Kaspersky for Business

KASPERSKY lab

Protección de endpoints de última generación

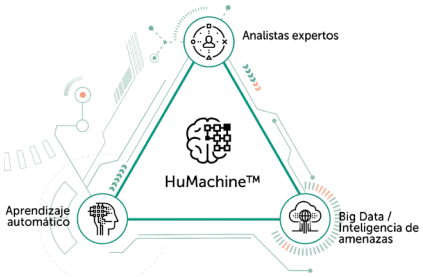
www.kaspersky.com/business
#truecybersecurity

Kaspersky®
Endpoint Security
for Business

Protección como parte de su estrategia de continuidad del negocio

La tecnología es una fuerza transformadora para las empresas. Hay que estar al día para no estancarse. Sin embargo, la tecnología también abre las puertas a los delincuentes y es el endpoint el objetivo principal y el origen de la mayoría de los problemas. Solo en el último año, más del 38 % de las empresas han sufrido un ciberataque, mientras que el 39 % de los ataques dirigidos a endpoints protegidos han tenido éxito. Con este panorama, las empresas deben ser más inteligentes que los ciberdelincuentes que los atacan.

Mientras hay seres humanos detrás de los ciberataques, será necesario que el intelecto humano se asocie con tecnologías innovadoras para luchar contra ellos. La protección de Kaspersky Lab se basa en nuestra inteligencia global de amenazas junto con algoritmos de aprendizaje automático, alimentado por la experiencia humana de los mejores especialistas del sector. Conocemos a esta combinación única como HuMachine™ y está en el ADN de nuestro productos.



En 2017, Kaspersky Lab recibió el galardón **Premios Gartner Peer Insights Customer Choice 2017** por su plataforma de protección endpoint. El premio es la máxima distinción posible en el competitivo mercado de plataformas de protección de endpoints. Nuestras aplicaciones de endpoints han logrado el porcentaje más alto (90 %) de los tres primeros puestos en pruebas independientes en comparación con cualquier otro proveedor.

Invierta en el futuro

El impacto financiero medio de un solo robo de datos en pequeñas o medianas empresas es de 86 500 USD, mientras que para corporaciones más grandes alcanza los 992 000 USD. Un antivirus de última generación ya no es suficiente: solo una solución multidimensional que ofrezca seguridad en varios niveles tecnológicos y funcionales de la infraestructura de IT corporativa puede proporcionar la protección que necesita. La seguridad de endpoints combina una variedad de técnicas y tecnologías inteligentes para proteger a las empresas contra cualquier tipo de ciberamenaza, en cualquier plataforma. Si puede proteger toda su red de IT, puede garantizar la continuidad de su empresa.

Proteja aquello que más valor tiene con aplicaciones basadas en HuMachine™

Es posible que su presupuesto de seguridad de IT no crezca al mismo ritmo que lo hace su empresa. Los recursos deben optimizarse para dar respuesta a los retos actuales y futuros.
Kaspersky Endpoint Security for Business ofrece protección contra el ransomware, los exploits y las ciberamenazas más avanzadas aprovechando la inteligencia de HuMachine™. Con optimización de recursos, incluye potentes controles de seguridad, vulnerabilidad y gestión de parches automatizadas, cifrado integrado y que puede controlarse desde una única consola en la red corporativa.

Seguridad adaptable y ágil

El producto está diseñado para poder utilizarse en cualquier entorno de IT. Emplea una pila completa de tecnologías probadas y de última generación. Los sensores integrados y la integración con detección y respuesta en endpoints (EDR) permiten la captura y el análisis de grandes volúmenes de datos para garantizar la detección de los ciberataques más oscuros y sofisticados.

Seguridad orientada al futuro para IT externalizado

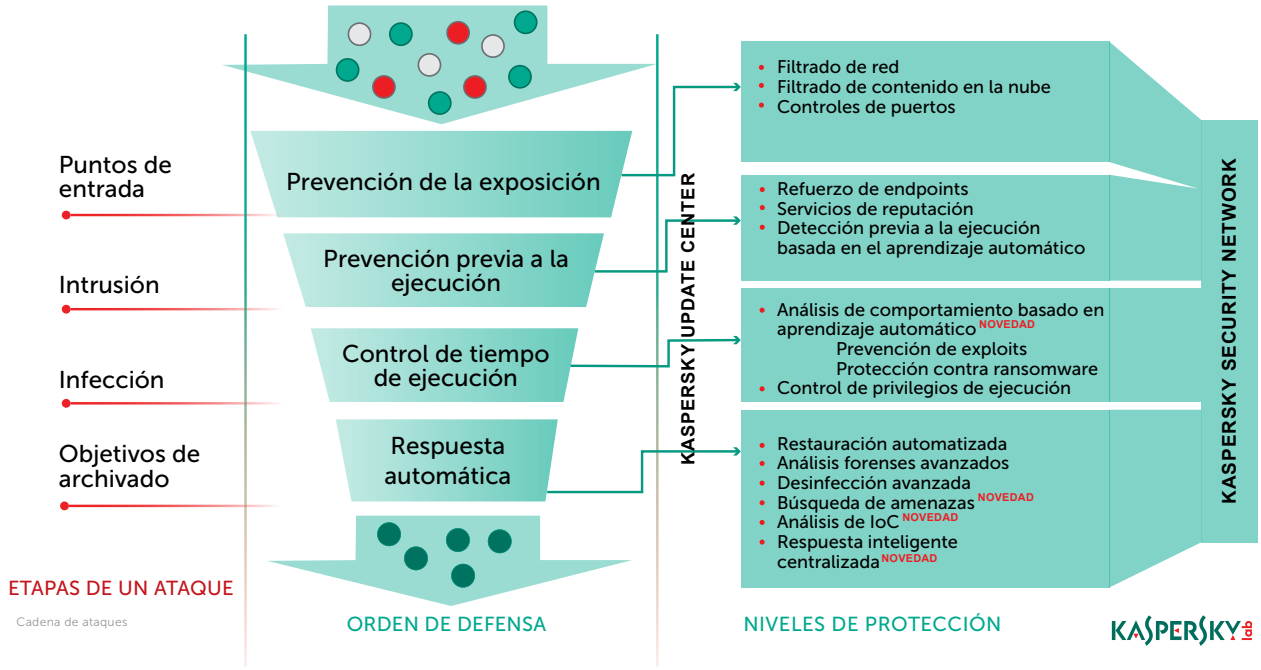
La arquitectura multiempresa, junto con la prevención de amenazas, la seguridad móvil, el cifrado de datos y la gestión de vulnerabilidades y parches permiten a los proveedores de servicios gestionados (MSP) agregar seguridad de IT a sus ofertas.

Bajo consumo de recursos, pero un gran rendimiento

Nuestra solución de seguridad más probada y galardonada basada en HuMachine ofrece una protección óptima con el mínimo impacto en los recursos del equipo. Los componentes sin firma garantizan que las amenazas se detecten incluso sin actualizaciones frecuentes.

Protección integral

Kaspersky Endpoint Security for Business utiliza varias tecnologías de última generación (como el refuerzo de la seguridad de los endpoints, el análisis del comportamiento basado en el aprendizaje automático, la prevención de exploits, etc.) para neutralizar la mayoría de amenazas antes de que a lleguen las capas de protección avanzada. Los archivos sospechosos que llegan hasta el endpoint se detectan y bloquean.



Esta combinación de tecnologías avanzadas con nuestro enfoque de varios niveles consigue el equilibrio perfecto entre rendimiento y una protección eficiente. Desempeña un rol fundamental en conseguir uno de los índices de detección más altos del sector, como demuestran continuamente las pruebas independientes.

Varias capas de protección para

- Windows, Linux o Mac
- Android y otros dispositivos móviles
- Medios de almacenamiento extraíbles
- Servidores de Windows y Linux
- Servidores de correo electrónico
- Pasarelas web
- Servidores de colaboración

Defensa sin precedentes contra

- Exploits de software
- Ransomware
- Malware móvil
- Amenazas desconocidas
- Amenazas sin archivos
- PowerShell y otros ataques basados en scripts
- Amenazas web
- Amenazas distribuidas por correo electrónico
- Ataques de phishing
- Spam

Protección antiransomware y antiexploit

Nuestras tecnologías siguen evolucionando, sobre la base de inteligencia de amenazas en tiempo real y aprendizaje automático. Proteja los endpoints contra las últimas exploits y mantenga sus datos y carpetas compartidas protegidos y a salvo de amenazas avanzadas y ransomware.

Bloquee las apropiaciones de cuentas

La detección del comportamiento implementa un mecanismo de protección de memoria, que protege los procesos críticos del sistema y evita las fugas de las credenciales de usuarios y administradores.

Reduzca su exposición a los ataques a través de las aplicaciones

Las funciones de marcado dinámico en lista blanca y control de aplicaciones le permiten reducir significativamente su exposición a los ataques de día cero, ya que proporcionan un control total sobre el software que se puede ejecutar en equipos de escritorio y servidores. El control de aplicaciones intercepta el inicio de archivos ejecutables, DLL y scripts de controles ejecutados por distintos intérpretes. La detección del comportamiento y la prevención de exploits supervisan el comportamiento de la aplicación, bloquean la posible actividad maliciosa y protegen a las aplicaciones legítimas para que el malware no pueda explotarlas ni utilizarlas. Las aplicaciones aprobadas y de confianza siguen ejecutándose sin problemas.

Neutralice el rootkit

Los atacantes utilizan rootkits y bootkits para ocultar sus actividades a las soluciones de seguridad. La tecnología anti-rootkit, parte de la protección de última generación a varios niveles de Kaspersky Lab ayuda a detectar incluso la infección más recóndita y la neutraliza.

Detecte más ataques e intrusiones, incluso las más oscuras

Los sensores integrados y la integración con Kaspersky Endpoint Detection and Response permiten la captura y el análisis de grandes volúmenes de datos sin que la productividad del usuario se vea afectada. Ofrece búsqueda avanzada de amenazas para pruebas de intrusiones, como indicadores de compromiso.

Evite la exposición a través de la red

El malware que utiliza un ataque de desbordamiento del búfer puede modificar un proceso ya ejecutándose en la memoria y ejecutar así el código malintencionado. La función de protección contra amenazas de red identifica ataques y exploits de red y los detiene en seco.

Mantenimiento y asistencia

Con operaciones en más de 200 países y 35 oficinas en todo el mundo, nuestro compromiso ininterrumpido con el soporte global se refleja en nuestros paquetes de soporte de acuerdos de servicio de mantenimiento (MSA). Nuestros equipos de Professional Services están preparados para asegurarse de que pueda sacar el máximo provecho de su solución Kaspersky Lab, para lo que le ofrecen ayuda con la implementación así como apoyo durante incidentes críticos.

Prueba gratuita

Descubra por qué solo True Cybersecurity combina la facilidad de uso con la inteligencia de **HuMachine™** para proteger su empresa frente a todo tipo de amenazas. Visite la página y obtenga una prueba gratuita de 30 días de la versión completa de **Kaspersky Endpoint Security for Business**. Al final del periodo de prueba, si decide comprar, solo tendrá que pagar las cuotas de licencia. Como la aplicación ya se ha estado ejecutando en los endpoints durante la prueba, no tendrá que hacer nada más.

Más allá de la protección de endpoints: ahora y en el futuro

Simplifique el inventario y la aplicación de parches

Detectar los detalles del inventario de hardware y software y gestionar la aplicación de parches de vulnerabilidades en el momento necesario es un proceso tedioso y que requiere mucho tiempo. Explotar las vulnerabilidades sin parches aplicados es una de las maneras más habituales que utilizan los cibercriminales para atacan la infraestructura de IT a través de un solo endpoint. Al ir más allá de la simple implementación remota del nuevo software de terceros, la evaluación de vulnerabilidades y la gestión de parches automatizadas, basadas en inteligencia continua de las vulnerabilidades aprovechadas, permiten mantener el software potencialmente vulnerable actualizado y que los administradores de IT puedan ahorrar tiempo que podrán dedicar a otras tareas.

Intercambio de datos seguro mediante cifrado

El cifrado con certificación FIPS 140-2 transparente para el usuario protege completamente los datos confidenciales en dispositivos portátiles y on site. La tecnología integrada significa que se puede aplicar de forma centralizada el cifrado de datos corporativos en el nivel de archivo, disco o dispositivo y permitir un intercambio seguro de datos a través de la red.

Soporte\ de escenarios remotos y móviles

Se puede acceder, en cualquier momento, a los datos que se mueven libremente por todo el perímetro. La seguridad móvil protege contra amenazas dirigidas específicamente a los datos en movilidad, así como intentos de utilizar las debilidades de los dispositivos como trampolín para una infiltración posterior en la infraestructura. El control de dispositivos protege contra las consecuencias de la pérdida de datos en dispositivos portátiles sin cifrar o no aprobados, y contra la carga de datos infectados desde los dispositivos.

Optimice la eficiencia con la gestión de todas las plataformas.

Una única consola le ofrece una visibilidad completa y un control sobre todas las estaciones de trabajo, servidores y dispositivos móviles, independientemente de la ubicación donde se encuentren y las acciones que estén realizando. La solución, que se puede escalar casi sin límites, proporciona acceso a licencias, solución de problemas remota y controles de red. La gestión centralizada se complementa con la integración de Active Directory, el modelo basado en roles y los paneles integrados.

Regule el acceso a datos confidenciales y dispositivos de grabación

Nuestra solución restringe los privilegios de las aplicaciones de acuerdo con los niveles de confianza asignados y limita el acceso a recursos como datos cifrados. En paralelo con bases de datos de reputación locales y en la nube (KSN), el sistema de prevención de intrusiones en el host (HISP) controla las aplicaciones y restringe el acceso a los recursos esenciales del sistema, y a los dispositivos de grabación de audio y vídeo.

Detenga las amenazas de la web antes de que lleguen a los endpoints

Al detener la mayoría de las amenazas entrantes al nivel de la pasarela, podemos reducir significativamente el impacto del factor humano y las características específicas de la seguridad de la estación de trabajo al no dejarlas llegar a los endpoints.

Una pasarela segura sigue siendo la primera línea de defensa para la mayoría de los escenarios de seguridad corporativa, a pesar de la incursión de la movilidad en los procesos de trabajo. Nuestras tecnologías de seguridad filtran el tráfico de las pasarelas y bloquean automáticamente las amenazas entrantes antes de que lleguen a los puntos finales y servidores. Esto reduce significativamente el riesgo de explotación de vulnerabilidades y reduce considerablemente la sobrecarga de trabajo para el personal de seguridad de IT.

Aumente la productividad y reduzca las amenazas

La tecnología antispam de próxima generación de Kaspersky, con asistencia en la nube, detecta incluso el spam más sofisticado y desconocido, y registra un nivel mínimo de falsos positivos. Al detenerlo, reducirá el tiempo empleado, los recursos y los riesgos derivados, con lo que ahorrará recursos humanos y del sistema. La protección incorpora varios niveles de seguridad proactiva, como el aprendizaje automático y la inteligencia contra amenazas basada en la nube, para filtrar archivos adjuntos maliciosos que puedan estar presente en correos electrónicos entrantes.

Permita la colaboración segura

Nuestra seguridad para Microsoft SharePoint® incluye antimalware, filtrado de contenido y filtrado de archivos para ayudar a que su empresa aplique sus políticas de colaboración e impida que se almacene contenido inadecuado en la red corporativa.

Kaspersky Endpoint Security for Business permite a los administradores supervisar, controlar y proteger su entorno de IT. La tecnologías y herramientas de última generación consiguen un equilibrio inteligente entre los niveles progresivos para responder a sus necesidades de IT y de seguridad cambiantes en todos los puntos de su viaje de negocios.

Kaspersky® Total Security for Business

Las empresas que tienen entornos de IT maduros, con una mezcla de sistemas nuevos y antiguos, necesitan ajustar su sistema de seguridad para los diferentes sistemas. Nuestra solución de seguridad para endpoints más completa, infraestructura y servidores de colaboración le permiten hacer exactamente eso para que pueda conseguir una seguridad rigurosa que puede adaptar a su entorno de IT.

Kaspersky® Endpoint Security for Business Advanced

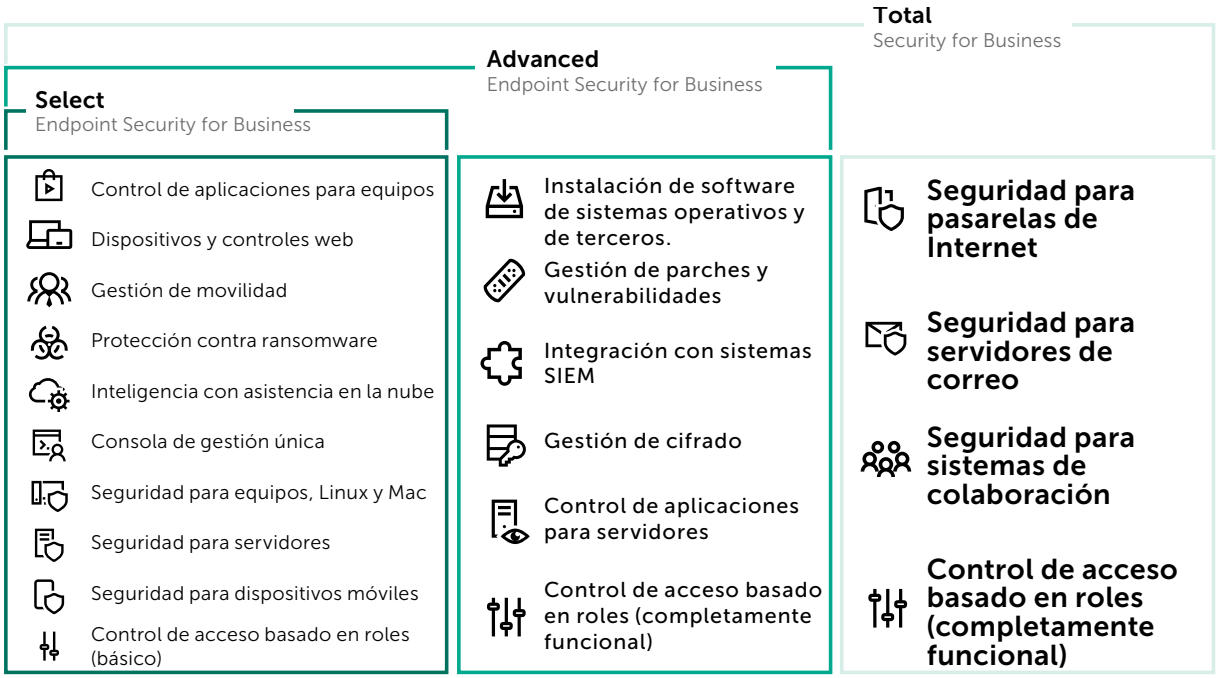
Para obtener una seguridad más eficaz para proteger su empresa, elija **Kaspersky Endpoint Security for Business Advanced**. Además de proteger todos sus endpoints y servidores, proporciona niveles adicionales de seguridad para proteger datos confidenciales y eliminar vulnerabilidades, además de ayudar a simplificar también las tareas de gestión de sistemas.

Kaspersky® Endpoint Security for Business Select

Dado el creciente número de operaciones comerciales que se realizan digitalmente, necesita proteger todos sus servidores, equipos portátiles y dispositivos móviles. Le proporcionamos seguridad de última generación con la que proteger todos los endpoints de su empresa, en una única solución y con una consola de gestión flexible.

¿Qué nivel de protección es el más adecuado para usted?

Cualesquiera que sean sus necesidades de IT, **Kaspersky Endpoint Security for Business** tiene la solución ideal para usted.



Mayor seguridad cuando la necesita

Automatizar y centralizar la detección de vulnerabilidades de software y la gestión de parches permite protegerse contra las amenazas más peligrosas, incluido el ransomware. Para los clientes de **Kaspersky Endpoint Security for Business Select**, esta automatización está disponible con el **complemento Kaspersky Vulnerability and Patch Management** .

Asimismo, para los clientes de Select, el **complemento Kaspersky Encryption** permite el cifrado de disco completo o de archivos, utilizando potentes algoritmos de cifrado y con soporte para el inicio de sesión único para permitir el acceso inmediato a archivos cifrados, así como mediante tarjetas smartcard o tokens para la autenticación de dos factores. Le permite cifrar archivos y carpetas que estén almacenados en unidades locales y extraíbles.

Para contar incluso con un nivel superior de seguridad sin ninguna complejidad adicional, basta con activar las funcionalidades necesarias desde Kaspersky Security Center.

¿Por qué actualizar su protección de endpoints actual?

Cuente siempre con las últimas tecnologías de forma rápida y fácil: un servidor, una consola, un único agente

Apoye cualquier proceso de negocio a través de una integración más profunda: una única base de código, creada de forma interna

Evite los costes ocultos y tener distintas licencias. Toda la funcionalidad que necesita en una compra única

Capacidad de control y auditoría mejorada; gestión unificada con el acceso basado en roles

En Kaspersky Lab, desarrollamos y perfeccionamos todas nuestras propias tecnologías de forma interna, lo que hace que todas nuestras aplicaciones sean más estables y eficientes. Nos hemos comprometido con nuestro propio programa de I+D e incorporamos numerosas innovaciones tecnológicas a nuestros productos. A continuación algunos ejemplos:

- Aprendizaje automático a varios niveles mediante el uso de métodos de aprendizaje, en diferentes etapas de la cadena de ataque en los endpoints y en la nube.
- Búsqueda activa de amenazas como resultado de la integración entre la protección de endpoints y las soluciones Endpoint Detection & Response o Anti Targeted Attack.
- El modo exclusivo en la nube para proteger los componentes ofrece la máxima protección con el mínimo impacto en los recursos del equipo y en el uso de ancho de banda de Internet.
- Soporte para contenedores de Microsoft Windows Server, gestión del tráfico externo y de los firewalls.
- Control de dispositivos mejorado y funcionalidad anticonexión.
- Control de aplicaciones mejorado con categoría de certificados de confianza y modo de prueba de las políticas.
- La nueva interfaz de usuario muestra la protección a varios niveles, mostrando el estado de la protección y la efectividad de las últimas tecnologías de Kaspersky Lab en acción.

True Cybersecurity: es parte de nuestro ADN

Kaspersky Lab ofrece potentes soluciones de ciberseguridad mediante la inteligencia de amenazas líder mundial que forma parte de nuestro ADN e influye en todo lo que hacemos. Como empresa independiente, somos mucho más eficientes, pensamos de forma diferente y actuamos más rápido.

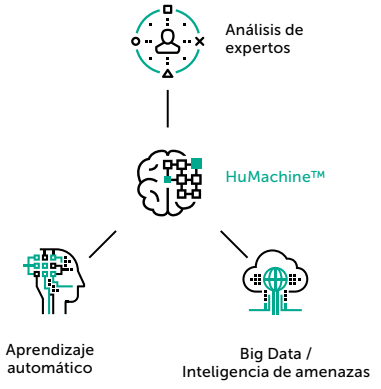
- **Nuestros conocimientos expertos se extienden desde los niveles superiores hasta los inferiores**, empezando por nuestro director ejecutivo, Eugene Kaspersky.
- **Nuestro equipo de análisis e investigación global (GReAT)**, un grupo de élite de expertos en seguridad ha descubierto muchas de las amenazas de malware y ataques dirigidos más peligrosos del mundo.
- Nuestra innovadora **iniciativa de transparencia global** es una prueba más de nuestro compromiso para proteger a los clientes de ciberamenazas, independientemente de su origen o su propósito.

Cumpla con el GDPR con True Cybersecurity

Kaspersky Lab da a conocer los aspectos relacionados con la ciberseguridad de GDPR. Nuestras soluciones ayudan a los clientes a reducir los riesgos de las fugas de datos y a prevenir incidentes de seguridad. También ayudamos a los responsables de protección de datos (DPO) de nuestros clientes a mejorar la visibilidad de la infraestructura supervisada.

Visión de conjunto: soluciones de seguridad de IT de Kaspersky para empresas

La protección de endpoints, aunque es fundamental, es solo el principio. Tanto si sigue una estrategia de seguridad de categoría superior como si trabaja con una sola fuente, Kaspersky Lab ofrece una amplia gama de productos que se entrelazan o trabajan de manera independiente, para que pueda elegir a su gusto sin sacrificar el rendimiento o la libertad de elección. Obtenga más información en nuestro sitio web.



Kaspersky Lab Iberia
Encuentre un partner próximo: **www.kaspersky.com/buyoffline**
Kaspersky for Business: **www.kaspersky.com/business**
True Cybersecurity: **www.kaspersky.es/true-cybersecurity**
Noticias de seguridad de IT: **www.business.kaspersky.com**

#truecybersecurity
#HuMachine

www.kaspersky.es

KESB_Product_Datasheet_Next_Generation_Endpoint_Protection_Customer_0218_ES_GLB