Kaspersky Endpoint Security Cloud

Protección de endpoints para empresas ágiles

kaspersky

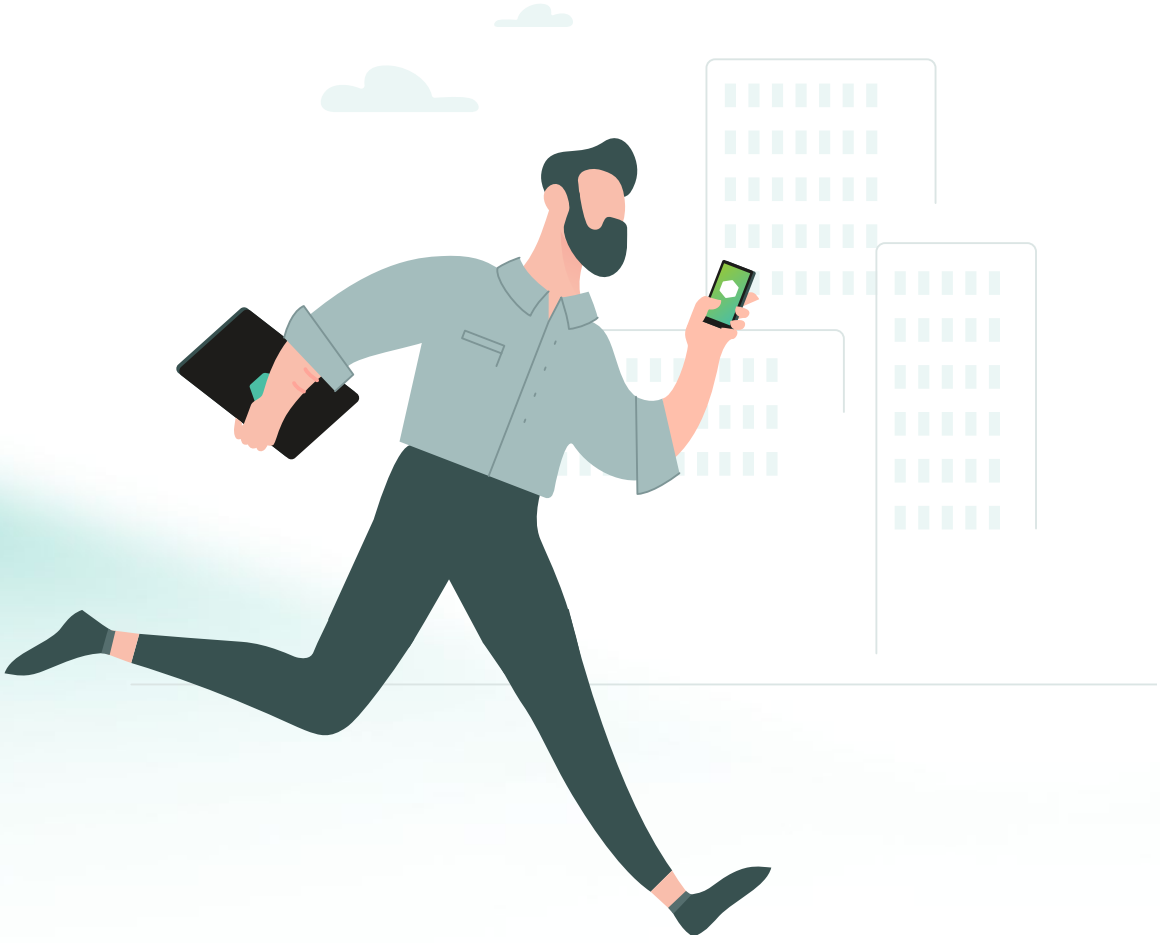
Agilidad en el día a día

Kaspersky Endpoint Security Cloud está diseñado para los negocios ágiles

Su negocio está creciendo. La cantidad de tareas de seguridad de TI con las que debe lidiar también sigue creciendo. Pero aún no está listo para contratar a un especialista en seguridad dedicado. Por eso, creamos **Kaspersky Endpoint Security Cloud Plus** para ayudar a administrar las tareas de seguridad de rutina con facilidad, y hacer que ahorre tiempo y dinero.

Kaspersky Endpoint Security Cloud Pro va mucho más allá, ya que le proporciona la tranquilidad de la protección contra las amenazas evasivas a medida que se desarrolla su seguridad.

Kaspersky Endpoint Security Cloud está diseñado para los negocios ágiles. Desde la simple interfaz de usuario hasta la fácil implementación y las operaciones fluidas, desde la incorporación de nuevos empleados hasta el mantenimiento diario, es fácil de administrar y está listo para proteger su organización de las ciberamenazas más actuales e incipientes.



Siéntase como un especialista en ciberseguridad gracias a nuestras capacidades de EDR

Comience con el análisis de la causa raíz (que se incluye en la licencia Plus) y, luego, continúe con Kaspersky Endpoint Security Cloud Pro. Obtendrá más opciones de respuesta automatizada, como el análisis de IoC y el aislamiento del host.

Admitámoslo, los administradores de TI abarcan muchas áreas y la de ciberseguridad suele ser solo una más entre muchas otras. Aunque los administradores inteligentes comprenden la necesidad de contar con soluciones sólidas de ciberseguridad, no es su especialización. Mientras tanto, las amenazas continúan evolucionando, y las que se solían observar con poca frecuencia o tenían como objetivo a las grandes empresas se vuelven cada vez más comunes y generalizadas. Por lo tanto, desde la perspectiva del presupuesto, es importante elegir una solución que se actualice de forma regular con tecnologías de vanguardia, de forma que cuente con una protección completa en el futuro sin necesidad de realizar inversiones considerables más adelante.

Endpoint Detection and Response le da acceso a una herramienta de ciberseguridad de grado empresarial, y a la oportunidad de mejorar en la detección y respuesta ante amenazas evasivas. Al mismo tiempo, nuestro enfoque promete que la experiencia de usuario general de EDR será simple y sin complicaciones, y que no requerirá ningún cambio en su infraestructura.

Nuestro **análisis de la causa raíz** ofrece capacidades de visibilidad y detección de amenazas avanzadas, en conjunto con acceso a herramientas profesionales de investigación de incidentes, sin necesidad de realizar ajustes en la infraestructura.

De esta forma, usted, como administrador de TI, puede realizar investigaciones de incidentes mediante el uso del contexto y los detalles del mismo. Puede realizar un análisis de la causa raíz con un esquema de propagación del ataque y desglosar los detalles para revisar lo siguiente:

- Datos del host: versión del sistema operativo, interfaces de red y usuarios
- Datos del archivo: nombre, hash, parámetros de creación y modificación, parámetros de descarga, etc.
- Datos del proceso: fecha y hora, parámetros de inicio
- Detecciones e incidentes relacionados, y mucho más

Las opciones de respuesta automatizada ayudan a detener los ataques de las amenazas, y así evitar la ejecución de archivos, mediante el uso del aislamiento del host y las verificaciones de análisis de IoC (indicador de compromiso). En el caso de que se produzca un ataque, el sistema aísla al host de la red, lo cual evita que el ataque se propague a otros dispositivos. Luego, mediante el análisis de IoC, se comprueban todos los dispositivos en busca de IoC similares al que estuvo involucrado en el ataque inicial y se aíslan todos los dispositivos que puedan verse afectados.

Ahora que usa la camiseta de seguridad con confianza, puede proteger la red, responder preguntas e iniciar automáticamente el activador de emergencia. Imagine lo feliz que podría ser... y qué fácil le será conciliar el sueño a partir de ahora.

Detenga el caos de la “TI invisible” y tome el control de los servicios en la nube

Cloud Discovery le permite bloquear el acceso de los usuarios a recursos de nube innecesarios, inapropiados y no autorizados, para que sus datos estén seguros en su control, y sus colegas mantengan la concentración y la productividad.

Mire a sus colegas de trabajo: ¿puede saber quién está perdiendo el tiempo en Facebook en este momento y quién está chateando por mensajería instantánea? Y, lo que es aún más importante, ¿quién comparte datos corporativos en servicios de almacenamiento en la nube sin que usted lo sepa? Correcto, no tiene ni idea. Por eso, Cloud Discovery, incluido en Kaspersky Endpoint Security Cloud, está aquí para ayudar.

Cloud Discovery le permite ver el panorama real y desarrollar un plan de acción. Puede bloquear el acceso de los usuarios a recursos innecesarios, inapropiados y no autorizados en la nube, de forma que sus datos estén seguros en su control, y sus colegas mantengan la concentración y la productividad. Con solo unos pocos clics, tendrá una imagen completa del uso de la nube en su infraestructura, a través de un widget interactivo o un informe exportable. Al contar con estas estadísticas, puede resaltar a la gerencia el problema del uso compartido y la divulgación incontrolados de los datos corporativos, así como el tiempo desperdiciado en redes sociales y aplicaciones de mensajería.

En muchos casos, esto genera oportunidades de crecimiento. Por lo general, las personas no se proponen provocar daños mediante el uso de servicios en la nube no autorizados. Muchas veces, solo intentan trabajar de forma más eficiente. Si, por ejemplo, implementó una solución corporativa de conferencias de video o CRM en la nube, pero resulta que sus usuarios siguen utilizando soluciones públicas o propagando tablas de documentos de Google, vale la pena preguntarse por qué sucede esto.

Puede que la respuesta lo sorprenda. Puede que, en ellas, se incluyan problemas con el uso de software corporativo, hábitos de uso antiguos o falta de conocimiento, o puede que solo se pasaran por alto un correo electrónico con las nuevas directivas de la empresa. Problemas como estos pueden retardar la transformación digital y el crecimiento de la empresa en general. Las estadísticas de Cloud Discovery pueden indicar la forma de educar mejor a los usuarios o mejorar el cuidado de la seguridad.

Cloud Discovery es una alternativa simple y rentable en comparación con soluciones complejas y costosas de **CASB (Agente de seguridad de acceso a la nube)**. Podrá detectar y bloquear el uso de servicios en la nube no autorizados y de TI invisible como parte de sus defensas cibernéticas estándar, sin necesidad de contar con habilidades especiales.

Seguridad para Microsoft Office 365 incluida

Incluso con Cloud Discovery a bordo, es posible que, como muchas empresas, tenga preocupaciones de seguridad sobre Microsoft Office 365. Para ayudar en mayor medida a tomar el control de la nube, incluimos la protección para Office 365 con los niveles **Plus** y **Pro** de **Kaspersky Endpoint Security Cloud**. Por cada 10 licencias, brindamos la protección de Kaspersky Security for Microsoft Office 365 a 15 usuarios o casillas de correo. **Nuestra solución de seguridad Office 365 ofrece** protección avanzada contra amenazas todo en uno para los servicios de comunicación y colaboración de Microsoft Office 365, que incluye lo siguiente:

- **Microsoft Exchange Online, OneDrive, SharePoint Online y Teams**
- **Protección avanzada (antiphishing, antimalware, antispam, eliminación de archivos adjuntos no deseados, protección a petición)**

Cumplimiento del RGPD sin muchos problemas

Cumplir con el RGPD no es negociable, independientemente del tamaño de su operación. Data Discovery, también incluido en los niveles **Plus** y **Pro** de **Kaspersky Endpoint Security Cloud**, le ofrece la visibilidad y el control que necesita para evitar las fugas de datos y cumplir con la normativa. Ahora puede ver exactamente dónde, y por qué se almacenan y procesan en la nube todos los datos de los que es responsable, comprobar si los datos personales pueden ser accesibles para terceros, detectar los datos que se almacenan durante más tiempo del debido, y mucho más. De repente, cumplir con la normativa es mucho más simple.

Administración de parches sin esfuerzo

A nadie le agrada colocar parches en dispositivos de forma manual, pero es una actividad que se debe hacer con regularidad por razones de cuidado cibernético. Es como cepillarse los dientes: aburrido pero efectivo. Entonces, ¿por qué no liberarse de la molestia y dejar todo en manos de la administración programada automática de parches? Se incluye en **Kaspersky Endpoint Security Cloud Plus** y **Kaspersky Endpoint Security Cloud Pro**

Cifrado de dispositivos sin esfuerzo

El cifrado de unidades de disco basado en FileVault (macOS) y BitLocker (Windows) también se puede administrar mediante la consola de Kaspersky Endpoint Security Cloud, y el cifrado se puede aplicar de forma remota si es necesario.

Casi todas las organizaciones recopilan y almacenan diferentes formas de información de identificación personal, datos financieros, documentos confidenciales y otros datos confidenciales en sus sistemas de TI. La divulgación o pérdida de estos datos puede dar lugar a multas y juicios, también puede tener un impacto muy negativo en el negocio en general. El cifrado de datos ayuda a garantizar que estos datos no se vean comprometidos si alguien irrumpe en su sistema o si le roban un dispositivo.

Implementación eficiente del agente de endpoint: ¿con AD (Active Directory) o sin AD?

Descargue su cliente de Kaspersky Endpoint Security y, a continuación, agregue el script de inicio de sesión simple proporcionado a su directiva de dominio de AD

Si solo debe cuidar de unas pocas computadoras, es fácil instalar la protección de endpoints con solo una unidad flash. Una vez que tenga entre 50 y 100 dispositivos, la situación se vuelve menos simple, pero la implementación sigue siendo rápida y sin problemas.

Kaspersky Endpoint Security Cloud ofrece dos opciones de instalación, según lo que funcione mejor para usted:

1. Implementación remota por correo electrónico

Se envía un enlace a cada dispositivo a través de la **consola de Kaspersky Endpoint Security Cloud**. El usuario hace clic en el enlace para activar la descarga e instalación de la aplicación en el endpoint. Después, este endpoint se hace visible en la lista de dispositivos protegidos en su consola.

2. Implementación automática con AD (Active Directory)

Descargue su **cliente de Kaspersky Endpoint Security**, y a continuación agregue el script de inicio de sesión simple proporcionado a su directiva de dominio de AD. La aplicación se implementará automáticamente en sus endpoints y los verá enumerados como dispositivos protegidos en la **consola de Kaspersky Endpoint Security Cloud**. Consulte las instrucciones aquí.

¡Anímese y compruébelo por usted mismo!

Para obtener más información sobre cómo Kaspersky Endpoint Security Cloud puede ayudar a proteger sus negocios de manera fácil y para probar nuestros productos, visite **https://cloud.kaspersky.com/**

Noticias sobre amenazas cibernéticas: securelist.lat
Noticias sobre seguridad de TI: business.kaspersky.com
Seguridad de TI para pequeñas y medianas empresas: kaspersky.com/business
Seguridad de TI para grandes empresas: kaspersky.com/enterprise

latam.kaspersky.com

Estamos probados. Somos independientes. Somos transparentes. Nos comprometemos con la construcción de 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 ofrece la tecnología. Incorpore ciberseguridad para disfrutar de un futuro más seguro.
Obtenga más información en latam.kaspersky.com/about/transparency

Proven. Transparent. Independent.