▶ KASPERSKY SECURITY FOR MOBILE

Seguridad, gestión y control a varios niveles para todos los endpoints móviles

Los dispositivos móviles son cada vez más atractivos para los cibercriminales. Mientras tanto, la iniciativa "traiga su propio dispositivo" (BYOD) contribuye a una mezcla cada vez más compleja de dispositivos, creando así un entorno de gestión y control desafiante para los administradores de IT.
Kaspersky Security for Mobile garantiza que el dispositivo esté protegido, independientemente de dónde esté. Protege contra malware móvil que evoluciona constantemente. 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.

- **Potente antimalware**
- **Antiphishing y antispam**
- **Protección web**
- **Control de aplicaciones**
- **Detección de liberación de dispositivos**
- **Contenerización**
- **Antirrobo**
- **Gestión de dispositivos móviles**
- **Portal de autoservicio**
- **Gestión centralizada**
- **Consola Web**
- **Plataformas compatibles:**
  - Android™
  - iOS
  - Windows Phone

INFORMACIÓN DESTACADA

ANTIMALWARE AVANZADO PARA GARANTIZAR LA SEGURIDAD DE LOS DISPOSITIVOS Y DATOS MÓVILES

Solo en 2014, Kaspersky Lab se enfrentó a casi 1,4 millones de ataques de malware contra dispositivos móviles. Kaspersky Security for Mobile combina antimalware con profundos niveles de tecnologías de protección que protegen contra amenazas conocidas y desconocidas para los datos almacenados en los dispositivos móviles.

GESTIÓN DE DISPOSITIVOS MÓVILES (MDM)

La integración con las principales plataformas de gestión de dispositivos móviles permite la implementación y el control inalámbricos de forma remota para facilidad de uso y gestión más sencillas de dispositivos Android, iOS y Windows Phone.

GESTIÓN DE APLICACIONES MÓVILES (MAM)

La contenerización y las funciones de borrado selectivo permiten la separación de los datos personales y de empresa en un mismo dispositivo, lo que fomenta las iniciativas BYOD. Junto con nuestras funciones de cifrado y tecnologías antimalware, esto hace de Kaspersky Security for Mobile una solución de protección para móviles proactiva, en lugar de una solución que simplemente intente aislar un dispositivo y sus datos.

GESTIÓN CENTRALIZADA

La gestión de varias plataformas y dispositivos desde la misma consola, como ocurre con otros endpoints, aumenta la visibilidad y el control sin necesidad de un esfuerzo adicional ni de más tecnología que gestionar.

FUNCIONES DE SEGURIDAD Y GESTIÓN DE DISPOSITIVOS MÓVILES

POTENTE ANTIMALWARE
Protección basada en firmas, proactiva y con asistencia en la nube (a través de Kaspersky Security Network, KSN) frente a las amenazas de malware, conocidas y desconocidas, que afectan a los dispositivos móviles. Los análisis a petición y programados se combinan con las actualizaciones automáticas para aumentar la protección.

ANTIPHISHING Y ANTISPAM
Potentes tecnologías antiphishing y antispam protegen tanto el dispositivo como sus datos de ataques de phishing, y ayudan a descartar mediante un filtro las llamadas y los textos no deseados.

CONTROL WEB/NAVEGADOR SEGURO
Compatibles con Kaspersky Security Network (KSN), estas tecnologías funcionan en tiempo real para bloquear el acceso a sitios web maliciosos y no autorizados. Un navegador seguro ofrece análisis de reputación continuamente actualizados, garantizando así una navegación móvil segura.

CONTROL DE APLICACIONES
Integrado con KSN, los controles de aplicaciones restringen el uso de las aplicaciones exclusivamente a software autorizado, prohibiendo el uso de software no autorizado o gris. Permite que las funciones del dispositivo dependan de la instalación de las aplicaciones requeridas. El control de inactividad de las aplicaciones permite a los administradores solicitar que el usuario vuelva a iniciar una sesión si una aplicación está inactiva durante un periodo de tiempo definido. Esto protege los datos incluso si una aplicación está abierta cuando el dispositivo se pierde o es robado.

DETECCIÓN DE LIBERACIÓN DE DISPOSITIVOS
La detección y comunicación automáticas de liberación de dispositivos se puede seguir con el bloqueo automático del acceso a los contenedores, el barrido selectivo o el borrado total del dispositivo.

CONTENERIZACIÓN
Separe los datos empresariales de los personales "envolviendo" las aplicaciones en contenedores. Se pueden aplicar políticas adicionales, como el cifrado, para proteger los datos confidenciales. El borrado selectivo permite la eliminación de datos almacenados en los contenedores en un dispositivo cuando un empleado deja de trabajar en la empresa, sin que ello repercuta en sus datos personales.

ANTIRROBO
En el caso de pérdida o robo de un dispositivo, se pueden activar las funciones antirrobo remotas, incluidas el borrado, el bloqueo del dispositivo, la localización, la vigilancia de la SIM, la realización de una foto de identificación y la alarma de detección de dispositivo. En función del caso, los comandos antirrobo se puede aplicar de forma muy flexible. Por ejemplo, la integración con el servicio de mensajería en la nube de Google (GCM) permite proporcionar los comandos casi al instante, agilizando así los tiempos de reacción y mejorando la seguridad, mientras que el envío de comandos a través del portal de autoservicio no requiere ninguna acción por parte del administrador.

GESTIÓN DE DISPOSITIVOS MÓVILES (MDM)
La compatibilidad con Microsoft Exchange ActiveSync, Apple MDM y Samsung KNOX 2.0 ofrece una gran variedad de políticas a través de una interfaz unificada, con independencia de la plataforma. Por ejemplo, implemente el cifrado y el uso de contraseñas o controle el uso de la cámara mediante la aplicación de políticas a usuarios individuales o grupos, la gestión de la configuración APN/VPN, etc.

PORTAL DE AUTOSERVICIO
Delegue la gestión rutinaria de la seguridad en los empleados y active el registro automático de dispositivos aprobados. Durante el proceso de activación del nuevo dispositivo, todos los certificados necesarios se pueden enviar automáticamente a través del portal sin necesidad de que el administrador realice ninguna acción. En el caso de pérdida del dispositivo, el empleado puede realizar todas las acciones antirrobo disponibles a través del portal.

GESTIÓN CENTRALIZADA
Gestione todos los dispositivos móviles de forma centralizada, desde una única consola, que también permite gestionar la seguridad de IT para todos los demás endpoints.
La consola web permite a los administradores controlar y gestionar los dispositivos de forma remota, desde cualquier equipo.

Cómo comprarlo

Kaspersky Security for Mobile se incluye en:

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

Kaspersky Security for Mobile también se puede adquirir por separado como solución adaptada.

Póngase en contacto con su distribuidor para obtener más información y consultar los precios.

Kaspersky Security for Mobile/15 de febrero/Global