Kaspersky® Endpoint Security for Linux

Protection fiable pour les stations de travail et les serveurs Linux

Souvent choisi pour les serveurs hautes performances et les postes de travail économiques, le système d'exploitation Linux gagne du terrain dans les entreprises. Son adoption croissante entraîne un besoin de protection adaptée. Il est utilisé avec une gamme de plus en plus développée de systèmes d'entreprise critiques et il est désormais crucial de sécuriser les terminaux et les serveurs Linux contre des menaces qui évoluent rapidement.

Kaspersky Endpoint Security for Linux fournit une protection de nouvelle génération contre tout type de cybermenaces, sur une gamme complète de plateformes Linux. L'application offre une protection multi-niveaux ayant un impact minime sur les autres applications ou sur la performance globale du système. Elle est disponible dans notre gamme complète de produits, y compris dans Kaspersky Endpoint Security for Business.

Un leader reconnu

En 2017, les produits de sécurité de Kaspersky Lab ont fait l'objet de 86 tests et études indépendants. Ils ont terminé 72 fois en première position et 78 fois parmi les trois premiers. Nos technologies de sécurité les plus testées et les plus primées au monde atteignent des taux de détection supérieurs à ceux des autres principaux éditeurs.

Approche Kaspersky HuMachine™

Des fonctionnalités de Machine Learning, une Threat Intelligence au niveau mondial à partir du big data et deux décennies d'expertise humaine convergent pour offrir une protection optimale d'une efficacité inégalée.

Kaspersky Security Network

Kaspersky Security Network (KSN) est une infrastructure distribuée complexe, qui offre une réponse plus rapide que jamais aux nouvelles menaces, améliorant ainsi les dispositifs de protection et réduisant le risque de faux positifs.

Intégrée dans un produit unique : pas de coûts cachés

La protection pour les appareils Linux n'est qu'une application parmi d'autres qui sont intégrées à Kaspersky Endpoint Security for Business et à d'autres produits. Il n'y a aucun coût caché : un produit implique une licence, avec tout ce dont vous avez besoin pour protéger votre parc informatique.

Points forts

Solution de protection de nouvelle génération

Nos technologies de sécurité proactives permettent de réduire considérablement les menaces éventuelles sur vos terminaux et d'aider à identifier et à bloquer les menaces visant votre environnement Linux. En plus de détecter et de bloquer les menaces qui ciblent les ordinateurs Linux, elles surveillent également les menaces pour Windows et Mac pouvant se trouver sur l'un de vos ordinateurs Mac.

Haut niveau de performances et très simple d'utilisation

L'application est spécifiquement conçue pour avoir un impact minime sur les autres programmes et sur les performances globales du système. L'interface utilisateur graphique (GUI) est conçue pour les grands environnements de bureau. Cette conception, combinée à l'amélioration des capacités de gestion des lignes de commande, simplifie l'exécution des tâches et les rapports quotidiens.

Console de gestion unique

Toutes les fonctions de sécurité sont contrôlées simplement via une console d'administration unique, le Kaspersky Security Center, qui centralise également la gestion de nombreuses autres applications de sécurité de Kaspersky Lab.

Fonctionnalités

Protection multi-niveaux

Protection contre les menaces « zero-day »

La fonction de Threat intelligence basée dans le Cloud de Kaspersky Security Network permet une détection rapide en temps quasi réel et une réponse aux menaces ciblées sur Linux et autres systèmes d'exploitation, avec un minimum de faux positifs et une perturbation du flux de travail réduite.

Protection contre les ransomwares

Cette fonction contient un mécanisme contre le chiffrement capable de bloquer le chiffrement de fichiers de ressources partagées par un processus malveillant exécuté sur une autre machine du même réseau.

Détection de programme malveillant « sans corps »

L'analyse des secteurs d'amorçage des disques, ainsi que de la mémoire des processus lancés, aide à repérer les menaces sophistiquées, telles que les programmes malveillants « sans corps » ou tout en mémoire vive.

Surveillance de l'intégrité des fichiers

Cette fonction peut garantir l'intégrité des fichiers système, des journaux et des applications critiques grâce au suivi des modifications non autorisées dans les fichiers et répertoires importants.

Protection en temps réel et analyses à la demande

Cette fonction surveille tous les fichiers lancés ou ouverts et désinfecte les fichiers infectés. Elle analyse les zones spécifiées du système, conformément à un calendrier ou à la demande, et prend en charge l'analyse de fichiers pour les utilisateurs sans privilèges.

Performances optimisées

Équilibrage de la charge

Les technologies d'équilibrage de la charge et d'analyse optimisée, dotées d'une option permettant d'exclure les processus de confiance, améliorent les performances générales tout en réduisant la consommation de ressources.

Prise en charge de Fanotify

Cette fonction prend en charge Fanotify et permet d'exécuter une analyse en temps réel sur des noyaux, sans avoir besoin de compiler des modules supplémentaires.

Économies de ressources

Cette fonction ajuste automatiquement l'utilisation des ressources système et réalise des contrôles automatiques permettant de réduire la charge du serveur tout en maintenant des niveaux de protection optimaux.

Gestion de la sécurité améliorée

Gestion du pare-feu

Cette fonction vous permet de configurer et de gérer les paramètres de pare-feu intégrés du système d'exploitation Linux : l'application permet la création de règles de pare-feu, de journaux d'activité réseau et d'examens des incidents de sécurité, de manière centralisée.

Interface utilisateur améliorée

L'interface utilisateur graphique (GUI) est optimisée pour les systèmes Linux. Cette conception, combinée à l'amélioration des capacités de gestion des lignes de commande, simplifie l'exécution des tâches et les rapports quotidiens.

Fonctionnement ininterrompu

Après une mise à jour du système d'exploitation sur un poste de travail ou sur un serveur, il n'est plus nécessaire de réinstaller ou d'effectuer une toute nouvelle installation : la protection est automatiquement rétablie, sans intervention d'un administrateur.

Configuration

Pour connaître la configuration requise la plus complète et à jour, veuillez consulter la https://support.kaspersky.com/fr.

Configuration générale

- Processeur Intel Core 2 Duo 1,86 GHz ou plus rapide
- RAM : 1 Go pour un système d'exploitation 32 bits (2 Go pour un système d'exploitation 64 bits)
- 1 Go d'espace disque disponible

Systèmes d'exploitation

- CentOS-6.9 x86/x64
- Debian GNU/Linux 8.9 x86/x64 ou version supérieure
- Red Hat® Enterprise Linux® 7.4 x64 ou version supérieure
- Serveur Ubuntu 16.04 LTS x64 ou supérieur
- openSUSE® 42.3 ou version supérieure

Configuration requise pour l'abonnement

Veuillez vérifier auprès de votre partenaire local la disponibilité de la souscription dans votre pays et consultez la configuration requise pertinente https://support.kaspersky.com/fr/subscription.aspx.

Comment acheter

Kaspersky Endpoint Security for Linux est inclus dans les produits suivants :

- https://www.kaspersky.fr/small-to-medium-business-security/total
- https://www.kaspersky.fr/small-to-medium-business-security/endpoint-advanced
- https://www.kaspersky.fr/small-to-medium-business-security/endpoint-select

Ces produits peuvent également être achetés avec une souscription mensuelle flexible.

Vous pouvez également les acheter en tant que solutions à la carte https://www.kaspersky.fr/small-to-medium-business-security/file-server et https://www.kaspersky.fr/small-to-medium-business-security/virtualization-hybrid-cloud.

Rechercher un partenaire près de chez vous :
https://kas.pr/kasperskypartnersfr
#truecybersecurity
#HuMachine

www.kaspersky.fr