KASPERSKY SECURITY FOR MOBILE

KASPERSKY lab

KASPERSKY SECURITY FOR MOBILE

Dix ans de leadership dans le domaine de la sécurité mobile

Une technologie en constante évolution, des menaces en constante évolution.

Kaspersky Lab détecte, signale et analyse des programmes mobiles malveillants depuis 2004, à l'époque où Cabir, le premier virus mobile au monde, a fait son apparition sur les systèmes de nos analystes.

Dix ans plus tard, pendant l'année 2014, Kaspersky Lab a paré près de **1,4** million d'attaques de programmes mobiles malveillants,[1] un chiffre qui continue d'augmenter et qui représente une hausse considérable par rapport aux 335 000 attaques uniques enregistrées l'année précédente.

Alors que les smartphones et les tablettes se sont définitivement intégrés à notre vie professionnelle et personnelle, les menaces qui les ciblent se sont elles aussi intensifiées :

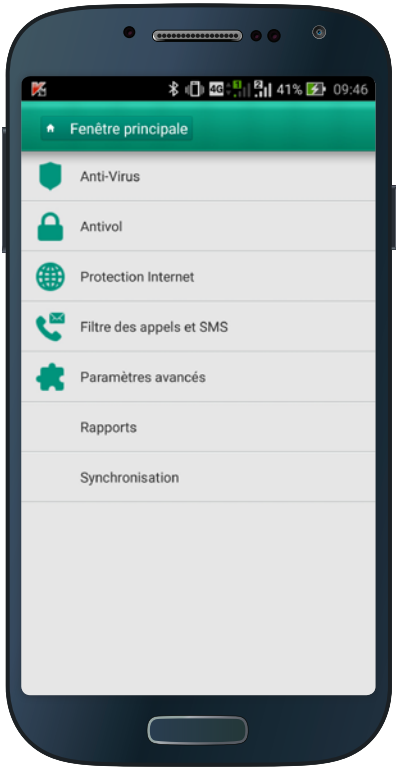
- **Programmes mobiles malveillants** : augmentent à un rythme exponentiel. En 2014, Kaspersky Lab a détecté :
  - **4 643 582** paquets d'installation malveillants
  - **295 539** nouveaux programmes mobiles malveillants
- **BYOD** : entraîne presque autant de risques que d'avantages, sans protection des données d'entreprise, avec un risque de mélange entre les applications personnelles et professionnelles, ainsi que des problèmes d'intégrité des données liés aux tendances d'utilisation.
- **Accès incontrôlé aux données sensibles** : des appareils non sécurisés reçoivent l'accès à des données d'entreprise, sans mot de passe fort, sans chiffrement, sans protection contre le déverrouillage des appareils et sans technologie pour contrôler le sort des données sensibles quand l'appareil est perdu ou volé.
- **Complexité informatique** : l'employé moyen possède trois appareils intelligents ou plus. La diversité des plateformes, des appareils et des applications de gestion qu'il utilise aggrave le problème de gestion informatique.

Kaspersky Security for Mobile offre une sécurité, une gestion et un contrôle proactifs **pour tous les terminaux mobiles**. Nos technologies assurent la sécurité de vos appareils, où qu'ils se trouvent.

Kaspersky Security for Mobile vous protège contre les programmes mobiles malveillants malgré leur constante évolution et vous permettent de bénéficier en toute simplicité d'une visibilité et d'un contrôle complets des smartphones et des tablettes se trouvant dans votre environnement. Le tout à partir d'un point central et avec un minimum de perturbations.

1 http://securelist.com/analysis/kaspersky-security-bulletin/68010/kaspersky-security-bulletin-2014-overall-statistics-for-2014/

PROTECTION AVANCÉE CONTRE LES PROGRAMMES MOBILES MALVEILLANTS



PROTECTION MULTINIVEAUX CONTRE LES TECHNOLOGIES DE PROGRAMMES MALVEILLANTS

Les technologies de sécurité mobile de Kaspersky Lab combinent une protection puissante contre les programmes malveillants à base de signatures avec des technologies proactives assistées par le cloud (Kaspersky Security Network), ce qui leur permet de proposer des taux de détection particulièrement performants tout en parant les menaces mobiles connues et inconnues.

Des analyses à la demande et planifiées associées aux mises à jour automatiques à distance rehaussent la protection des appareils mobiles et des données qu'ils renferment.

PROTECTION WEB

Le contrôle Web mobile intégré assure la sécurité de l'expérience d'un utilisateur en ligne avec son smartphone ou sa tablette, car la technologie de Kaspersky Lab bloque l'accès aux sites malveillants.

Le Safe Browser, qui s'appuie sur notre Kaspersky Security Network (KSN) dans le cloud, permet une analyse constamment mise à jour des ressources en ligne, protège les utilisateurs contre le hameçonnage et contre d'autres attaques en ligne.

SÉPARER LES DONNÉES D'ENTREPRISE DES DONNÉES PERSONNELLES SUR LES APPAREILS PERSONNELS UTILISÉS SUR LE LIEU DE TRAVAIL (BYOD)

MISE EN CONTENEUR D'APPLICATIONS

L'aptitude à séparer les données d'entreprise des données personnelles sur un appareil renforce la sécurité, notamment dans les environnements BYOD.

Kaspersky Security for Mobile permet la « mise en conteneur », c'est-à-dire l'emballage de chaque application professionnelle dans son propre conteneur sécurisé auquel il est possible d'appliquer des politiques supplémentaires, telles que le chiffrement, pour protéger les données d'entreprise sensibles. Les données dans le conteneur ne peuvent pas être copiées ni collées à l'extérieur de celui-ci.

Il est possible de veiller à l'autorisation de l'utilisateur final pour tous les conteneurs avant l'ouverture des applications correspondantes. 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 aux données de bénéficier d'une couche supplémentaire de protection, même si l'application était ouverte au moment du vol ou de la perte de l'appareil.

SUPPRESSION SÉLECTIVE

Quand des employés quittent votre société, assurez-vous qu'ils ne prennent pas vos données avec eux. Kaspersky Security for Mobile permet de supprimer des données d'entreprise mises en conteneur tout en laissant les photos, les listes de lecture, les contacts et d'autres paramètres personnels intacts.

GÉRER ET PROTÉGER L'ACCÈS AUX DONNÉES D'ENTREPRISE

GESTION DES APPAREILS MOBILES

Politiques MDM unifiées pour Microsoft Exchange ActiveSync et MDM pour iOS avec prise en charge de l'application de mots de passe, chiffrement du périphérique, gestion de l'appareil photo et des autres fonctionnalités du périphérique. Une seule interface unifiée gère les plateformes Android, iOS et Windows Phone.

PRISE EN CHARGE DE SAMSUNG KNOX

Kaspersky Security for Mobile prend en charge Samsung KNOX 1.0 et 2.0, assurant la configuration du pare-feu et de l'APN/VPN, ainsi que des paramètres Microsoft Exchange Server pour les téléphones portables et les tablettes Samsung.

OUTILS DE CONTRÔLE

Les contrôles d'application permettent aux administrateurs de gérer et limiter l'utilisation des applications aux logiciels approuvés par la société. Les applications grisées ou non autorisées peuvent être bloquées et les fonctionnalités de l'appareil peuvent être liées à l'installation des applications exigées par la société. Le contrôle d'inactivité des applications permet de demander à l'utilisateur de se reconnecter si une application est inactive pendant un certain temps.

Les contrôles Web permettent à l'administrateur de contrôler l'accès aux sites qui ne sont pas conformes aux politiques de sécurité ou d'utilisation de la société, tels que les réseaux sociaux, les sites de jeu d'argent, les sites pour adultes, les serveurs proxy et d'autres sites indésirables.

DÉTECTION DES TERMINAUX DÉVERROUILLÉS

Les appareils déverrouillés et pour lesquels un accès racine a été obtenu, qu'ils fassent partie d'une initiative BYOD ou qu'ils appartiennent à la société, posent à la société un risque de sécurité considérable. Compte tenu de l'insuffisance des couches de sécurité existantes, le risque lié à la perte de contrôle de ces appareils est sérieux. Kaspersky Security for Mobile peut automatiquement détecter et bloquer les appareils déverrouillés, envoyer des alertes aux administrateurs et même supprimer les données d'un appareil à distance.

PROTECTION AVANCÉE POUR LES APPAREILS PERDUS OU VOLÉS

PRÉVENTION DES VOLS

Kaspersky Security for Mobile propose des fonctionnalités intégrées de protection contre le vol, notamment :

- Verrouillage et déverrouillage de l'appareil à distance
- Localisation d'appareil : permet de trouver un appareil sur une carte
- Les fonctionnalités d'alarme et mugshot facilitent la détection des appareils*
- Surveillance SIM : informe le propriétaire si la carte SIM est remplacée
- Effacement des données : supprime les données sélectionnées dans des conteneurs ou effacent toutes les données de l'appareil.

L'administrateur ou le propriétaire de l'appareil, le cas échéant, peut activer l'ensemble de ces fonctionnalités à distance. L'intégration avec Google Cloud Messaging permet aux administrateurs d'activer des commandes immédiatement (mode push), tandis que le portail libre-service de Kaspersky Lab permet aux utilisateurs d'activer les fonctions anti-vol par eux-mêmes, ce qui assure une réponse rapide en cas de vol ou de perte de l'appareil.

*rafale de 5 photos

SIMPLIFICATION DE LA GESTION INFORMATIQUE

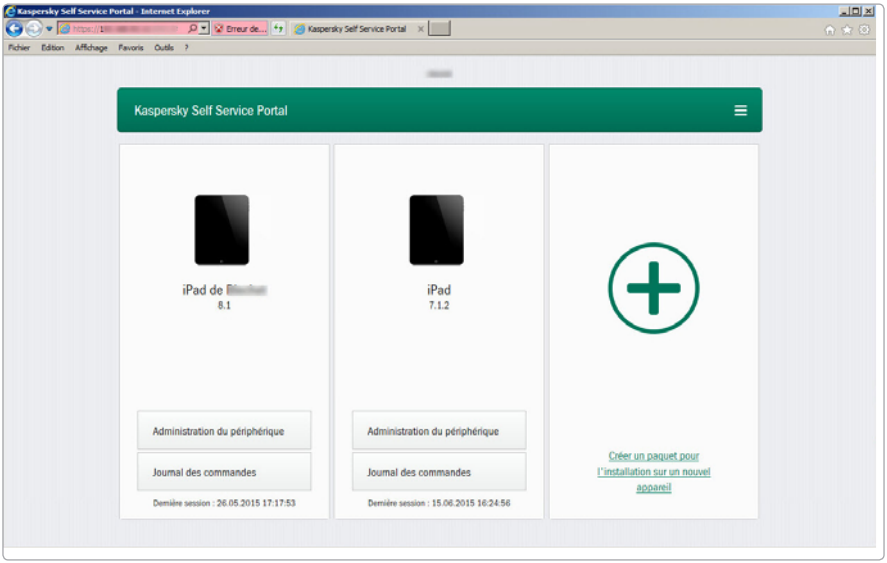
PORTAIL LIBRE-SERVICE

Kaspersky Security for Mobile permet aux administrateurs de mettre en œuvre un portail libre-service confiant certaines tâches routinières et fastidieuses aux utilisateurs finaux. À titre d'exemple, les employés peuvent enregistrer leurs appareils autorisés en quelques clics seulement. Il est possible d'installer automatiquement et d'activer tous les certificats nécessaires par le biais du portail.

En cas de perte ou de vol d'un appareil, les utilisateurs peuvent activer les fonctionnalités de verrouillage, de suppression des données et localisation de l'appareil, entre autres, par le biais du portail libre-service, ce qui permet de réagir le plus rapidement possible dans ce genre de situation.

CONSOLE WEB

Tous les appareils mobiles (et les terminaux fixes) peuvent aussi être gérés à distance sur un navigateur Web, ce qui permet aux administrateurs de bénéficier d'une plus grande souplesse. La console Web Kaspersky Security Center a été étendue pour prendre en charge les fonctions de sécurité et de gestion des appareils mobiles.



PLATEFORME INTÉGRÉE DE SÉCURITÉ INFORMATIQUE : CONSOLE D'ADMINISTRATION UNIQUE

Contrairement à la plupart des autres éditeurs de solutions de sécurité informatique, la gamme étendue de Kaspersky Lab est issue d'un investissement considérable dans des activités internes de recherche et développement, et non d'acquisitions d'entreprises.

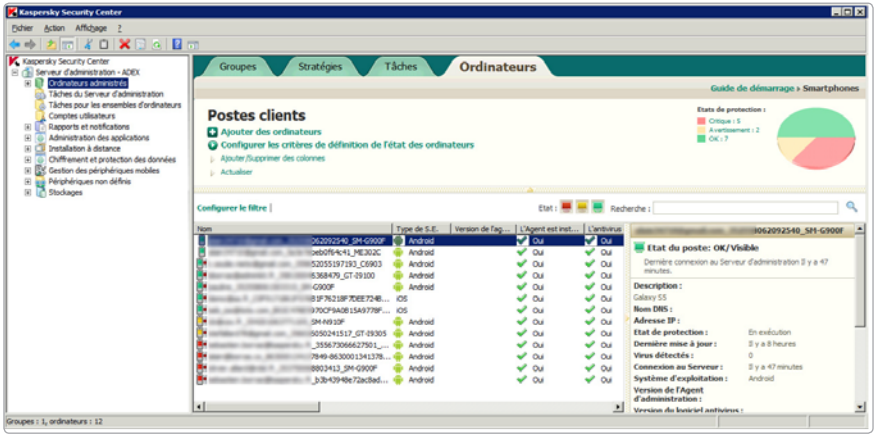
Toutes les technologies de Kaspersky Lab sont développées en interne par des équipes composées d'experts de la sécurité totalement engagés dans leur travail. Cela nous permet de proposer une plateforme intégrée de technologies capable de protéger et de gérer de façon centralisée chaque aspect de la sécurité informatique d'une grande entreprise.

PRISE EN CHARGE DE TOUTES LES PRINCIPALES PLATEFORMES MOBILES

Les smartphones et les tablettes Android, iOS et Windows Phone sont protégés et gérés à l'aide de Kaspersky Security for Mobile.*

GÉRER LES TERMINAUX FIXES ET LES APPAREILS MOBILES À PARTIR D'UN SEUL ÉCRAN

L'utilisation de la console d'administration unique Kaspersky security Center permet la gestion centralisée de tous les smartphones et toutes les tablettes en parallèle avec les ordinateurs fixes traditionnels (Windows, Mac, Linux). Cela permet aux administrateurs informatiques d'obtenir une plus grande visibilité des actifs de l'entreprise tout en homogénéisant l'application des politiques à tous les niveaux de l'entreprise. En outre, en améliorant l'efficacité de la gestion et de la maintenance.



* fonctionnalités variables selon le système d'exploitation

CONCESSION DE LICENCE

Kaspersky Security for Mobile est inclus dans :

- **Kaspersky Endpoint Security for Business – Select** : comprend la sécurité des terminaux et des serveurs de fichier, ainsi que des outils de contrôle, de protection des terminaux mobiles et de MDM.
- **Kaspersky Endpoint Security for Business – Advanced** : comprend toutes les caractéristiques de la version Select et propose des fonctionnalités supplémentaires, notamment le chiffrement et la gestion de parc (comprenant la gestion des vulnérabilités tous éditeurs).
- **Kaspersky Total Security for Business** : une plateforme complète et étendue pour la protection des terminaux comprenant toutes les caractéristiques des versions antérieures avec la protection du Web et de la messagerie.
- **Kaspersky Security for Mobile en tant que solution 'à la carte'** : protection et gestion des terminaux mobiles à l'aide des technologies de sécurité mobile de Kaspersky Lab, au sein d'une solution autonome achetée séparément.

CENTRALISATION DE LA SÉCURITÉ, DE LA VISIBILITÉ ET DE LA GESTION POUR LES TERMINAUX D'ENTREPRISE ET BYOD

Kaspersky Security for Mobile veille à la sécurité des appareils, quel que soit l'endroit où ils se trouvent, qu'ils appartiennent à l'entreprise ou qu'ils soient utilisés dans le cadre du processus BYOD. 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.

Obtenez la visibilité dont vous avez besoin : plus besoin de jouer aux devinettes pour essayer d'identifier et de comprendre le statut de chaque appareil. Sachez avec précision quels sont les appareils mobiles des employés qui accèdent aux ressources de votre entreprise.

Réduisez le risque de perte de données lié au vol d'appareil ou aux programmes malveillants : activez les fonctionnalités de protection mobile pour protéger les appareils et les données qu'ils renferment.

Simplifiez la gestion informatique : protégez et gérez les appareils mobiles et les terminaux fixes ensemble, à l'aide de la même plateforme de sécurité informatique intégrée et à partir de la même console d'administration centralisée.


Twitter.com/
kasperskyfrance


Facebook.com/
kasperskylabfrance


Youtube.com/user/
KasperskyFrance

Kaspersky Lab
www.kaspersky.fr

Tout savoir sur la sécurité sur Internet :
www.viruslist.com/fr/

Trouver un partenaire près de chez vous :
http://www.kaspersky.fr/partners/buyoffline/liste-des-partenaires

Mars 15/Global

KASPERSKY lab