KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Select

Des outils pour répondre aux problématiques des équipes itinérantes, assurer le respect des politiques de sécurité informatique et bloquer les programmes malveillants.

La version « Select » de Kaspersky comprend le déploiement et la protection des terminaux mobiles en s'appuyant sur le module Mobile Device Management (gestion de flotte mobile) et sur une solution de lutte contre les programmes malveillants destinée à ces plates-formes. Les outils de contrôle (des applications, des périphériques et le filtrage de contenu web) permettent à votre entreprise de renforcer sa politique de sécurité informatique en protégeant les composants essentiels de votre infrastructure .

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

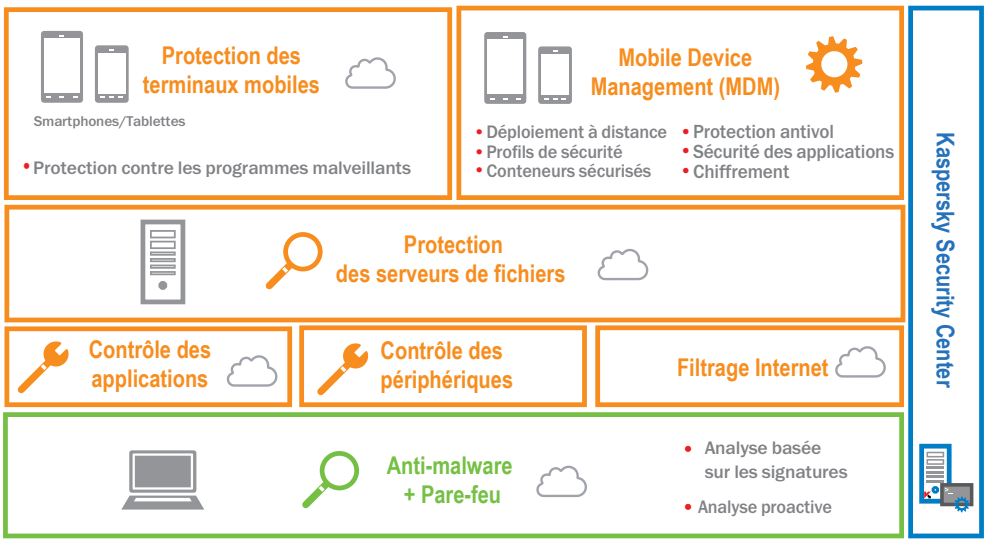
Kaspersky intègre dans ses solutions pour les entreprises des fonctionnalités avancées et évolutives, simplifiées au maximum pour s'adapter à toutes les typologies d'entreprises.

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)
- ADMINISTRATION CENTRALISÉE AVEC KASPERSKY SECURITY CENTER



FONCTIONNALITÉS PRINCIPALES :

PROTECTION AVANCÉE DES TERMINAUX CONTRE LES PROGRAMMES MALVEILLANTS
Le moteur d'analyse de Kaspersky fonctionne à différents niveaux du système d'exploitation pour identifier les programmes malveillants. Le cloud Kaspersky Security Network (KSN) protège les utilisateurs en temps réel contre les nouvelles menaces.

DES OUTILS DE CONTRÔLE FLEXIBLES ET MODULAIRES
Une base de données dans le cloud contient des catégories d'applications et de sites web considérés comme sains ou non. Elle permet à l'administrateur de définir et d'appliquer des politiques de contrôle des applications et de navigation sur le Web. En outre, des contrôles granulaires veillent à ce que seuls des périphériques spécifiques puissent être connectés aux machines sur le réseau.

PROTECTION ET GESTION DE FLOTTE MOBILE (SMARTPHONES ET TABLETTES)
La sécurité des appareils Android™, Blackberry®, Symbian et Windows® s'appuie sur un agent installé localement. Des politiques et des logiciels pour périphériques mobiles peuvent être déployés en toute sécurité et à distance sur ces appareils ainsi que sur des périphériques IOS grâce au module de gestion des périphériques mobiles (MDM) de Kaspersky.

ANALYSE DES VULNÉRABILITÉS
Identification des vulnérabilités pouvant affecter les matériels et les logiciels.

FONCTIONNALITÉS DE LA PROTECTION DES TERMINAUX :

MISES À JOUR RÉGULIÈRES ET PROTECTION À BASE DE SIGNATURES
Méthode traditionnelle avancée basée sur des signatures pour détecter les programmes malveillants.

ANALYSE DES COMPORTEMENTS SUSPECTS BASÉE SUR LE CLOUD KASPERSKY SECURITY NETWORK
Surveillance proactive permettant de détecter les menaces qui ne sont pas encore référencées dans les bases de signatures.
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 !

SYSTÈME DE PRÉVENTION DES INTRUSIONS HÉBERGÉ SUR L'HÔTE AVEC PARE-FEU INDIVIDUEL (HIPS)
Grâce à des règles prédéfinies pour des centaines d'applications les plus couramment utilisées, la configuration du pare-feu s'effectue plus rapidement.

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 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.

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.

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

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

KESB-S/Version 0.1/Nov12/Global

© 2012 Kaspersky Lab ZAO. Tous droits réservés. Les marques déposées et marques de service sont la propriété de leurs détenteurs respectifs. Windows est une marque déposée de Microsoft Corporation aux États-Unis et dans d'autres pays. Android est une marque commerciale de Google, Inc. La marque commerciale BlackBerry appartient à Research In Motion Limited ; elle est déposée aux États-Unis et peut être déposée ou en instance de dépôt dans d'autres pays.

KASPERSKY lab