KASPERSKY MOBILE SECURITY FOR ENTERPRISE

Sécuriser les appareils mobiles au-delà de votre périmètre

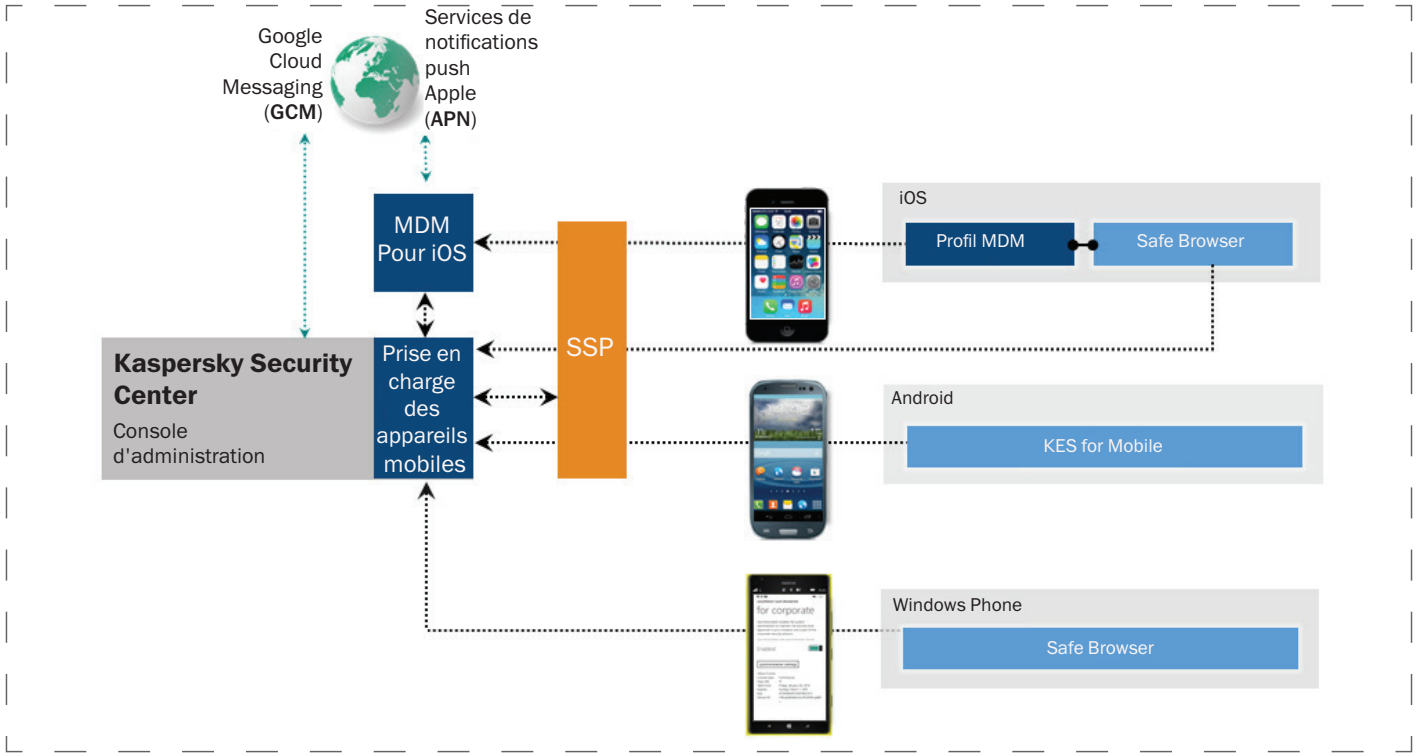
La quantité et le degré de sophistication des cybermenaces qui ciblent les appareils mobiles en particulier sont en constante évolution, car les cybercriminels connaissent la valeur des données d'entreprise qu'ils peuvent contenir. Mais la menace ne s'arrête pas là. Un appareil mobile mal sécurisé peut servir de tremplin pour accéder à votre réseau, avec des conséquences catastrophiques à long terme au niveau de la réputation, et des pertes financières.

Les avantages de l'accès aux données « partout et à tout moment » en termes de productivité sont trop importants pour être ignorés, et le BYOD (l'utilisation par les employés de leurs propres smartphones et tablettes pour effectuer leur travail) est une tendance qui s'affirme. Mais ces comportements introduisent de nouveaux risques qui doivent être totalement pris en compte pour que l'entreprise dans son ensemble demeure sécurisée. Le besoin en technologies de sécurité mobile efficaces n'a jamais été aussi grand.

Kaspersky Security for Mobile protège et contrôle les données de votre entreprise sur les appareils mobiles et sécurise ces derniers, couvrant toutes les principales plateformes dans une seule solution pour les entreprises.

Les niveaux de protection renforcée contre les menaces se combinent au contrôle du Web et des applications pour réguler l'accès et l'utilisation, tandis que la « conteneurisation d'applications » isole et sécurise les données de l'entreprise dans des conteneurs chiffrés sur l'appareil, qu'il est possible de supprimer. Une large palette de fonctionnalités antivol, activées par l'utilisateur ou le service informatique, permet de prendre des mesures décisives et immédiates si un appareil est égaré, dérobé ou subit une menace.

La gestion des applications et des appareils mobiles (MDM/MAM) est combinée à la protection puissante et à plusieurs niveaux de Kaspersky Lab pour former une solution de sécurité unifiée administrée à partir d'une console unique (Kaspersky Security Center) avec tous vos terminaux virtuels et physiques, ou administrée en fonction du rôle selon votre préférence.



Architecture de la solution

Principales fonctionnalités

PROTECTION MULTI-NIVEAUX CONTRE LES PROGRAMMES MALVEILLANTS

Protection basée sur les signatures, proactive et basée dans le cloud (via Kaspersky Security Network - KSN) contre les programmes malveillants mobiles connus et inconnus. Des analyses programmées ou à la demande sont combinées à des mises à jour automatiques pour une protection supérieure.

CONTRÔLE DES APPLICATIONS

L'utilisateur peut être limité aux applications sûres, en interdisant l'utilisation de logiciels non autorisés ou figurant sur liste grise ; la fonctionnalité de l'appareil peut même être dépendante en installant des applications spécifiques. Le contrôle de l'inactivité requiert que l'utilisateur se connecte de nouveau si une application est inactive pendant une durée précisée, ce qui permet de protéger les données en cas de perte ou de vol de l'appareil même si une application est restée ouverte.

PROTECTION CONTRE LE PHISHING ET LE COURRIER INDÉSIRABLE

Les technologies puissantes de protection contre le phishing et le courrier indésirable protègent l'appareil et les données qu'il contient.

PROTECTION ANTIVOL

La protection antivol à distance comprend la suppression des données, le verrouillage de l'appareil, la localisation, la surveillance de la carte SIM, le « mugshot » et l'alarme. L'application de ces fonctionnalités est rapide : la messagerie instantanée avec Google Cloud Messaging (GCM) diminue le temps de réaction, tandis que l'utilisation du portail en libre-service (voir ci-dessous) ne requiert aucune action de l'administrateur.

DÉTECTION DES TERMINAUX DÉVERROUILLÉS

Détection et signalement automatiques suivis du blocage automatique de l'accès au conteneur, avec suppression de données sélectionnées ou de l'intégralité des données se trouvant sur l'appareil.

GESTION CENTRALISÉE OU BASEE SUR DES RÔLES

Tous les appareils mobiles sont gérés à partir d'une console unique, avec les autres terminaux. La gestion à distance à partir d'un ordinateur se fait via une console Web. L'administration basée sur des rôles peut être mise en place si nécessaire.

GESTION DES APPAREILS MOBILES (MDM)

La prise en charge de Microsoft® Exchange ActiveSync, Apple MDM, Samsung KNOX 2.0 permet d'appliquer un grand nombre de politiques à travers une interface unifiée, quelle que soit la plateforme. (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.)

CONTRÔLE WEB/NAVIGATION SÉCURISÉE

Les analyses en temps réel de la réputation (continuellement mises à jour) sont utilisées pour bloquer l'accès aux sites Web malveillants et non autorisés, ainsi que pour garantir une navigation sécurisée.

CONTENEURISATION

Permet de séparer les données de l'entreprise et les données personnelles en « empaquetant » vos applications dans des conteneurs. Les données sensibles conteneurisées peuvent être chiffrées ou supprimées de manière sélective sur l'appareil d'un employé sans répercussion sur les données personnelles. Pour les appareils Android, les applications peuvent également être installées, confinées et contrôlées dans un « profil professionnel » déployé sur l'appareil qu'il est possible de supprimer.

PORTAIL LIBRE-SERVICE

Déléguez à l'employé les tâches quotidiennes d'administration de la sécurité, telles que l'enregistrement des appareils approuvés (génération automatique du certificat comprise). En cas de perte d'un appareil, l'employé peut effectuer toutes les actions antivol disponibles directement via le portail.

Pour en savoir plus sur la protection de vos terminaux mobiles, veuillez contacter l'équipe commerciale de Kaspersky Lab Enterprise.

Kaspersky Mobile Security for Enterprise/15 déc/Global

KASPERSKY lab