Kaspersky® Endpoint Security Cloud

Protection puissante, simple à administrer

Toutes les entreprises sont vulnérables aux mêmes cybermenaces, mais certaines sont mieux préparées que d'autres.

Les cybercriminels savent que les entreprises et les multinationales investissent massivement dans des solutions de sécurité informatique. C'est la raison pour laquelle ils lancent des attaques de plus en plus nombreuses contre les TPE/PME qu'ils considèrent désormais comme des cibles faciles.

Kaspersky Endpoint Security Cloud : La sécurité Plug & Play

Une seule attaque ciblant une entreprise qui ne s'est pas préparée à affronter de tels risques peut entraîner :

- la perte de données sensibles, y compris de propriété intellectuelle ;
- la fuite d'informations confidentielles relatives aux clients et aux collaborateurs ;
- un impact négatif sur la productivité des collaborateurs qui se répercute directement sur la rentabilité.

Contrairement aux grandes sociétés, les TPE/PME ne disposent généralement pas d'équipes informatiques internes importantes. Elles ont besoin d'une solution de sécurité facile à installer et à mettre en œuvre, voire d'externaliser sa gestion à distance.

La solution **Kaspersky Endpoint Security Cloud** couvre les besoins spécifiques de ces entreprises en les aidant à protéger l'ensemble de leurs terminaux Windows et Mac, de leurs serveurs de fichiers Windows et de leurs appareils mobiles Android et iOS. La protection leader du marché qu'elle offre est rapide à déployer, à mettre en œuvre et à exécuter sans qu'il soit nécessaire d'acheter du matériel supplémentaire. En outre, tous les paramètres de sécurité peuvent être gérés à distance, depuis tout appareil doté d'une connexion Internet.

La solution de sécurité la plus testée et la plus primée

Ces trois dernières années, nos technologies de sécurité ont participé au plus grand nombre de tests et obtenu les prix les plus prestigieux. Lors d'une série complète de tests indépendants, nos produits ont constamment remporté bien plus de prix et figuré bien plus souvent dans le top 3 des meilleures notes que ceux de tout autre éditeur (pour obtenir des informations détaillées, veuillez consulter https://www.kaspersky.fr/top3).

Une gestion centralisée pour simplifier la sécurité

Toutes les fonctionnalités de sécurité sur l'ensemble des ordinateurs de bureau et ordinateurs portables Windows ou Mac, des serveurs de fichiers Windows, sans oublier des appareils mobiles Android et iOS, peuvent être configurées et gérées via une console d'administration centralisée. Vous n'avez pas besoin de compétences particulières en matière de sécurité informatique pour utiliser la console et gérer votre sécurité. Par ailleurs, les politiques de sécurité que vous appliquez sur tous vos terminaux sont faciles à définir.

Console basée dans le Cloud pour une administration simple et flexible

La console basée dans le Cloud et prête à l'emploi permet aux administrateurs d'utiliser quasiment n'importe quel appareil doté d'une connexion à Internet pour configurer et régler l'ensemble des fonctionnalités de protection, pour tous les terminaux. Si vous choisissez d'externaliser la gestion de votre sécurité informatique, la console permettra également à vos consultants externes de la gérer à distance, en toute simplicité. Étant basée dans le Cloud, vous n'aurez pas besoin d'investir dans du matériel supplémentaire ou d'en assurer la maintenance et bénéficierez d'une configuration initiale extrêmement rapide.

Fonctionnalités

Protection pour tous vos appareils

Des technologies de sécurité primées assurent la protection des ordinateurs Windows et Mac, et serveurs de fichiers Windows contre les menaces informatiques connues et inconnues, y compris les attaques de type ransomware. Plusieurs niveaux de sécurité sont proposés : protection traditionnelle, proactive et basée dans le Cloud contre les programmes malveillants pour les fichiers, les e-mails et le Web, et technologies de pare-feu, de blocage des attaques réseau (Network Attack Blocker) et System Watcher puissantes. La solution intègre des politiques de sécurité par défaut, développées par nos experts en sécurité, afin que tous vos appareils puissent bénéficier d'une protection immédiate.

Contrôle de l'accès aux périphériques et à Internet

Les outils de contrôle des périphériques facilitent la gestion des appareils autorisés à accéder à votre réseau informatique d'entreprise. Les outils de contrôle du Web vous permettent de définir vos politiques d'accès à Internet et de surveiller l'utilisation d'Internet. Le contrôle des privilèges des applications restreint les activités du terminal, en fonction du « niveau de confiance » qui a été attribué à l'application.

Simplification de la gestion des appareils mobiles

Notre fonctionnalité de gestion des appareils mobiles (MDM) permet de connecter des smartphones et des tablettes à votre réseau d'entreprise, de configurer le réseau Wi-Fi et Bluetooth, de contrôler la complexité des mots de passe, de gérer l'utilisation de l'appareil photo et de régler d'autres paramètres à l'aide de fonctions à distance. Le serveur MDM iOS est automatiquement déployé dans le Cloud, vous n'aurez donc pas besoin d'investir dans du matériel supplémentaire pour gérer vos appareils iOS.

Protection contre les menaces mobiles

Les technologies de sécurité mobile avancées protègent vos appareils Android et iOS contre les menaces les plus récentes, notamment le nombre croissant de cryptomalwares et autres attaques. Le système anti-phishing assure la protection contre les sites Web qui tentent de dérober des informations confidentielles ou d'identité. Les tentatives d'obtention d'un accès racine ou de déverrouillage sont détectées automatiquement pour que les appareils à risque puissent être immédiatement bloqués. Le filtrage des appels et des SMS pour appareils Android permet de bloquer les appels ou SMS indésirables.

Solution prête à l'emploi et facile à déployer

Toutes les fonctions sont gérées dans le Cloud, il n'est donc pas nécessaire de télécharger une console de gestion sur vos serveurs. Il vous suffit d'accéder à la console basée dans le Cloud sur cloud.kaspersky.com et de déployer le logiciel de sécurité sur vos PC, serveurs de fichiers et appareils mobiles.

Protection des données sensibles, même sur des appareils perdus

En cas de perte ou de vol d'un appareil, des fonctions de sécurité gérées à distance permettent de protéger vos données d'entreprise. Les administrateurs peuvent verrouiller l'appareil perdu ou volé et supprimer toutes les données ou uniquement celles de l'entreprise.

Essai gratuit pour vos ordinateurs de bureau, ordinateurs portables, serveurs de fichiers et appareils mobiles
Rendez-vous sur cloud.kaspersky.com pour bénéficier d'une version d'évaluation **gratuite** de 30 jours de Kaspersky Endpoint Security Cloud. Si, à l'issue de cette période, vous choisissez d'acheter la solution, il vous suffira de payer les frais de licence. Vous n'aurez pas à définir de paramètres de configuration puisque vous aurez déjà utilisé la solution Kaspersky Endpoint Security Cloud sur vos terminaux.

Plates-formes prises en charge

Systèmes d'exploitation Windows et Mac

Serveurs de fichiers Windows

Appareils Android et iOS

Kaspersky Lab
Kaspersky for Business : **www.kaspersky.com/fr/business-security**
Actualités sur les cybermenaces : **www.viruslist.fr**
Actualités sur la sécurité informatique : **business.kaspersky.com**

#truecybersecurity
#HuMachine

www.kaspersky.fr