KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Advanced

Kaspersky Lab propose un ensemble d'outils de sécurité intégrant des fonctionnalités d'optimisation informatique.

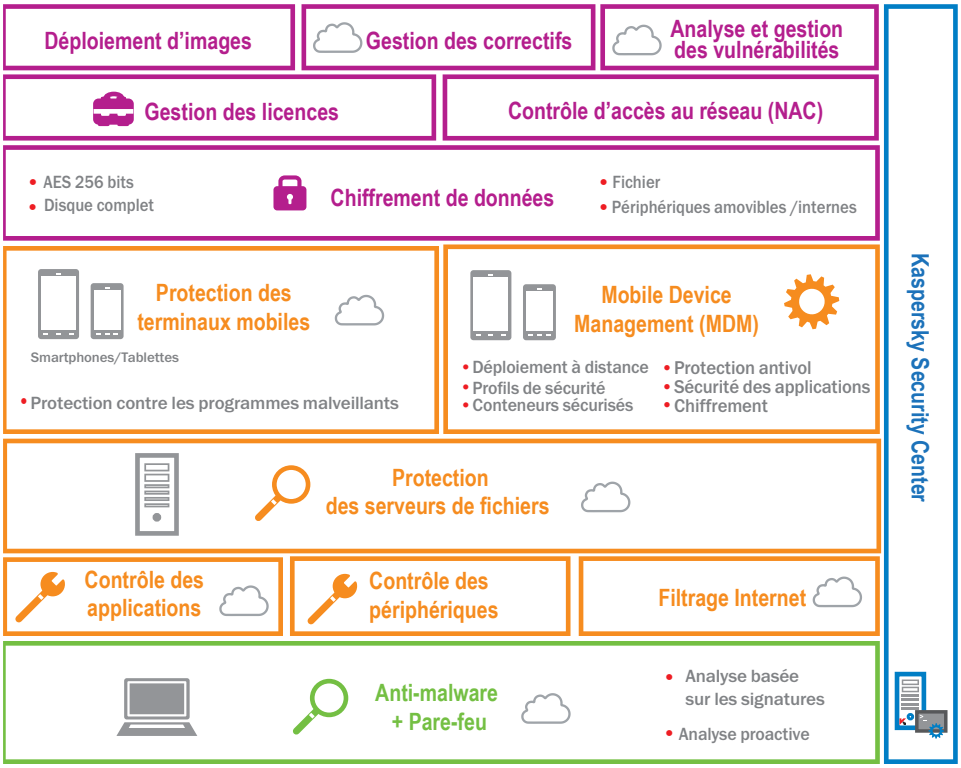
La version Advanced de Kaspersky Endpoint Security for Business permet à votre entreprise de déployer et d'administrer ses procédures informatiques, de protéger ses utilisateurs des programmes malveillants et d'éviter la perte de données tout en optimisant les performances de l'environnement informatique.

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

Kaspersky intègre dans ses solutions pour les entreprises des fonctionnalités avancées et évolutives, simplifiées au maximum pour s'adapter à toutes les typologies d'entreprises.

Quelle version répond le mieux à vos besoins ?

- CORE
- SELECT
- **ADVANCED**
- TOTAL



FONCTIONNALITÉS INCLUSES :

- PROTECTION CONTRE LES PROGRAMMES MALVEILLANTS
- PARE-FEU
- PROTECTION BASÉE SUR LE CLOUD VIA KASPERSKY SECURITY NETWORK
- CONTRÔLE DES APPLICATIONS
- LISTE BLANCHE D'APPLICATIONS
- FILTRAGE DE CONTENU WEB
- CONTRÔLE DES PÉRIPHÉRIQUES
- PROTECTION DES SERVEURS DE FICHIERS
- GESTION DE FLOTTE MOBILE (MDM)
- PROTECTION DES TERMINAUX MOBILES (POUR TABLETTES ET SMARTPHONES)
- CHIFFREMENT
- CONFIGURATION ET DÉPLOIEMENT DES SYSTÈMES
- CONTRÔLE D'ACCÈS AU RÉSEAU
- ANALYSE AVANCÉE DES VULNÉRABILITÉS
- GESTION DES CORRECTIFS (PATCH MANAGEMENT)

LA SEULE PLATE-FORME DE SÉCURITÉ VÉRITABLEMENT INTÉGRÉE

1 CONSOLE UNIQUE

Les produits Kaspersky sont conçus de manière à ce que l'administrateur puisse visualiser et gérer de manière centralisée l'ensemble des périphériques nécessitant une protection : machines virtuelles, périphériques physiques et mobiles.

1 PLATE-FORME UNIQUE

Kaspersky Lab est le seul éditeur de sécurité à avoir fait le choix de développer sa console, ses modules de sécurité et ses outils en interne plutôt que d'en faire l'acquisition auprès de sociétés tierces. Les mêmes programmeurs ont développé, à partir du même code source, des technologies qui communiquent et travaillent ensemble pour vous faire bénéficier, au final, d'une stabilité accrue, de politiques intégrées, d'une interaction totale entre les fonctions ainsi que des outils de rapport intégrés et intuitifs.

1 COÛT UNIQUE

Nous proposons tous les outils Kaspersky sous la forme d'un seul "paquet" d'installation, dans lequel le client choisit les briques qui l'intéressent.
Chaque version comporte ainsi un ensemble de fonctionnalités que vous activez au moment où vous en avez besoin.

CHIFFREMENT ET PROTECTION DES DONNÉES :

CHIFFREMENT DES DONNÉES
Possibilité de choisir un chiffrement complet du disque dur ou par fichier, en s'appuyant sur la norme de chiffrement AES (Advanced Encryption Standard) 256 bits pour sécuriser les données stratégiques de l'entreprise en cas de vol ou de perte des périphériques.

PARTAGE SÉCURISÉ DES DONNÉES
Possibilité de créer facilement des paquets de données chiffrées et auto-extractibles, pour protéger les données partagées via des périphériques amovibles, des e-mails, un réseau ou le Web.

SUPPORT DES PÉRIPHÉRIQUES AMOVIBLES
Sécurité optimisée par le biais de politiques qui imposent le chiffrement des données sur les périphériques amovibles.

TRANSPARENCE POUR LES UTILISATEURS FINAUX
La solution de chiffrement de Kaspersky est transparente pour les utilisateurs et n'a aucune incidence négative sur la productivité, aucun impact sur les paramètres, ni sur les mises à jour des applications.

OUTILS DE CONTRÔLE :

CONTRÔLE DES APPLICATIONS
Les administrateurs peuvent définir des politiques visant à autoriser, bloquer ou réglementer l'usage des applications (ou de catégories d'applications).

CONTRÔLE DES PÉRIPHÉRIQUES
Les administrateurs sont en mesure 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 (port USB ou tout autre type de connexion).

FILTRAGE DE CONTENU WEB
Les règles liées à l'usage d'Internet suivent l'utilisateur, qu'il soit sur le réseau d'entreprise ou en déplacement.

LISTE BLANCHE DYNAMIQUE
La réputation des fichiers en temps réel réalisée par le cloud Kaspersky Security Network et l'utilisation de la liste blanche permettent de s'assurer que les utilisateurs travaillent avec des applications approuvées et sans programmes malveillants.

FONCTIONNALITÉS DE LA PROTECTION DES TERMINAUX :

PROTECTION RENFORCÉE CONTRE LES PROGRAMMES MALVEILLANTS SUR LES TERMINAUX
Protection en temps réel combinant des technologies de détection par signatures, des analyses proactives, et une vérification de réputation basée sur le cloud pour détecter les programmes malveillants.

PROTECTION BASÉE SUR LE CLOUD
Kaspersky Security Network (KSN) permet une lutte contre les menaces potentielles bien plus rapide que les méthodes de protection traditionnelles. Le délai de réponse de KSN face à une menace ne dépasse pas 0,02 seconde !

LES FONCTIONNALITÉS NE SONT PAS TOUTES DISPONIBLES SUR L'ENSEMBLE DES PLATES-FORMES.
Pour en savoir plus, rendez-vous sur **www.kaspersky.com/fr**

GESTION DES CONFIGURATIONS SYSTÈME ET DES CORRECTIFS :

GESTION DES CORRECTIFS (PATCH MANAGEMENT)
Analyse avancée et approfondie des vulnérabilités associée à l'installation automatisée des correctifs.

DÉPLOIEMENT LOGICIEL À DISTANCE
Déploiement logiciel centralisé vers les machines client, y compris pour les sites distants.

CONTRÔLE D'ACCÈS AU RÉSEAU (NAC)
Grâce au contrôle d'accès au réseau, vous pouvez définir une politique d'accès aux données pour les visiteurs. Les périphériques des visiteurs (y compris les périphériques mobiles) sont automatiquement reconnus et dirigés vers un portail de l'entreprise, à partir duquel ils pourront, en saisissant des identifiants ad hoc, utiliser les ressources que vous avez approuvées.

DÉPLOIEMENT DES IMAGES DE SYSTÈMES D'EXPLOITATION ET DES APPLICATIONS
Simplicité de création, de stockage et de déploiement des images système depuis un point unique. Idéal pour une migration vers Microsoft Windows® 8.

GESTION DES MATÉRIELS, DES LOGICIELS ET DES LICENCES
Des rapports répertoriant les matériels et les logiciels permettent de contrôler les obligations liées aux licences. Vous réalisez ainsi des économies d'échelle en centralisant les droits relatifs aux logiciels.

FONCTIONNALITÉS DE L'OFFRE DE PROTECTION DES TERMINAUX MOBILES :

TECHNOLOGIES INNOVANTES DE LUTTE CONTRE LES PROGRAMMES MALVEILLANTS
Protection en temps réel combinant des technologies de détection par signatures, des analyses proactives et une vérification de réputation basée sur le cloud. Sécurité renforcée grâce à un navigateur sécurisé et un antispam.

TECHNOLOGIE « OVER THE AIR » (OTA)
Possibilité de préconfigurer et de déployer des applications de manière centralisée via l'envoi d'un sms ou d'un email contenant un lien vers le portail de l'entreprise, d'où les utilisateurs peuvent télécharger les applications approuvées par l'entreprise.

PROTECTION 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
Contrôle les applications installées sur un appareil mobile en se basant sur des politiques de groupe prédéfinies. Inclut un groupe d' « applications obligatoires ».

SUPPORT DES APPAREILS PERSONNELS DES EMPLOYÉS
Les données et les applications de l'entreprise sont isolées dans des conteneurs chiffrés transparents pour l'utilisateur. Ces données peuvent être supprimées de manière séparée.

KASPERSKY LAB FRANCE
IMMEUBLE L'EUROPÉEN, BÂT C
2 RUE JOSEPH MONIER
92859 RUEIL-MALMAISON CEDEX
FRANCE
commercial@kaspersky.fr
www.kaspersky.fr

KESB-ADV/Version 0.2/Nov12/Global