KASPERSKY SECURITY FOR MOBILE

KASPERSKY lab

KASPERSKY SECURITY FOR MOBILE

Diez años de liderazgo en seguridad para dispositivos móviles

Tecnología en constante evolución contra las amenazas en constante evolución.

Kaspersky Lab lleva detectando, denunciando y analizando malware contra dispositivos móviles desde 2004, cuando Cabir, el primer virus para dispositivos para móviles del mundo, llegó a los sistemas de nuestros analistas.

Una década después, y solo en 2014, Kaspersky Lab se enfrentó a casi **1,4** millones de ataques de malware contra dispositivos móviles[1], un importante crecimiento en constante aumento frente a los 335 000 ataques registrados el año anterior.

Como los smartphones y las tablets se han integrado en nuestra vida laboral y trabajo diarios, las amenazas que los acompañan han aumentado:

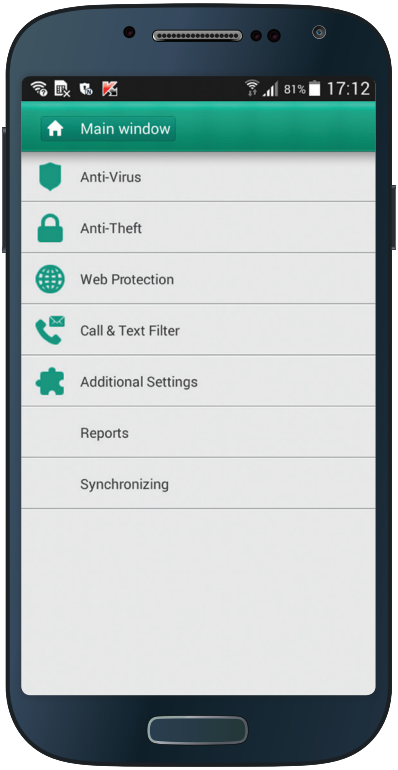
- **Malware contra dispositivos móviles**: se incrementa a un ritmo exponencial tanto para las plataformas Android como iOS. Solo en 2014, Kaspersky Lab ha detectado:
  - **4 643 582** paquetes de instalación maliciosos
  - **295 539** nuevos programas maliciosos para dispositivos móviles
- **Iniciativa BYOD ("traiga su propio dispositivo")**: introduce casi tantos riesgos como beneficios, ya que los datos empresariales no protegidos junto con las aplicaciones personales y los patrones de uso plantean problemas de integridad de los datos.
- **Acceso no controlado a los datos confidenciales**: los dispositivos sin protección obtienen acceso incontrolado a los datos de la empresa mediante las contraseñas poco seguras, la ausencia de cifrado, los dispositivos liberados y la ausencia de una tecnología que controle lo que le ocurre a los datos confidenciales en dispositivos perdidos o robados.
- **Complejidad de IT**: el empleado medio trabaja con tres o más dispositivos inteligentes. Las diferentes plataformas, los diferentes dispositivos, las diferentes aplicaciones de gestión... Todo ello se traduce en un gran problema de gestión de IT.

Kaspersky Security for Mobile ofrece seguridad, gestión y control proactivos **de todos los endpoints móviles**. Nuestras tecnologías garantizan que su dispositivo está protegido, independientemente de dónde se encuentre.

Kaspersky Security for Mobile le permite protegerse del malware contra dispositivos móviles en constante evolución y obtener visibilidad fácil y completa, y control de los smartphones y tablets en su entorno. Todo ello desde una ubicación central y con interrupción mínima.

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

ANTIMALWARE CONTRA DISPOSITIVOS MÓVILES AVANZADO



TECNOLOGÍAS ANTIMALWARE A VARIOS NIVELES

Las tecnologías de seguridad para dispositivos móviles de Kaspersky Lab combinan un potente antimalware basado en firma con tecnologías proactivas y con asistencia en la nube (Kaspersky Security Network) para proporcionar índices de detección avanzados a la vez que protegen de amenazas de malware, conocidas y desconocidas, que afectan a los dispositivos móviles.

Los análisis a petición y programados se combinan con las actualizaciones automáticas inalámbricas para aumentar la protección para los dispositivos móviles y los datos que estos almacenan.

PROTECCIÓN WEB

El control web para dispositivos móviles integrado garantiza una experiencia en Internet segura para smartphones y tablets; la tecnología de Kaspersky Lab bloquea el acceso a sitios maliciosos.

Respaldado por nuestra red Kaspersky Security Network (KSN) en la nube, Safe Browser ofrece análisis de reputación continuamente actualizados de los recursos web, protegiendo a los usuarios de ataques de phishing y otros ataques maliciosos basados en la web.

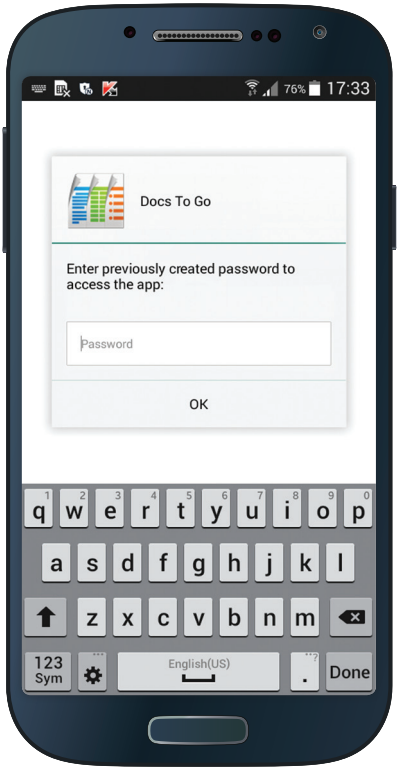
SEPARACIÓN DE LOS DATOS DE LA EMPRESA Y PERSONALES PARA BYOD

CONTENERIZACIÓN

La capacidad de separar los datos personales y de la empresa en cualquier dispositivo añade un nivel adicional de seguridad, especialmente en entornos BYOD.

Kaspersky Security for Mobile permite la "contenerización", envolviendo cada aplicación empresarial en su propio contenedor seguro al que se pueden aplicar políticas adicionales, como el cifrado, para proteger los datos de la empresa confidenciales. Los datos del contenedor no se pueden copiar ni pegar fuera del contenedor.

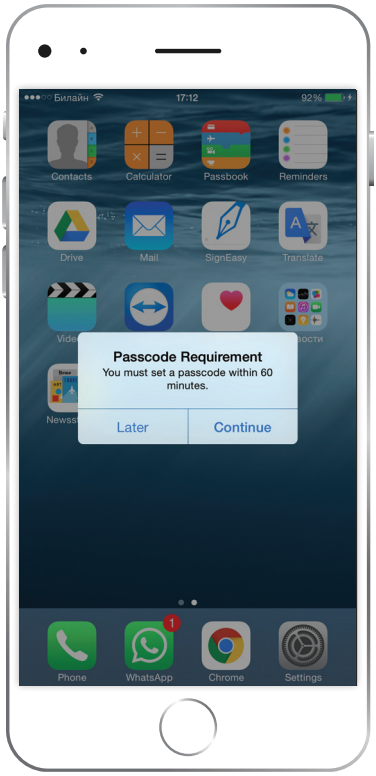
Se puede implementar la necesidad de autorización por parte del usuario final en todos los contenedores antes del inicio de la aplicación. El control de inactividad de las aplicaciones permite a los administradores obligar al usuario a que vuelva a iniciar una sesión cuando la aplicación está inactiva durante un periodo de tiempo específico. Esto añade un nivel adicional de protección a los datos, incluso si una aplicación está abierta en el dispositivo perdido o robado.



BORRADO SELECTIVO

Cuando los empleados cambien de empresa, asegúrese de que no se llevan sus datos. Kaspersky Security for Mobile permite eliminar los datos de la empresa almacenados en contenedores y dejar intactos las fotografías, las listas de reproducción, los contactos y otros ajustes personales.

GESTIÓN Y PROTECCIÓN DEL ACCESO A LOS DATOS DE LA EMPRESA



GESTIÓN DE DISPOSITIVOS MÓVILES (MDM)

Las políticas MDM unificadas para Microsoft Exchange ActiveSync y MDM para iOS son compatibles con la aplicación de contraseñas, el cifrado del dispositivo, la utilización de la cámara y otras funciones del dispositivo relacionadas. Una interfaz unificada gestiona las plataformas Android, iOS y Windows Phone.

COMPATIBILIDAD CON SAMSUNG KNOX

Kaspersky Security for Mobile es compatible con Samsung KNOX 1.0 y 2.0, y permite la configuración del firewall y APN/VPN, así como la configuración de Microsoft Exchange Server para teléfonos móviles y tablets Samsung.

HERRAMIENTAS DE CONTROL

Los controles de aplicaciones permiten a los administradores gestionar y restringir el uso de aplicaciones, de forma que solo el software aprobado por la empresa se pueda ejecutar. Las aplicaciones no deseadas o no autorizadas se pueden bloquear, y se puede establecer que la funcionalidad del dispositivo dependa de la instalación de aplicaciones necesarias para la empresa. El control de inactividad de las aplicaciones obliga al usuario a que vuelva a iniciar una sesión si una aplicación está inactiva durante un periodo de tiempo definido previamente.

Los controles web permiten que el administrador tenga control sobre el acceso a los sitios que no se ajusten a las políticas de seguridad o uso de la empresa (por ejemplo, sitios de redes sociales, apuestas, contenido para adultos, servidores proxy u otros sitios no deseados).

DETECCIÓN DE LIBERACIÓN DE DISPOSITIVOS

Los dispositivos liberados, tanto si forman parte de una iniciativa BYOD como si son propiedad de la empresa, representan un riesgo de seguridad importante para la empresa. Como siempre carecen de niveles de seguridad fundamentales, el riesgo asociado a la pérdida de control sobre estos dispositivos es muy grave. Kaspersky Security for Mobile puede detectar y bloquear automáticamente los dispositivos liberados, emitir alertas de administrador e incluso borrar de forma remota los datos del dispositivo.

PROTECCIÓN AVANZADA PARA DISPOSITIVOS PERDIDOS O ROBADOS

ANTIRROBO

Kaspersky Security for Mobile contiene funciones antirrobo integradas, entre las que se incluyen las siguientes:

- Bloqueo/desbloqueo remoto del dispositivo.
- Localización del dispositivo, que permite localizar el dispositivo en un mapa.
- La alarma y la captura de instantáneas facilitan la detección del dispositivo.
- Vigilancia de la SIM, que notifica al propietario si se ha sustituido la tarjeta SIM.
- Borrado del dispositivo, que elimina los datos seleccionados en contenedores o borra completamente el dispositivo.

Todas estas funciones se pueden activar de forma remota por el administrador o el propietario del dispositivo, en función de la situación. La integración con el servicio de mensajería en la nube de Google, por ejemplo, permite al administrador introducir los comandos casi de inmediato, mientras que el portal de autoservicio de Kaspersky Lab permite a los usuarios activar las funciones antirrobo personalmente, lo que garantiza una respuesta rápida ante la pérdida o el robo de un dispositivo.

REDUCCIÓN DE LA COMPLEJIDAD DE LA GESTIÓN DE IT

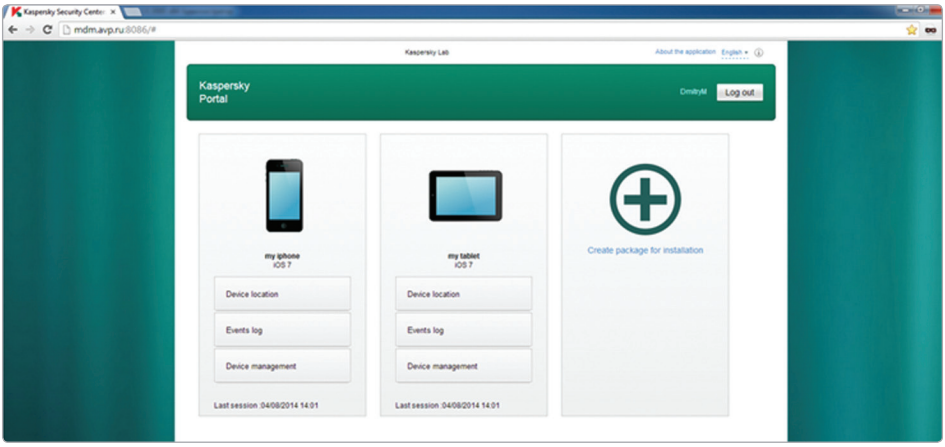
PORTAL DE AUTOSERVICIO

Kaspersky Security for Mobile permite a los administradores implementar un portal de autoservicio a través del cual se pueden delegar en los usuarios finales aquellas tareas rutinarias y que consumen mucho tiempo. Por ejemplo, los empleados pueden registrar sus dispositivos autorizados en la red con solo unos pocos clics. Todos los certificados necesarios pueden instalarse automáticamente y activarse a través del portal.

En caso de pérdida o robo de un dispositivo, los usuarios pueden activar el bloqueo, el borrado, la localización y otras funciones relacionadas con el dispositivo a través del portal de autoservicio, garantizando así los tiempos de respuesta más eficaces.

CONSOLA WEB

Para que el administrador disfrute de flexibilidad adicional, todos los dispositivos móviles (y endpoints tradicionales) se pueden gestionar de forma remota a través de un navegador web. La consola web de Kaspersky Security Center se ha ampliado para admitir seguridad en los dispositivos móviles y capacidades de gestión.



PLATAFORMA DE SEGURIDAD DE IT INTEGRADA: UNA ÚNICA CONSOLA DE ADMINISTRACIÓN

A diferencia de la mayoría de los demás proveedores de seguridad de IT, la cartera de productos ampliada de Kaspersky Lab es el resultado de importantes inversiones en investigación y desarrollo internos, no de adquisiciones de empresas.

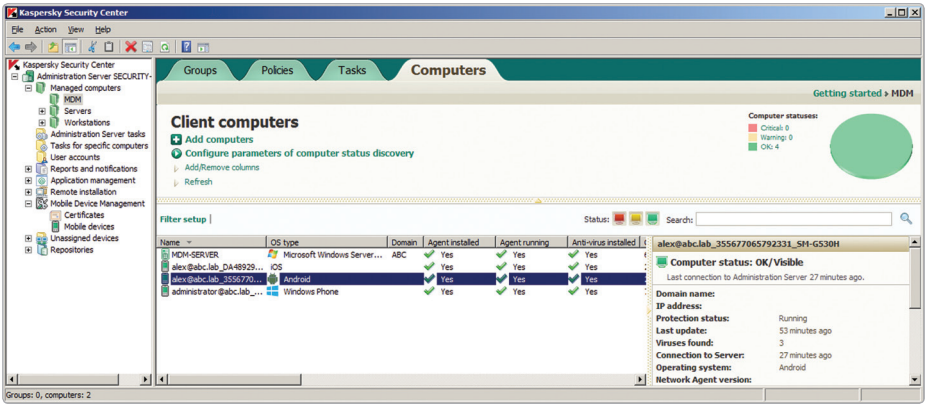
Todas las tecnologías de Kaspersky Lab han sido desarrolladas por equipos de expertos especializados en seguridad. El resultado es una plataforma integrada de tecnologías, capaz de proteger y gestionar de forma centralizada todos los aspectos de la seguridad de IT empresarial.

COMPATIBILIDAD CON TODAS LAS PRINCIPALES PLATAFORMAS MÓVILES

Los smartphones y tablets Android, iOS y Windows Phone están protegidos y gestionados con Kaspersky Security for Mobile.

GESTIÓN DE LOS ENDPOINTS TRADICIONALES Y DISPOSITIVOS MÓVILES DESDE UNA ÚNICA PANTALLA

Como parte de una plataforma de seguridad integrada, Kaspersky Security for Mobile permite que todos los smartphones y tablets se gestionen de forma centralizada, junto con sus endpoints homólogos tradicionales. Esto proporciona a los administradores de IT una mayor visibilidad de los activos de la empresa, junto con la capacidad de aplicar políticas coherentes de forma generalizada. Por otra parte, gracias a la mejora en la eficiencia de la gestión y el mantenimiento, los administradores podrán centrarse en otros aspectos de la empresa.



LICENCIAS

Kaspersky Security for Mobile se incluye en:

- **Kaspersky Endpoint Security for Business – Select**: incluye seguridad para endpoints y servidores de archivos, con herramientas de control y movilidad.
- **Kaspersky Endpoint Security for Business – Advanced**: incluye todas las funciones de seguridad para endpoints de Select, además de funciones adicionales, como cifrado, gestión de parches, funciones de gestión ampliadas y movilidad.
- **Kaspersky Total Security for Business**: una plataforma de protección para endpoints amplia y completa que incluye todas las funciones de los otros niveles, protección para web y mensajería, y funciones de movilidad.
- **Kaspersky Security for Mobile como solución adaptada**: protección y gestión de endpoints móviles con las tecnologías de seguridad para dispositivos móviles de Kaspersky Lab mediante una solución independiente que se vende por separado.

SEGURIDAD, VISIBILIDAD Y GESTIÓN CENTRALIZADAS PARA EMPRESAS Y PARA ENDPOINTS BYOD

Kaspersky Security for Mobile garantiza que los dispositivos están protegidos, independientemente de dónde estén y tanto si son parte de la iniciativa BYOD o los proporciona la empresa. Ofrece, de forma rápida y sencilla, mayor visibilidad y control sobre los smartphones y tablets de su entorno desde una ubicación central y sin apenas interrupciones.

Obtenga la visibilidad que necesita: elimine las conjeturas a la hora de intentar identificar y comprender el estado de cada dispositivo. Obtenga una sólida comprensión de los dispositivos móviles de los empleados que tienen acceso a los recursos de la empresa.

Minimice el riesgo de pérdida de datos por el robo de dispositivos o malware: active funciones de protección para dispositivos móviles que garanticen que los dispositivos están protegidos y que los datos que tienen almacenados están seguros.

Reduzca la complejidad de la gestión de IT: proteja y gestione los dispositivos móviles y los endpoints tradicionales de forma simultánea mediante el uso de la misma plataforma de seguridad de IT integrada y la consola de administración centralizada.


Twitter.com/
Kaspersky


Facebook.com/
Kaspersky


Youtube.com/
Kaspersky

Kaspersky Lab
www.kaspersky.es

Todo sobre seguridad en Internet:
www.viruslist.com/sp

Encuentre un partner próximo:
www.kaspersky.com/buyoffline

Marzo de 2015/Global

KASPERSKY lab