



Kaspersky Endpoint Security for Business

La tecnología es una fuerza transformadora para las empresas: siga el ritmo o se estancará. Pero la tecnología también abre las puertas a los delincuentes, y el endpoint es un objetivo principal. Por eso, debe ser más inteligente que los ciberdelincuentes que lo tienen en sus sitios, al implementar soluciones rigurosas y fiables para proteger lo que más valora su empresa.

Desafíos



Aumento de la presión de los ataques

Ahora, las herramientas de ciberseguridad son tan baratas que hay un crecimiento drástico de los eventos de seguridad y del riesgo. El ransomware, el spyware financiero, el phishing y otras amenazas pueden golpear a su organización con graves pérdidas, especialmente si está en plena transformación digital.



Una infraestructura heterogénea para proteger

La proliferación del trabajo remoto, los servicios en la nube y los procesos ágiles hacen que toda la estrategia de seguridad deba cubrir la gama completa de dispositivos de endpoint, incluidos las computadoras portátiles, las estaciones de trabajo, los servidores y los dispositivos móviles, incluso los dispositivos personales utilizados para el trabajo. También tiene que pensar en los distintos sistemas operativos que admite.



Altos niveles de complejidad a los que enfrentarse

Tener una infraestructura informática compleja, y los conocimientos necesarios para apoyarla y protegerla, todo esto tiene un costo. Debe invertir eficazmente en las soluciones adecuadas para satisfacer los cambiantes requisitos de seguridad de su empresa, en términos de tiempo, presupuesto, personal y competencias específicas.

Solución



Seguridad adaptable ágil

Tiene que ser capaz de lo siguiente:

- Proteger completamente sus datos, empleados e infraestructura, sin que esto afecte al rendimiento.
- Confiar en la inteligencia de amenazas más reciente y fiable para detectar y contrarrestar las amenazas nuevas y emergentes que se dirigen hacia usted.
- Reconocer los patrones de comportamiento de las amenazas, para poder neutralizar incluso las amenazas desconocidas.
- Reducir su superficie de ataque al controlar qué aplicaciones, sitios web y dispositivos pueden interactuar con sus endpoints y usuarios.



Una solución única para cualquier plataforma

Estará buscando lo siguiente:

- La mejor seguridad posible para cada estación de trabajo, servidor y dispositivo móvil que transporta sus datos, independientemente de dónde se encuentren y de si son o no de su propiedad. Piense también en los puntos de entrada de las amenazas y en cómo proteger las puertas de enlace de la web y el correo electrónico sin darle más trabajo a su equipo.
- La seguridad de que puede cubrir todos los sistemas operativos de su entorno mixto, incluidos Windows, Mac, Linux, iOS y Android, con una única solución, trabajando desde una única consola.



Gestión flexible y automatización de tareas

Y querrá maximizar sus recursos con los siguientes:

- Altos niveles de automatización, sobre todo en tareas esenciales pero rutinarias, como la aplicación de parches y la implementación del sistema operativo. El tiempo y la experiencia de su equipo son demasiado valiosos como para desperdiciarlos.
- Capacidades de gestión remota: ya sea para configurar estaciones de trabajo en oficinas domésticas o para proteger los datos con opciones de cifrado.
- Centralización. No hay que andar esquivando entre consolas: necesita una gestión directa e integrada en una sola pantalla, en su perímetro o en la nube.

Costo de las vulneraciones de datos

USD 105 000 para las pymes
USD 927 000 para las empresas

USD 101 000 ▲ USD 105 000
 2020 2021
 USD 1,09 millones ▼ USD 927 000
 2020 2021

Fuente: Kaspersky IT Security Economics 2021

Tres paquetes de funciones progresivas

Las herramientas y las tecnologías de Kaspersky Endpoint Security for Business están equilibradas de manera inteligente entre todos los niveles progresivos, a fin de satisfacer las necesidades cambiantes de seguridad y TI a medida que su empresa crece.

<ul style="list-style-type: none"> Protección contra las amenazas web, de archivos, de red y de correo electrónico Protección para estaciones de trabajo, servidores y dispositivos móviles Detección del comportamiento Ransomware, prevención y reparación de exploits Acceso a Kaspersky Security Network (KSN) Consola de gestión en la nube o en las instalaciones Estaciones de trabajo de control de las aplicaciones Control web y de dispositivos Borrado de datos a distancia Evaluación de vulnerabilidades Administración de dispositivos móviles Exportación de eventos a través de Syslog Integración de EDR y sandbox en la nube 	Select Endpoint Security for Business
<ul style="list-style-type: none"> Control de acceso basado en funciones Control de aplicaciones para servidores Administración de parches Control adaptable de anomalías Gestión del cifrado (a nivel de archivo, disco y dispositivo) Inventario de HW y SW Instalación de sistemas operativos y de terceros Exportación automática a SIEM (compatible con CEF y LEFF) 	Advanced Endpoint Security for Business
<ul style="list-style-type: none"> Protege el correo electrónico y el tráfico web a nivel de pasarela Características antiphishing avanzadas Filtro por reputación y detección de direcciones maliciosas Antispam y filtrado de contenidos Detección de correo electrónico empresarial comprometido (BEC) Protección para los servicios de Microsoft Office 365 	Total Security For Business

Amenazas de ransomware

Estos ataques se han llevado a cabo contra individuos o empresas, y algunos de los más notables de los últimos años han afectado a grandes marcas.

El 88 % de los ejecutivos de las empresas que han sido atacadas anteriormente por ransomware dijeron que pagarían si fueran atacadas de nuevo.

El ransomware es un problema creciente para las empresas de todo el mundo, ya que el número de ataques de ransomware casi se duplicó solo en 2021. Esto puede atribuirse en parte a la pandemia, que hizo que más personas trabajaran desde sus hogares. Pero con un modelo de trabajo híbrido que parece que llegó para quedarse, la probabilidad de un ataque de ransomware sigue presente.

Lo que ofrecemos para usted

- Verdadera seguridad. Protegemos completamente todos sus endpoints contra las amenazas generalizadas y emergentes, gracias al rendimiento inigualable de las tecnologías de Kaspersky, como la **protección contra ataques sin archivos**, el análisis de comportamiento **basado en ML** y la protección específica contra exploits, ransomware y spyware financiero.
- Protección proactiva. Detenemos los ataques antes de que empiecen. La protección previa a la ejecución mediante **control adaptativo de anomalías** combina la sencillez de las reglas de bloqueo con la inteligencia del ajuste automático, basado en el análisis del comportamiento.
- Un ecosistema completo para su creciente madurez de seguridad de TI. La respuesta y el análisis automatizados aprovechan las **integraciones** con las soluciones **EDR** y **SIEM**.
- Valor para el usuario respecto al costo. Nuestro enfoque escalonado significa que usted paga solo por las capacidades que necesita en este momento.
- A prueba del futuro. La actualización es perfecta: solo hay que moverse a través de los niveles. Nuestra solución totalmente escalable está preparada para soportar **miles de dispositivos gestionados** a medida que su empresa crece.
- **Adopción agilizada de la nube**. Con protección avanzada para los servicios de **Microsoft Office 365**
- Flexibilidad. **Elija su opción de implementación preferida**: en la nube, en las instalaciones, en un espacio de aire y en implementaciones híbridas. A continuación, asigne diferentes niveles de acceso a los sistemas de seguridad a los distintos miembros del equipo con un control de acceso granular basado en funciones (**RBAC**).
- Tranquilidad. Todos sus datos confidenciales están totalmente protegidos, con un **conjunto de funcionalidades de protección de datos** que incluye la gestión del cifrado a nivel de archivo y de disco completo, y en dispositivos externos. El borrado remoto de datos erradica los datos en caso de pérdida o robo de un dispositivo.
- Defensas perimetrales. **Evitan que los ataques basados en la web y el correo electrónico** alcancen sus objetivos principales: los empleados y sus endpoints



La seguridad más galardonada... y la que nuestros clientes aprecian.

Entre 2013 y 2021, los productos de Kaspersky fueron parte de 741 pruebas y revisiones independientes. Nuestros productos obtuvieron el primer lugar en 518 ocasiones. Consulte más información en www.kaspersky.com/top3

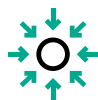
Casos de uso



Defienda sus sistemas automáticamente

La detección basada en el comportamiento es parte del enfoque de protección multicapa y de última generación de Kaspersky. Es una de las maneras más eficientes de protegerse contra amenazas avanzadas como los malware que no utilizan archivos, los ransomware y los malware de día cero.

El uso de datos de Kaspersky Security Network garantiza una respuesta más rápida a las nuevas amenazas, mejora el rendimiento de los componentes de protección y reduce la probabilidad de falsos positivos. A fin de cuentas, los índices de detección superiores y la seguridad adaptativa incorporada se traducen en una respuesta rápida a los ataques con un mínimo de falsos positivos. Kaspersky es el único proveedor de ciberseguridad que logró una tasa de protección contra el ransomware del 100 % en un estudio reciente de AV-Test. [Protección avanzada de endpoints de AV-Test: Prueba de protección contra el ransomware](#), AV-Test, 30 de septiembre de 2021



Reduzca su superficie de ataque

Alinee los dispositivos remotos con la seguridad informática de su empresa. Los controles de las aplicaciones afectan tanto a la productividad (al restringir el acceso a las aplicaciones de juegos o a las redes sociales, por ejemplo), como a la seguridad. Los empleados pueden ser víctimas de phishing y malware en aplicaciones crackeadas y sitios web dudosos, mientras que el simple hecho de conectar un módem USB o una impresora de red puede dar lugar a una fuga de datos confidenciales. Todos estos vectores de ataque, además del riesgo derivado de los errores humanos, pueden reducirse significativamente mediante la aplicación de controles granulares en las aplicaciones, la web y los dispositivos.

El Control Adaptativo de Anomalías significa que puede reforzar las políticas comunes y ver cómo el sistema aplicará las reglas, basándose en el comportamiento de los usuarios.



Minimice el tiempo, el esfuerzo y los costos

Gestione Kaspersky Endpoint Security for Business desde la consola en la nube.

Este enfoque basado en SaaS no requiere inversión en hardware y le permite centrarse en las iniciativas empresariales en lugar de dedicar tiempo a las actualizaciones, el soporte y la disponibilidad: nuestra infraestructura en la nube se encarga de todo.

Y piense en el tiempo que su equipo dedica al fortalecimiento de los endpoints, a la gestión remota de dispositivos, a la implementación del sistema operativo y a la gestión de parches y cifrado. Kaspersky Endpoint Security agiliza y automatiza todas estas tareas y más, y proporciona una única solución y una interfaz web para gestionar todo. Se acabaron las consolas separadas o los productos diferentes para cada tarea o tipo de dispositivo.



Construya una postura de protección de datos sólida

Los ataques actuales utilizan herramientas y aplicaciones legítimas que permiten a los actores de las amenazas encontrar nuevas vulnerabilidades y exploits de día cero en aplicaciones comunes. La gestión automatizada de parches reduce significativamente el riesgo de estos ataques para sus datos, mientras que el cifrado de datos garantiza que solo los usuarios legítimos puedan acceder a determinados archivos sensibles o dispositivos externos. El cifrado completo del disco duro también protege los datos en caso de pérdida o robo del dispositivo.

La integración disponible en Kaspersky Total Security for Business también protege la colaboración y el intercambio de archivos de Microsoft Office 365, y ayuda a evitar la fuga de información de identificación personal (PII).

EXPERIMÉNTALO USTED MISMO

¿Por qué no experimenta usted mismo nuestra protección adaptativa? Visite [esta página](#) para obtener una versión de prueba gratis durante 30 días de Kaspersky Endpoint Security for Business.



Un enfoque por etapas

Crear una base de seguridad para su organización mediante la elección del producto o servicio adecuado es solo el primer paso. Desarrollar una estrategia de ciberseguridad corporativa con visión de futuro es clave para el éxito a largo plazo.

Nuestra cartera refleja las demandas de seguridad de las empresas actuales, y responde a sus necesidades corporativas sea cual sea el tamaño de su organización o su nivel de madurez en materia de seguridad informática, mediante un enfoque único por etapas.

Este enfoque combina distintas capas de protección contra todos los tipos de amenazas cibernéticas y ayuda a evitar las amenazas de forma automática; luego, lo potencia de forma metódica y sistemática para que agregue nuevas capacidades avanzadas a fin de contrarrestar amenazas más sofisticadas a medida que la empresa se desarrolla. Vemos el panorama completo, para que usted pueda centrarse sin miedo en la innovación.



Kaspersky Security Foundations



Kaspersky Endpoint Security for Business



Kaspersky Security for Mail Server



Kaspersky Hybrid Cloud Security



Kaspersky Security for Internet Gateway



Kaspersky Embedded System Security



Kaspersky Professional Services



Kaspersky Security for Storage



Kaspersky Premium Support and Professional Services

- Protección para usuarios corporativos y dispositivos móviles
- Protección de servidores para entornos híbridos
- Protección para escritorios virtuales (VDI)
- Protección de endpoints especializados y PC heredadas
- Protección frente al vector de ataque más habitual: correo electrónico
- Protección de vanguardia frente a amenazas basadas en la web
- Asistencia durante la implementación, configuración y mantenimiento

Aproveche todo el potencial del ecosistema de Kaspersky



Kaspersky Security Foundations

Nuestra etapa de prevención de amenazas administrada en la nube permite que todas las organizaciones detengan las ciberamenazas genéricas de forma automática en cualquier dispositivo, VDI e infraestructura de servidor híbrido.

- Protege todos los dispositivos, incluidos los endpoints especializados y heredados
- Proporciona visibilidad y control sobre todos los activos de TI
- Ayuda a evitar o mitigar los errores de los usuarios
- Proporciona la automatización de administración de sistemas que necesita, sin gastar todo su dinero



Kaspersky Optimum Security

Ayuda a proteger las empresas de las amenazas nuevas, desconocidas y evasivas. Solución eficaz de detección y respuesta a las amenazas, con pocos recursos. Supervisión de seguridad 24/7, búsqueda automatizada de amenazas y respuestas guiadas y gestionadas con el apoyo de los expertos de Kaspersky.

- Actualiza la protección de endpoints contra amenazas evasivas
- Apoya el desarrollo de procesos esenciales de respuesta ante incidentes
- Optimiza el uso de recursos de ciberseguridad



Kaspersky Expert Security

Diseñado para satisfacer las necesidades cotidianas de cualquier empresa con seguridad de TI desarrollada en el momento de lidiar con las amenazas actuales más sofisticadas, incluidas las APT (amenazas persistentes avanzadas) y los ataques selectivos.

- Optimiza las cargas de trabajo de los expertos
- Mejora el conocimiento y las habilidades
- Respaldar a los expertos

Noticias sobre ciberamenazas:

www.securelist.com

Noticias de seguridad de TI:

business.kaspersky.com

Seguridad de IT para pymes:

kaspersky.com/business

Seguridad de IT para grandes empresas:

kaspersky.es/enterprise-security

latam.kaspersky.com

© 2022 AO Kaspersky Lab. Las marcas comerciales y de servicios registradas son propiedad de sus respectivos propietarios.



Hemos pasado pruebas. Somos independientes. Somos transparentes. Tenemos el compromiso de crear un mundo más seguro, en el que la tecnología mejore nuestras vidas. Por eso la protegemos, para que todas las personas del mundo puedan beneficiarse de las oportunidades que brinda la tecnología. Proteja su futuro gracias a la ciberseguridad.

Obtenga más información en

latam.kaspersky.com/about/transparency



**Proven.
Transparent.
Independent.**