▶ KASPERSKY SECURITY FOR MOBILE

Sécurité, administration et contrôle multicouches pour tous les terminaux mobiles

Les appareils mobiles sont devenus des cibles de choix pour les cyber-criminels. De plus, le BYOD (Bring Your Own Device) contribue à la diversification des appareils utilisés, ce qui complique le travail d'administration et de contrôle des services informatiques.
Avec Kaspersky Security for Mobile, vos appareils sont en sécurité, où qu'ils se trouvent. Protégez-vous des programmes malveillants en évolution constante et gagnez rapidement et facilement en visibilité et en contrôle pour tous les smartphones et tablettes de votre environnement, depuis une plateforme centralisée garantissant un minimum de perturbations.

- Puissant anti-malware
- Anti-phishing et filtrage des SMS et des appels entrants
- Protection Web
- Contrôle des applications
- Détection des terminaux 'jailbreakés'
- Mise en conteneur d'applications
- Protection contre le vol
- Gestion des appareils mobiles
- Portail libre-service
- Administration centralisée
- Console Web
- Plates-formes prises en charge :
  - Android™
  - iOS
  - Windows Phone

POINTS FORTS

PROTECTION AVANCÉE CONTRE LES PROGRAMMES MALVEILLANTS POUR LA SÉCURITÉ DES APPAREILS MOBILES ET DES DONNÉES

Rien qu'en 2014, Kaspersky Lab a géré près de 1,4 million d'attaques malveillantes différentes sur appareils mobiles. Kaspersky Security for Mobile lutte contre les menaces connues et inconnues visant les données stockées sur les appareils mobiles en associant une protection contre les programmes malveillants à diverses technologies de protection multicouches.

GESTION DES APPAREILS MOBILES

L'intégration à l'ensemble des principales plateformes de gestion des appareils mobiles permet un déploiement et un contrôle à distance « Over the Air » (OTA) pour une plus grande simplicité d'utilisation et d'administration sous Android, iOS et Windows Phone.

GESTION DES APPLICATIONS MOBILES

Les fonctions de mise en conteneur et de suppression sélective permettent de séparer les données de l'entreprise et les données personnelles sur un même appareil, favorisant ainsi les initiatives en faveur du BYOD. Également doté de notre fonction de chiffrement et de notre protection contre les programmes malveillants, Kaspersky Security for Mobile ne se contente pas d'isoler un appareil et ses données, mais propose une solution proactive de protection pour mobiles.

ADMINISTRATION CENTRALISÉE

Gérez plusieurs plateformes et appareils depuis la même console que pour vos autres terminaux et gagnez en visibilité et en contrôle sans effort ou technologie d'administration supplémentaires.

FONCTIONS DE GESTION ET DE SÉCURITÉ POUR MOBILES

PUISSANT ANTI-MALWARE
Protection proactive dans le cloud, basée sur la reconnaissance de signatures (via Kaspersky Security Network, KSN), pour contrer les attaques malveillantes sur mobiles connues et inconnues. Des analyses programmées ou à la demande sont combinées à des mises à jour automatiques pour une protection supérieure.

ANTI-PHISHING ET FILTRAGE DE SMS/APPELS ENTRANTS
Des technologies puissantes anti-phishing avec création d'une liste blanche et liste noire personnelles protègent l'appareil et ses données des attaques de phishing et aident à filtrer les appels et les messages indésirables.

CONTRÔLE WEB/NAVIGATION SÉCURISÉE
Des technologies gérées par Kaspersky Security Network (KSN) travaillent en temps réel pour empêcher l'accès à des sites Web malveillants et non autorisés. La fonction Safe Browser fournit une analyse de réputation constamment actualisée afin de garantir une navigation sécurisée sur appareil mobile.

CONTRÔLE DES APPLICATIONS
Des contrôles intégrés à KSN permettent de limiter l'utilisation d'applications aux logiciels approuvés, interdisant l'accès aux logiciels « grisés » ou non autorisés. Vous pouvez faire en sorte que l'appareil ne fonctionne qu'après installation de certaines applications. Le contrôle d'inactivité des applications permet aux administrateurs de demander à l'utilisateur de se reconnecter si une application est inactive pendant un certain temps. Cela permet de protéger les données même si une application est ouverte lors de la perte ou du vol de l'appareil.

DÉTECTION DES ACCÈS RACINE/'JAILBREAK'
Si un utilisateur ou une application tente de rooter le terminal Android ou jailbreaker les matériels sous iOS, ils seront détectés et consignés. Vous pouvez ensuite bloquer l'accès aux conteneurs, procéder à une suppression sélective ou supprimer toutes les données de l'appareil.

MISE EN CONTENEUR
Séparez les données de l'entreprise et les données personnelles en « empaquetant » vos applications dans des conteneurs. Vous pouvez appliquer d'autres politiques en complément, par exemple une fonctionnalité de chiffrement, pour protéger vos données sensibles. La suppression sélective permet de supprimer les données stockées dans les conteneurs sur un appareil lorsqu'un employé quitte la société, sans avoir à toucher à ses données personnelles.

PROTECTION CONTRE LE VOL
En cas de perte ou de vol d'un appareil, vous pouvez activer à distance des fonctions antivol, notamment la suppression des données, le verrouillage et la localisation de l'appareil, la surveillance SIM, le mugshot* et l'alarme. Selon la situation, ces commandes antivol seront appliquées avec une grande souplesse. Par exemple, les commandes sont envoyées immédiatement grâce à l'intégration à Google Cloud Messaging (GCM), pour un temps de réaction optimal et une sécurité accrue, et l'administrateur n'a pas à intervenir puisque les commandes sont envoyées sur le portail libre-service.

GESTION DES APPAREILS MOBILES
La prise en charge de Microsoft Exchange ActiveSync, Apple MDM, Samsung KNOX 2.0 et tout matériel Android, permet d'appliquer un grand nombre de politiques sur une interface unifiée, quelle que soit la plate-forme. (Ex : appliquer un chiffrement et des mots de passe ou contrôler l'utilisation de l'appareil photo, restreindre les politiques à des individus ou des groupes, gérer les paramètres APN/VPN, etc.)

PORTAIL LIBRE-SERVICE
Déléguez les tâches courantes d'administration de sécurité à vos employés et autorisez l'auto-enregistrement des appareils approuvés. Lors de la procédure d'enregistrement d'un nouvel appareil, tous les certificats requis sont automatiquement mis à disposition sur le portail, sans que l'administrateur ait à intervenir. En cas de perte de l'appareil, l'employé peut activer toutes les commandes antivol disponibles depuis le portail.

ADMINISTRATION CENTRALISÉE
Administrez tous vos appareils mobiles depuis une seule et même console, qui vous permettra également de gérer la sécurité informatique de tous les autres terminaux.
La console Web permet aux administrateurs de contrôler et d'administrer les appareils à distance depuis n'importe quel ordinateur.

*cliché du voleur capturé à l'aide de l'appareil photo frontal du périphérique mobile

Comment vous procurer ce produit ?

Kaspersky Security for Mobile est inclus dans :

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

Kaspersky Security for Mobile peut également être acheté séparément en tant que solution ciblée.

Contactez votre revendeur pour en savoir plus sur le produit et les tarifs.

Kaspersky Security for Mobile/Février 2015/Monde

KASPERSKY lab