

KASPERSKY TOTAL SECURITY FOR BUSINESS

Encriptación, eficiencia integral de TI y herramientas de aplicación de políticas, más protección de extremo a extremo contra el malware.

Kaspersky Total Security for Business ofrece la plataforma más completa de protección y manejo que se ofrece hoy día en la industria. Kaspersky Total Security for Business asegura cada nivel de su red e incluye potentes herramientas de configuración para garantizar que sus usuarios sean productivos y se encuentren libres de la amenaza del malware, independientemente del dispositivo o ubicación.

Las capacidades de protección y manejo que necesita

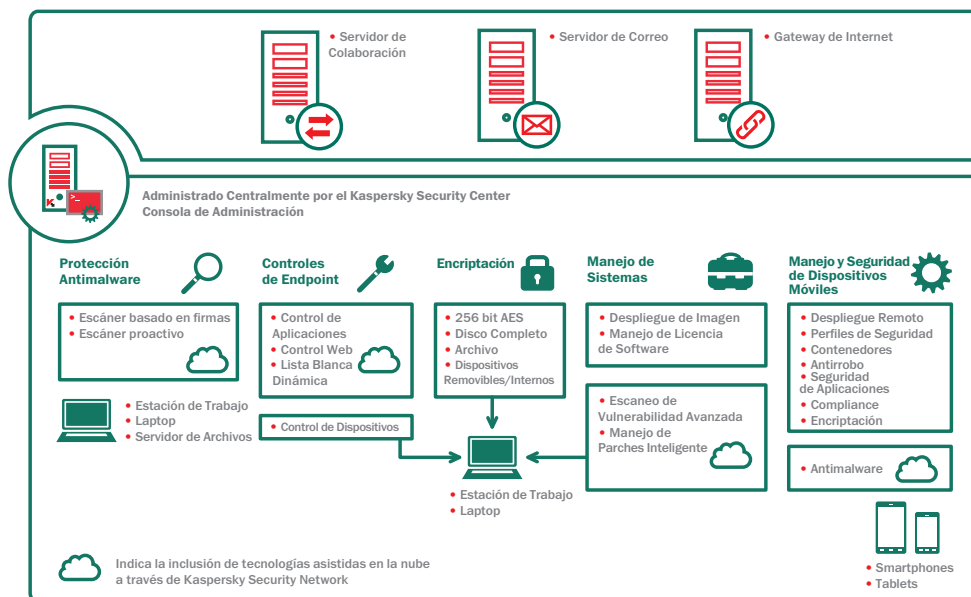
Kaspersky ha desarrollado potentes capacidades de clase empresarial en los niveles progresivos de nuestras ofertas; pero hemos hecho la tecnología lo suficientemente simple y sin complicaciones para negocios de cualquier tamaño.

¿Cuál es el nivel adecuado para Usted?

- CORE
- SELECT
- ADVANCED
- **TOTAL**

FUNCIONALIDADES INCLUIDAS:

- ANTIMALWARE
- FIREWALL
- PROTECCIÓN ASISTIDA EN LA NUBE A TRAVÉS DE KASPERSKY SECURITY NETWORK
- CONTROL DE APLICACIONES
- LISTA BLANCA DE APLICACIONES
- CONTROL WEB
- CONTROL DE DISPOSITIVOS
- PROTECCIÓN DEL SERVIDOR DE ARCHIVOS
- MANEJO DEL DISPOSITIVO MÓVIL (MDM)
- SEGURIDAD DE ENDPOINT MÓVIL (PARA TABLETS Y SMARTPHONES)
- ENCRYPTACIÓN
- CONFIGURACIÓN Y DESPLIEGUE DE SISTEMAS
- ESCÁNER DE VULNERABILIDADES AVANZADO
- CONTROL DE ADMISIÓN A LA RED
- MANEJO DE PARCHES
- SEGURIDAD PARA EL SERVIDOR DE CORREO
- PROTECCIÓN DEL GATEWAY DE WEB/INTERNET
- SEGURIDAD DEL SERVIDOR DE COLABORACIÓN



▶ LA ÚNICA PLATAFORMA DE SEGURIDAD REAL EN LA INDUSTRIA

Una única consola

Desde una misma pantalla, el administrador puede ver y manejar todo el esquema de seguridad —máquinas virtuales, dispositivos físicos y móviles.

Una única plataforma

Kaspersky Lab desarrolló su consola, módulos de seguridad y herramientas internamente y no los adquirió de otras compañías. Significa que los mismos programadores que trabajan desde el mismo código base desarrollaron tecnologías que dialogan y funcionan en conjunto. El resultado es estabilidad, políticas integradas, reportes útiles y herramientas intuitivas.

Un único costo

Todas las herramientas son de un mismo proveedor, se entregan en una misma instalación, de manera tal que no tiene que solicitar un nuevo presupuesto ni proceso de justificación para que sus riesgos de seguridad se encuentren en línea con los objetivos de su negocio.

CARACTERÍSTICAS DE LA SEGURIDAD MOVIL:

TECNOLOGÍAS ANTIMALWARE INNOVADORAS

La detección combinada basada en firmas, proactiva y con asistencia en la nube implica protección en tiempo real. Un navegador seguro y el antispam aumentan la seguridad.

SOPORTE PARA LOS DISPOSITIVOS DE PROPIEDAD DEL EMPLEADO

¿Iniciativa BYOD? Los datos y aplicaciones corporativos se aíslan en contenedores encriptados que son transparentes para el usuario. Estos datos se pueden borrar de manera independiente.

DESPLIEGUE CON APROVISIONAMIENTO OVER-THE-AIR (OTA)

Preconfiguración y despliegue de aplicaciones de manera centralizada, utilizando SMS, correo electrónico y PC.

HERRAMIENTAS ANTIRROBO REMOTAS

Supervisión de SIM, Bloqueo Remoto, Borrado y Búsqueda evitan el acceso no autorizado a los datos corporativos si se pierde o roba un dispositivo móvil.

CONTROL DE APLICACIONES PARA DISPOSITIVOS MÓVILES

Monitorea las aplicaciones instaladas en un dispositivo móvil, según las políticas grupales predefinidas. Incluye un grupo de "Aplicación Obligatoria".

PROTECCIÓN DE ENDPOINT:

ANTIMALWARE DE ENDPOINT SUPERIOR

Métodos tradicionales basados en firmas, proactivos, comprobados en la industria y basados en la nube para detectar amenazas de malware.

PROTECCIÓN ASISTIDA EN LA NUBE

Kaspersky Security Network (KSN) ofrece una respuesta a las posibles amenazas mucho más rápido que los métodos tradicionales de protección. El tiempo de respuesta de KSN a una amenaza de malware puede ser tan mínimo ¡que llega a 0.02 segundos!

CONFIGURACIÓN DEL SISTEMA Y MANEJO DE PARCHES:

MANEJO DE PARCHES

Escaneo profundo avanzado de vulnerabilidades, combinado con la distribución automatizada de parches.

DESPLIEGUE REMOTO DE SOFTWARE

Despliegue central de software a las máquinas del cliente, incluso en sucursales.

CONTROL DE ADMISIÓN A LA RED (NAC)

Con el Control de Admisión a la Red (NAC), se puede crear una política de red para "invitados". Los dispositivos de invitados (incluyendo los dispositivos móviles) se reconocen automáticamente y se envían a un portal corporativo en donde la contraseña de identificación correcta les permite utilizar los recursos que se les aprueban.

DESPLIEGUE DE IMAGEN DE APLICACIÓN Y SISTEMA OPERATIVO

Fácil creación, almacenamiento y despliegue de las imágenes del sistema desde una ubicación central. Perfecto para la migración a Microsoft® Windows® 8.

MANEJO DE HARDWARE, SOFTWARE Y LICENCIAS

Los reportes del inventario de hardware y software ayudan a mantener control sobre las obligaciones de licencia. De esta manera se pueden ahorrar costos al aprovisionar centralmente los derechos de software.

No todas las características se encuentran disponibles para todas las plataformas.

Para más información, favor consultar www.kaspersky.com

SEGURIDAD DE CORREO, COLABORACIÓN Y WEB:

PROTECCIÓN DEL SERVIDOR DE CORREO

Protege el correo en las últimas versiones de las principales plataformas de correo y colaboración: Servidores de correo basados en Microsoft® Exchange, IBM®, Lotus® Domino® y Linux®.

SEGURIDAD PARA GATEWAYS DE INTERNET

Garantiza acceso seguro a Internet en toda la organización al retirar automáticamente los programas maliciosos y potencialmente hostiles en tráfico HTTP(S) / FTP / SMTP y POP3.

ELIMINACIÓN VIRTUAL DEL SPAM

Al utilizar la tecnología Kaspersky basada en la nube, se aplican actualizaciones de inmediato, reduciendo la posibilidad de un ataque masivo de spam. Los correos electrónicos sospechosos se mantienen y verifican de nuevo, lo cual aumenta la tasa de captura y reduce los falsos positivos.

SEGURIDAD DE COLABORACIÓN

Kaspersky defiende a sus servidores de SharePoint® contra el malware, mientras que la capacidad de contenido y archivo ayudan a evitar el almacenamiento de contenido inadecuado.

CONTROLES DE ENDPOINT:

CONTROL DE APLICACIONES

Posibilita que los administradores de TI fijen políticas que permiten, bloquean o regulan aplicaciones (o categorías de aplicaciones).

CONTROL DE DISPOSITIVOS

Permite a los usuarios fijar, programar y aplicar políticas de datos con almacenamiento removible y otros controles de dispositivos periféricos conectados por USB o cualquier otro tipo de bus.

CONTROL WEB

Significa que los controles de navegación basados en el endpoint siguen al usuario, ya sea en la red corporativa o mientras se encuentra en roaming.

LISTA BLANCA DINÁMICA

Informes producidos por Kaspersky Security Network en tiempo real sobre la reputación de los archivos aseguran que sus aplicaciones aprobadas se encuentren libres de malware y ayudan a maximizar la productividad del usuario.

ENCRIPCIÓN Y PROTECCIÓN DE DATOS:

ENCRIPCIÓN INTEGRAL

Escoja entre nivel de disco completo o archivo, con el respaldo del Estándar de Encriptación Avanzado (AES) con encriptación de 256 bits para asegurar la información crítica del negocio en caso de robo o pérdida del dispositivo.

SOPORTE PARA DISPOSITIVOS REMOVIBLES

Aumenta su seguridad a través de políticas que aplican la encriptación de datos en los dispositivos removibles.

INTERCAMBIO SEGURO DE DATOS

Significa que los usuarios pueden fácilmente crear paquetes encriptados y de autoextracción para garantizar que los datos se protejan cuando se compartan mediante dispositivos removibles, correo electrónico, red o web.

TRANSPARENCIA PARA LOS USUARIOS FINALES

La solución de encriptación de Kaspersky es transparente e invisible para los usuarios y no tiene impacto adverso en la productividad. No hay impacto tampoco en las configuraciones o actualizaciones de las aplicaciones.