

► KASPERSKY SECURITY FOR MOBILE

Une administration et une sécurité des terminaux mobiles renforcées, sans la complexité d'une solution séparée.

Le déploiement, l'administration et la sécurité de votre environnement informatique mobile doivent être simples et économiques. **Mobile Device Management (MDM)** facilite la configuration sécurisée des périphériques mobiles en y installant un **agent mobile** pour le protéger contre les menaces. Ceci est également possible sur les appareils personnels des employés !

Principales caractéristiques :

- SUPPORT DES TABLETTES ET DES SMARTPHONES
- TECHNOLOGIE « OVER THE AIR » (OTA)
- SÉCURITÉ BASÉE SUR UN AGENT
- GESTION DES APPAREILS MOBILES D'APPLE ET DE MICROSOFT EXCHANGE ACTIVESYNC EN TOUTE SÉCURITÉ
- INTÉGRATION NATIVE À KASPERSKY SECURITY CENTER POUR DÉFINIR LES PARAMÈTRES DE CONFIGURATION, DE CONTRÔLE, DE RAPPORT, D'INVENTAIRE ET DE POLITIQUE

Plates-formes mobiles supportées :

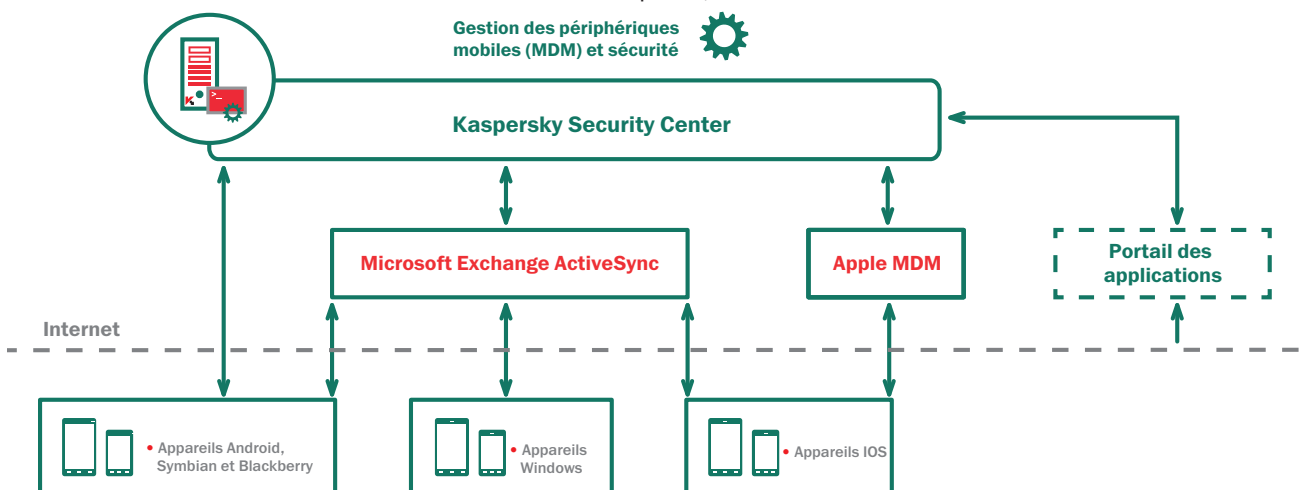
- IOS
- ANDROID™
- WINDOWS® PHONE
- WINDOWS MOBILE
- BLACKBERRY®
- SYMBIAN

► C'EST LA SOLUTION IDÉALE POUR S'ADAPTER AUX TENDANCES CONSISTANT À APPORTER SON PROPRE APPAREIL AU BUREAU (BYOD)

De nombreux employés utilisent leur propre appareil pour exécuter à la fois des tâches personnelles et professionnelles. En réalité, certaines entreprises encouragent leurs employés à acheter eux-mêmes leur smartphone ou leur tablette, avant de leur faire rajouter un logiciel de messagerie électronique ainsi qu'un accès d'entreprise par le service informatique.

Cette solution offre des avantages financiers et améliore la productivité de l'employé, mais elle peut également exposer l'entreprise à des problèmes de sécurité. Les données de l'entreprise, insuffisamment sécurisées et potentiellement mêlées à des données à caractère personnel, peuvent être aisément exploitées. Ces périphériques sont souvent utilisés par les membres de la famille, sans que ces derniers ne se préoccupent de la sécurité des applications. Certains sont mêmes accessibles par la racine ou déverrouillés.

Kaspersky Security for Mobile répond à cette problématique en permettant la configuration et le déploiement sécurisés des smartphones et des tablettes à partir de la même console que celle utilisée pour la sécurité de votre réseau. Les administrateurs informatiques sont ainsi assurés que les périphériques des utilisateurs sont configurés avec les paramètres appropriés et peuvent être sécurisés en cas de perte, de vol ou d'utilisation abusive.



► FONCTIONNALITÉS APPROFONDIES DE KASPERSKY SECURITY FOR MOBILE :

FONCTIONNALITÉS RELATIVES À L'EFFICACITÉ INFORMATIQUE :

SIMPLICITÉ DE LA CONFIGURATION VIA UNE CONSOLE UNIQUE

Contrairement aux autres solutions, Kaspersky Lab permet aux administrateurs d'utiliser une console unique pour gérer la sécurité des périphériques mobiles, des terminaux physiques, des systèmes virtuels ainsi que les outils de chiffrement et d'application des politiques.

PORTAIL DES APPLICATIONS DE L'ENTREPRISE

Les administrateurs mettent à disposition un portail d'entreprise comprenant des liens vers des applications approuvées. Les utilisateurs peuvent être contraints à utiliser ces applications uniquement.

TECHNOLOGIE « OVER THE AIR »

Sécurisation des téléphones à distance grâce à l'envoi d'un e-mail ou d'un SMS comprenant un lien vers le portail de l'entreprise à partir duquel les utilisateurs peuvent télécharger le profil et les applications que vous avez approuvés. L'accès aux données sera accordé après l'acceptation de l'utilisateur.

CONFIGURATION SÉCURISÉE

Intégrité des matériels et des logiciels garantie grâce à la détection des accès à la racine et des déverrouillages. Autres paramètres de sécurité : « désactivation de l'appareil photo », mot de passe obligatoire, etc.

APPLICATION DES RÈGLES ET POLITIQUES

Le contrôle des applications permet de surveiller et de contrôler l'utilisation des applications sur le périphérique notamment via les politiques « blocage par défaut » et « activation par défaut ».

CONTRÔLE DES RISQUES :

CHIFFREMENT

Les données en circulation sont protégées via un chiffrement transparent et intégral du disque et des fichiers qui peut également être appliqué à un conteneur.

PROTECTION ANTIVOL

Les administrateurs peuvent effectuer une suppression totale ou sélective des données du périphérique, localiser un appareil à l'aide de la fonctionnalité GPS de « Recherche » et recevoir une notification en cas de retrait ou de suppression d'une carte SIM.

PROTECTION DES APPAREILS MOBILES CONTRE LES PROGRAMMES MALVEILLANTS

Le moteur de protection contre les programmes malveillants de Kaspersky Lab intervient à plusieurs niveaux pour s'assurer que le périphérique n'est pas infecté. Il utilise notamment une protection basée sur le cloud, un navigateur sécurisé et un module antispam.

INTÉGRITÉ DES DONNÉES PROFESSIONNELLES ET PERSONNELLES :

CONTENEURS

Il est possible de placer les données et les applications de l'entreprise dans des conteneurs isolés sur l'appareil personnel d'un employé. Les données professionnelles sont ainsi sécurisées de manière optimale sans toucher au contenu personnel.

OUTILS DE PROTECTION DES DONNÉES À DISTANCE

En cas de perte d'un appareil, le verrouillage à distance peut être activé. Les données de l'entreprise placées dans un conteneur sur le périphérique peuvent être sécurisées, chiffrées, administrées et supprimées à distance, indépendamment des données personnelles présentes.

Comment acheter

Kaspersky Security for Mobile est compris dans les versions suivantes de Kaspersky Security for Business :

- Endpoint Security, Select
Endpoint Security, Advanced
- Kaspersky Total Security for Business

Kaspersky Security for Mobile peut également être acheté séparément. Contactez votre revendeur pour en savoir plus sur le produit et la tarification.

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

KASPERSKY LAB B.V.
PAPENDORPSEWEG 79
3528 BJ UTRECHT
THE NETHERLANDS
sales@kaspersky.be

KESB-MOBILE/Version 0.3/Nov12/Mondial

© 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. Mac OS est une marque déposée d'Apple 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 