Kaspersky® Endpoint Security for Business

Select

Kaspersky Endpoint Security for Business Select fournit une protection de nouvelle génération basée sur HuMachine™ pour une large gamme de plateformes, y compris les terminaux et serveurs Linux. Cette solution offre une sécurité multi-niveaux qui détecte les comportements suspects et bloque les menaces, y compris les ransomwares. Les contrôles dans le Cloud réduisent votre exposition aux attaques et des fonctionnalités de gestion mobile vous permettent de protéger les plateformes mobiles.

Les fonctionnalités de protection et d'administration qu'il vous faut

Kaspersky Lab a conçu de puissantes fonctionnalités. Nous avons veillé à ce que ces technologies soient faciles et simples à utiliser pour les entreprises de toutes tailles.

Quelle est la version la mieux adaptée à vos besoins ?

- **SELECT**
- ADVANCED
- TOTAL

Plusieurs niveaux de protection pour

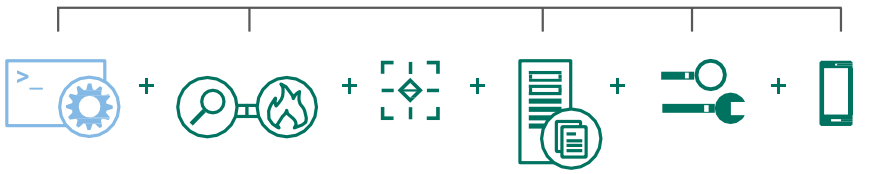
- Windows, Linux et Mac
- Serveurs Windows et Linux
- Android et autres appareils mobiles
- Stockage amovible

Sécurité inégalée contre

- Vulnérabilités logicielles
- Ransomwares
- Code malveillant sur les appareils mobiles
- Les menaces avancées
- Menaces sans fichiers
- Attaques basées sur un script et PowerShell
- Cybermenaces

Fonctionnalités incluses

- Protection contre les programmes malveillants amélioré
- Machine Learning statique
- Machine Learning dynamique nouveauté
- Isolation de processus
- Pare-feu
- Gestion du pare-feu du système d'exploitation nouveauté
- Protection basée dans le Cloud
- Agent EDR intégré nouveauté
- Contrôle des applications amélioré
- Liste blanche dynamique
- Contrôle Web
- Contrôle des appareils amélioré
- Protection des serveurs améliorée
- Protection pour Terminal servers améliorée
- Gestion de la mobilité dans l'entreprise améliorée
- Protection des terminaux mobiles améliorée
- Création de rapports améliorée



Protection et contrôle de nouvelle génération pour tous les terminaux

Une unique console d'administration

La console d'administration permet aux administrateurs d'afficher et de gérer l'ensemble de l'environnement de sécurité et d'appliquer les stratégies de sécurité choisies à chaque terminal de votre entreprise. Cette configuration vous aide à déployer une sécurité rapidement et avec un minimum d'interruptions, en utilisant n'importe quels scénarios préconfigurés de notre large gamme.

Sécurité agile

Ce produit est compatible avec n'importe quel environnement informatique. Il emploie de nombreuses technologies de nouvelle génération éprouvée. Les capteurs intégrés et l'intégration à Endpoint Detection and Response (EDR) permettent de capturer et d'analyser des volumes importants de données pour assurer la détection des cyberattaques les plus obscures et sophistiquées.

Un produit unique : pas de coûts cachés

Étant donné que de multiples technologies de sécurité sont réunies dans un seul produit, il n'y a pas de coûts cachés. Un produit implique une licence ainsi que tout ce dont vous avez besoin pour protéger vos terminaux.

Principales fonctionnalités

Des fonctionnalités d'avenir

Protection contre les exploits
Empêche les logiciels malveillants d'exécuter et d'exploiter les logiciels, en offrant un niveau de protection supplémentaire contre les menaces « zero-day » inconnues.

Détection comportementale et annulation automatique
Assure l'identification et la protection contre les menaces les plus sophistiquées, notamment les ransomwares, les attaques sans fichier et la prise de contrôle de comptes administrateur. La détection comportementale bloque les attaques, tandis que le retour automatique à l'état antérieur (Automatic Rollback) annule toutes les modifications déjà apportées.

Protection contre le chiffrement des dossiers partagés
Un mécanisme unique 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.

Protection contre les menaces réseau
Un programme malveillant utilisant une attaque par dépassement de la mémoire tampon peut modifier un processus en cours d'exécution dans la mémoire et exécuter ainsi son code. La protection contre les menaces réseau identifie les attaques réseau et stoppe leur progression.

Technologie anti-rootkit
Les pirates utilisent des rootkits et des bootkits pour que les solutions de sécurité ne puissent pas détecter leurs activités. La technologie anti-rootkit aide à déceler les infections même les plus profondément cachées et à les neutraliser.

Fonctionnalités de sécurité mobile

Technologies innovantes de lutte contre les programmes malveillants
Technologies basées sur des signatures, proactives et assistées par le cloud pour une protection en temps réel. Un navigateur sûr et des analyses programmées et sur demande pour assurer la sécurité.

Déploiement de la technologie « Over The Air » (OTA)
Cette fonction permet de préconfigurer et de déployer des applications de manière centralisée à l'aide de SMS, d'e-mails et de la synchronisation PC.

Outils antivol à distance
Les outils SIM-Watch, Remote Lock, Wipe and Find empêchent tout accès non autorisé aux données de l'entreprise en cas de perte ou de vol d'un périphérique mobile.

Contrôle des applications pour appareils mobiles
Le contrôle des applications fournit des données sur les logiciels installés et permet aux administrateurs d'imposer l'installation et l'utilisation d'applications spécifiques.

Contrôle des terminaux dans le Cloud

Contrôle des applications
Réduisez votre exposition aux attaques avec le contrôle des applications, qui offre une maîtrise totale de l'exécution des logiciels sur les ordinateurs et repose sur la création dynamique de listes blanches dans notre laboratoire interne. Les scénarios de blocage par défaut et d'autorisation par défaut sont pris en charge.

Liste blanche dynamique
Pour une meilleure catégorisation des applications, le contrôle des applications peut utiliser la base de données de la liste blanche dynamique développée par Kaspersky Lab grâce à la systématisation des connaissances des logiciels légitimes.

Contrôle des périphériques
Cette fonction permet aux utilisateurs de définir, programmer et appliquer des procédures sur l'accès aux données avec un contrôle des supports de stockage amovibles ainsi que d'autres périphériques (connexion USB ou tout autre type de port).

Prévention des intrusions de l'hôte
Cette fonction régule l'accès aux données sensibles et aux appareils d'enregistrement en utilisant la base de données de réputation locale et dans le Cloud (Kaspersky Security Network), sans nuire aux performances des applications autorisées.

Maintenance et assistance

Opérant dans plus de 200 pays et 35 bureaux dans le monde entier, nos équipes en charge des services professionnels sont prêtes à intervenir à tout moment pour que vous puissiez profiter au maximum des avantages de votre installation de sécurité Kaspersky Lab.

Essai gratuit

Découvrez pourquoi seule True Cybersecurity, associe flexibilité et facilité d'utilisation à et est en mesure de protéger votre entreprise contre tous les types de menaces. Rendez-vous sur cette page pour bénéficier d'une version d'évaluation gratuite de 30 jours de **Kaspersky Endpoint Security for Business**.

Solutions de sécurité Kaspersky Lab
Trouver un partenaire près de chez vous :
https://kas.pr/kasperskypartnersfr
Kaspersky for Business :
https://www.kaspersky.fr/small-to-medium-business-security
Actualités de la sécurité informatique : business.kaspersky.com
Notre approche unique : www.kaspersky.com/true-cybersecurity

#truecybersecurity
#HuMachine

www.kaspersky.fr