KASPERSKY ENDPOINT SECURITY FOR ENTERPRISE

Protección de última generación contra amenazas avanzadas dirigidas a sus endpoints y usuarios

El entorno de las amenazas avanza de manera exponencial, lo que supone un riesgo cada vez mayor ante ataques de día cero para los procesos empresariales de especial importancia, datos confidenciales y recursos económicos. A fin de mitigar el riesgo para su organización, debe ser más inteligente, estar mejor equipado y contar con mayor información que los ciberprofesionales que le están atacando.

Sin embargo, nos encontramos ante un hecho indiscutible: la mayoría de los ciberataques contra empresas se inician a través del endpoint. Si puede proteger de manera eficaz todos los endpoints corporativos, tanto fijos como móviles, dispondrá de una sólida base para su estrategia de seguridad global.

POTENTE SEGURIDAD

La total protección de todos los endpoints contra todo tipo de ciberamenazas conocidas y desconocidas es una tarea de gran envergadura. La protección antivirus tradicional no es en absoluto suficiente. Solo mediante el uso de una plataforma de seguridad de vanguardia y la adopción de un enfoque a varios niveles se puede esperar proteger completamente cada endpoint dentro y fuera del perímetro.

POTENTE RENDIMIENTO

La protección de endpoints debería ser algo tan natural e inconsciente como respirar. La exclusiva plataforma de seguridad integrada de Kaspersky Lab late continuamente en el corazón de su infraestructura de IT y aplica una potente protección de endpoints con un impacto mínimo en la velocidad o los recursos. Creada internamente como plataforma integrada única y totalmente escalable, la solución proporciona un rendimiento óptimo sin conflictos de software y sin brechas de seguridad.

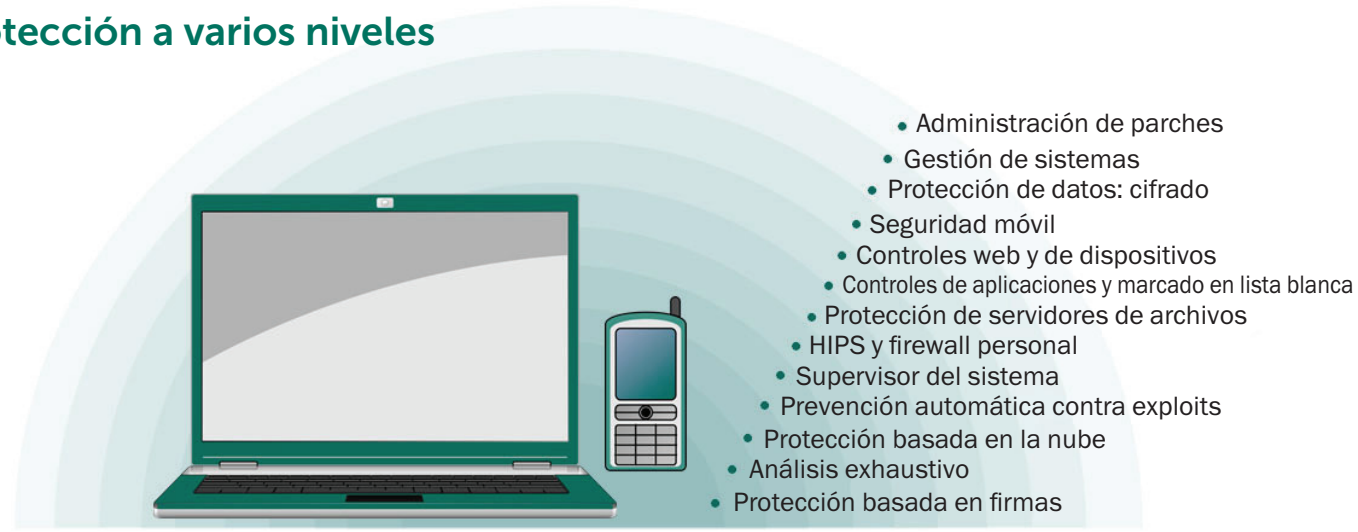
POTENTE INTELIGENCIA DE AMENAZAS

Basadas en fuentes inigualables de inteligencia de amenazas en tiempo real, nuestras tecnologías evolucionan continuamente para proteger a su empresa incluso frente a las amenazas más sofisticadas y recientes, incluidos los exploits de día cero. Mediante la alineación de su estrategia de seguridad con los líderes mundiales en detección de amenazas avanzadas, adoptará la mejor protección de endpoints, ahora y en el futuro. No hay mejor postura de seguridad para su empresa.

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.

Protección a varios niveles



Prevención y eliminación inigualables de amenazas de próxima generación

En el núcleo de su estrategia de seguridad se encuentra el motor de protección de endpoints más potente y eficaz del sector, tal como confirman continuamente pruebas independientes[1].

Los distintos niveles de protección inteligente y proactiva se entremezclan para proporcionar defensas potentes y resistentes contra las ciberamenazas más sofisticadas, conocidas, desconocidas y avanzadas.

- **Análisis heurístico** de varios algoritmos: detecta malware desconocido, complementando así las tecnologías tradicionales **basadas en firmas**.
- **Kaspersky Security Network (KSN) con asistencia en la nube:** facilita la identificación y el bloqueo de nuevas amenazas de malware en tiempo real, a medida que vayan surgiendo.
- **Prevención automática frente a exploits:** ayuda a detener de manera proactiva incluso las más avanzadas amenazas mediante el bloqueo de los exploits que utilizan los cibercriminales.
- **Supervisor del sistema:** bloquea amenazas desconocidas mediante la detección de patrones de comportamiento sospechoso y restaura archivos clave si el sistema se ve afectado.
- **Sistema de prevención de intrusiones basado en host (HIPS):** restringe las actividades y concede privilegios según el nivel de confianza del software.
- **Firewall personal:** restringe la actividad de la red.
- **Network Attack Blocker:** detiene los ataques basados en la red.
- **Servidores de archivos:** también están totalmente protegidos.

Cada endpoint bajo su control

Reduzca al mínimo la exposición de los endpoints a los posibles riesgos y aumente asimismo la productividad. Controle el acceso individual de los endpoints a las aplicaciones, los sitios web y los complementos: identifique y bloquee los accesos inapropiados, regule el acceso a elementos innecesarios y promueva los elementos valiosos y de confianza.

Todas las herramientas de control están integradas con Active Directory, y la creación y aplicación de políticas simplificadas, personalizables o automáticas pueden realizarse de manera centralizada o basada en roles, según sus preferencias.

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 del software que se permite ejecutar. Las aplicaciones incluidas en la lista negra se bloquean y las que se comportan de manera sospechosa o inapropiada se detectan, se analizan y, a continuación, se bloquean o restringen con ayuda del Supervisor del sistema e HIPS. Mientras, las aplicaciones aprobadas y de confianza siguen ejecutándose sin problemas.

MARCADO EN LISTA BLANCA FLEXIBLE BASADO EN LA NUBE

A través de nuestro propio laboratorio de marcado en lista blanca, admite un escenario de denegación predeterminada, que se puede ejecutar en un entorno de banco de pruebas.

VENZA LOS PELIGROS DE LA NAVEGACIÓN WEB

El **control web** supervisa, filtra y controla a qué sitios web pueden acceder los usuarios finales en el lugar de trabajo, lo que aumenta la productividad y reduce su vulnerabilidad a la penetración e infiltración en sus sistemas a través de sitios web y social media.

CONTROL DEL USO DE DISPOSITIVOS PORTÁTILES

El **control de dispositivos** protege contra las consecuencias perjudiciales de la pérdida de datos corporativos y de clientes en dispositivos portátiles sin cifrar o no aprobados, y contra la carga de datos infectados desde los dispositivos.

Protección de datos mediante el cifrado integrado

El potente **cifrado** transparente para los usuarios protege totalmente los datos delicados y confidenciales en movilidad, en dispositivos portátiles e in situ. La tecnología integrada significa que se puede aplicar de manera centralizada el cifrado de datos corporativos por archivo, disco o dispositivo mediante políticas de seguridad claras dirigidas a grupos de endpoints o incluso a dispositivos individuales.

1 Referencia: Top3.

Eliminación de vulnerabilidades mediante parches inteligentes

Una de las maneras más habituales de acceder a la infraestructura de IT a través de un solo endpoint consiste en usar exploits para las vulnerabilidades no protegidas de una aplicación de confianza. Para establecer prioridades y gestionar la oportuna y eficiente aplicación de parches a las vulnerabilidades se requiere una comprensión profunda de los exploits, sus comportamientos y sus objetivos actuales. El sistema de **análisis de vulnerabilidades y gestión de parches automático** de Kaspersky Lab, basado en inteligencia global en tiempo real sobre las actividades de los exploits, mantiene actualizados los parches críticos, sin que ello afecte a los sistemas y usuarios.

Protección de dispositivos móviles más allá de su perímetro

Actualmente, los datos corporativos son accesibles desde cualquier lugar, en cualquier momento, en smartphones y tablets que se mueven libremente por su perímetro de IT. **La seguridad de dispositivos móviles** protege frente a las amenazas dirigidas a los datos confidenciales en movilidad, así como frente a las que intentan utilizar los puntos débiles de la seguridad en los dispositivos corporativos o de los empleados como "punto de partida" para infiltrarse en los sistemas.

Funciones incluidas

- **Potente protección a varios niveles** contra las amenazas de malware para las principales plataformas móviles.
- Tecnología **antiphishing** que bloquea los enlaces peligrosos en mensajes y páginas web, y filtros de llamadas y SMS que impiden comunicaciones no deseadas.
- Al **envolverse las aplicaciones**, se puede aplicar una técnica de contenedorización, cifrado y borrado por separado a los datos corporativos en los dispositivos propiedad de los empleados.
- El **control de aplicaciones y el control web**, respaldados por KSN, bloquean el acceso no autorizado a software y sitios web.
- Las funciones **antirrobo**, que incluyen el borrado, el bloqueo del dispositivo, la localización, la vigilancia de la SIM, la foto de identificación y el envío de una alarma para detectar el dispositivo, permiten deshabilitar rápidamente los dispositivos y borrar los datos confidenciales cuando un dispositivo se extravía o es robado.
- Detección e informes de **dispositivos liberados**, para poder tomar medidas.
- **Gestión centralizada**, incluida la gestión de dispositivos móviles y aplicaciones (MDM/MAM). Las políticas pueden implementarse en dispositivos heterogéneos en las principales plataformas desde una sola interfaz.

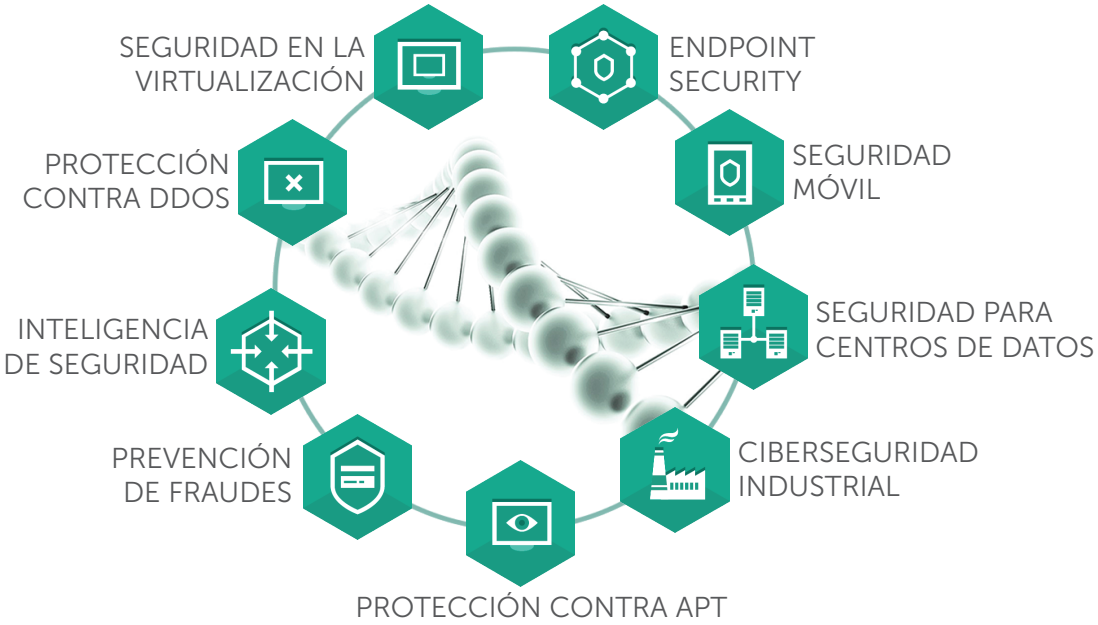
Eficiencia optimizada y gestión integrada

Kaspersky Endpoint Security for Enterprise proporciona a los equipos de seguridad total visibilidad y control de todos los endpoints, tanto fijos como móviles, bajo su jurisdicción, con independencia de su ubicación y sus actividades. Con una escalabilidad casi infinita, la solución proporciona acceso a los inventarios, las licencias, la solución de problemas remota y los controles de red desde una sola consola, **Kaspersky Security Center**.

La gestión centralizada desde una sola consola se complementa con funcionalidad de gestión basada en roles a fin de asignar las responsabilidades y los derechos de acceso a los profesionales de seguridad individuales según sea necesario.

Visión de conjunto: soluciones de seguridad 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 soluciones para empresas** que se entrelazan o trabajan de manera independiente, para que pueda elegir a su gusto sin sacrificar el rendimiento o la libertad de elección. Las soluciones que abarcan **sistemas, servidores e infraestructuras tanto físicas** como **virtuales** se complementan con las dirigidas a **cuestiones específicas del sector**, como el fraude financiero y los ataques denegación del servicio (DDoS) y por nuestra gama de **Security Intelligence Services**.



Mantenimiento y asistencia

Con operaciones en más de 200 países y 34 oficinas en todo el mundo, nuestro compromiso ininterrumpido con la asistencia mundial se refleja en nuestros paquetes de asistencia 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 instalación de seguridad de Kaspersky Lab.

Para obtener más información sobre cómo proteger sus endpoints de manera más eficaz, póngase en contacto con el equipo de ventas para empresas de Kaspersky Lab.

Kaspersky Enterprise Security for Endpoints/V 1.0/Nov. 15/Global

© 2015 Kaspersky Lab. Todos los derechos reservados. Las marcas registradas y logos son propiedad de sus respectivos dueños. Microsoft, Windows Server y SharePoint son marcas comerciales o marcas comerciales registradas de Microsoft Corporation en Estados Unidos y en otros países.