : En plus de la puissance des couches de sécurité de la solution, des politiques de sécurité précises et configurées de manière cohérente avec les processus opérationnels existants sont essentielles à l'efficacité de la solution. Kaspersky Web Traffic Security propose un système de configuration de règles flexible, simple à utiliser et à apprendre, pour une gestion granulaire de la sécurité de votre passerelle.

Système d'accès basé sur les rôles : Les administrateurs peuvent définir un rôle pour restreindre les droits d'administration en fonction des catégories d'administrateurs. C'est utile pour la délégation interne des tâches ou pour fournir le degré de contrôle nécessaire aux clients desservis dans le cas d'un MSP.

Intégration d'Active Directory : Kaspersky Web Traffic Security peut obtenir des informations sur les entités du domaine de l'entreprise (utilisateurs, groupes d'utilisateurs, ordinateurs, etc.) pour configurer ses règles d'accès basées sur les rôles et ses politiques de sécurité autour d'objets connus opérant dans le réseau informatique d'entreprise. Les données décrivant les objets sont constamment synchronisées entre l'Active Directory et l'application elle-même pour maintenir la cohérence avec les derniers changements dans l'infrastructure de l'entreprise.

Solution multi-clients : Un mode spécial pour les MSP et les entreprises diversifiées vous permet d'attribuer des espaces dédiés (« espaces de travail ») à différentes unités ou entreprises gérées et de les piloter séparément, tout en combinant les politiques « globales » et « locales » le cas échéant.



Comment acheter
Kaspersky Web Traffic Security est une application activée dans plusieurs produits Kaspersky Lab différents, en fonction de la licence que vous avez achetée.
- Kaspersky Security for Internet Gateways
- Kaspersky Security for Storages
- Kaspersky Security for xSP
- Kaspersky Total Security for Business

www.kaspersky.fr

© 2018 AO Kaspersky Lab. Tous droits réservés. Les marques déposées et marques de service sont la propriété de leurs détenteurs respectifs.