



# Kaspersky Endpoint Security Cloud Plus

Protección de endpoints para negocios flexibles

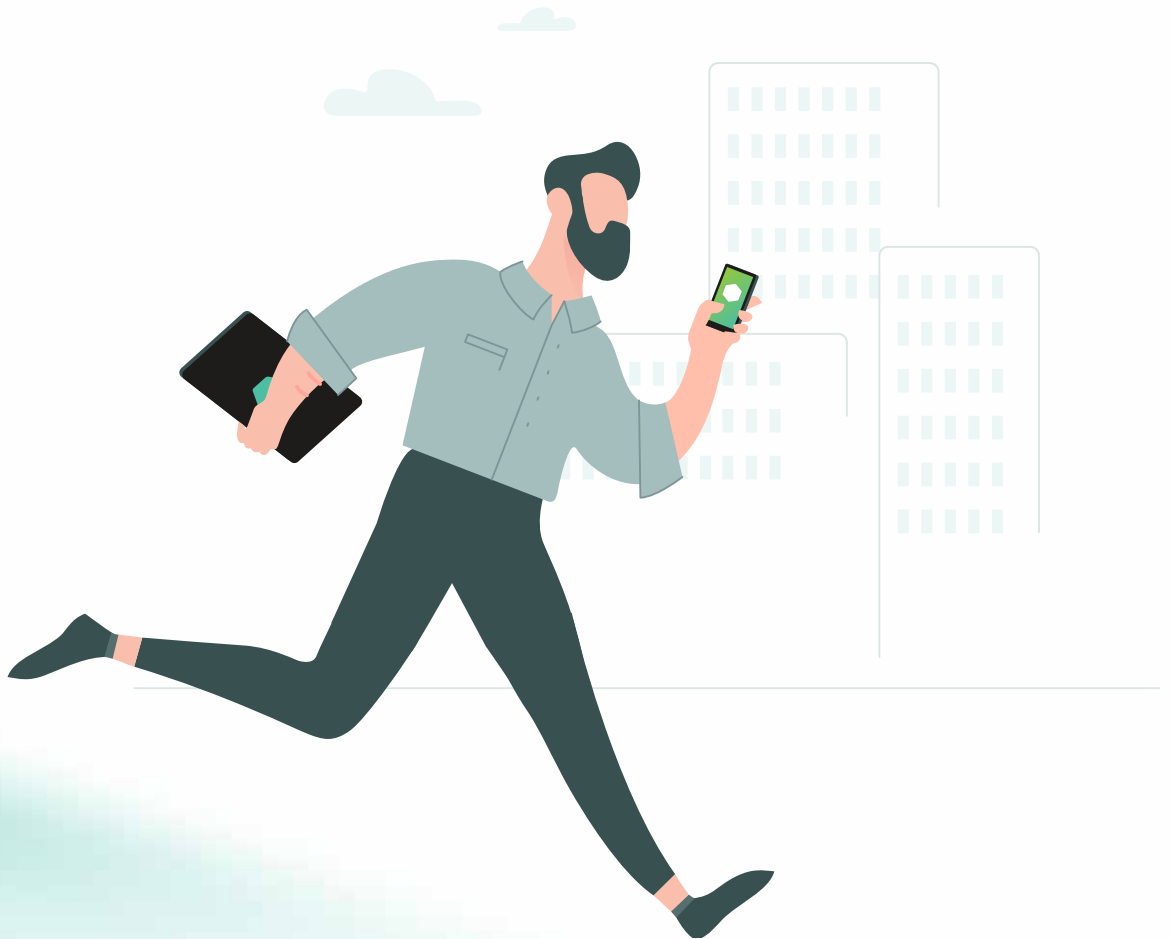
kaspersky

## Flexibilidad en su día a día

**Kaspersky Endpoint Security Cloud Plus se ha diseñado para ofrecer flexibilidad**

Su negocio está creciendo. El número de tareas de seguridad de IT con las que tiene que lidiar crece de la misma manera. Sin embargo, aún no está preparado para contratar a un especialista en seguridad. Por esa razón, hemos creado **Kaspersky Endpoint Security Cloud Plus** para ayudarle a gestionar las tareas de seguridad rutinarias con facilidad, lo que le permitirá ahorrar tiempo y dinero.

**Kaspersky Endpoint Security Cloud Plus** se ha diseñado para ofrecer flexibilidad. Esta solución es fácil de gestionar: desde su sencilla interfaz de usuario a través de un fácil despliegue y operaciones sin problemas hasta para la incorporación de nuevos empleados y el mantenimiento diario. Además, está preparada para proteger a su organización de las ciberamenazas avanzadas.



Descargue su cliente de Kaspersky Endpoint Security y, a continuación, añada el script de inicio de sesión simple que se proporciona a su política de dominios de AD

## Implementación eficaz de agente para endpoints: ¿con AD (Active Directory) o sin AD?

Es fácil instalar la protección de endpoints con una unidad flash si solo tiene un par de ordenadores. Si tiene entre 50 y 100 dispositivos, la situación se complica un poco, pero la implementación debería seguir siendo rápida y sencilla.

**Kaspersky Endpoint Security Cloud Plus** ofrece dos opciones de instalación, en función de lo que mejor se adapte a sus necesidades:

### 1. Implementación automática con AD (Active Directory)

Descargue su **cliente de Kaspersky Endpoint Security** y, a continuación, añada el script de inicio de sesión simple que se proporciona a su política de dominios de AD. La aplicación se implementará automáticamente en los endpoints y verá que aparecen como dispositivos protegidos en la **consola de Kaspersky Endpoint Security Cloud**. Consulte las instrucciones [aquí](#).

### 2. Implementación remota por correo electrónico

Se envía un enlace por correo electrónico 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, tras lo cual el endpoint aparecerá en la lista de dispositivos protegidos de la consola.



---

## Cifrado de dispositivos sin esfuerzo

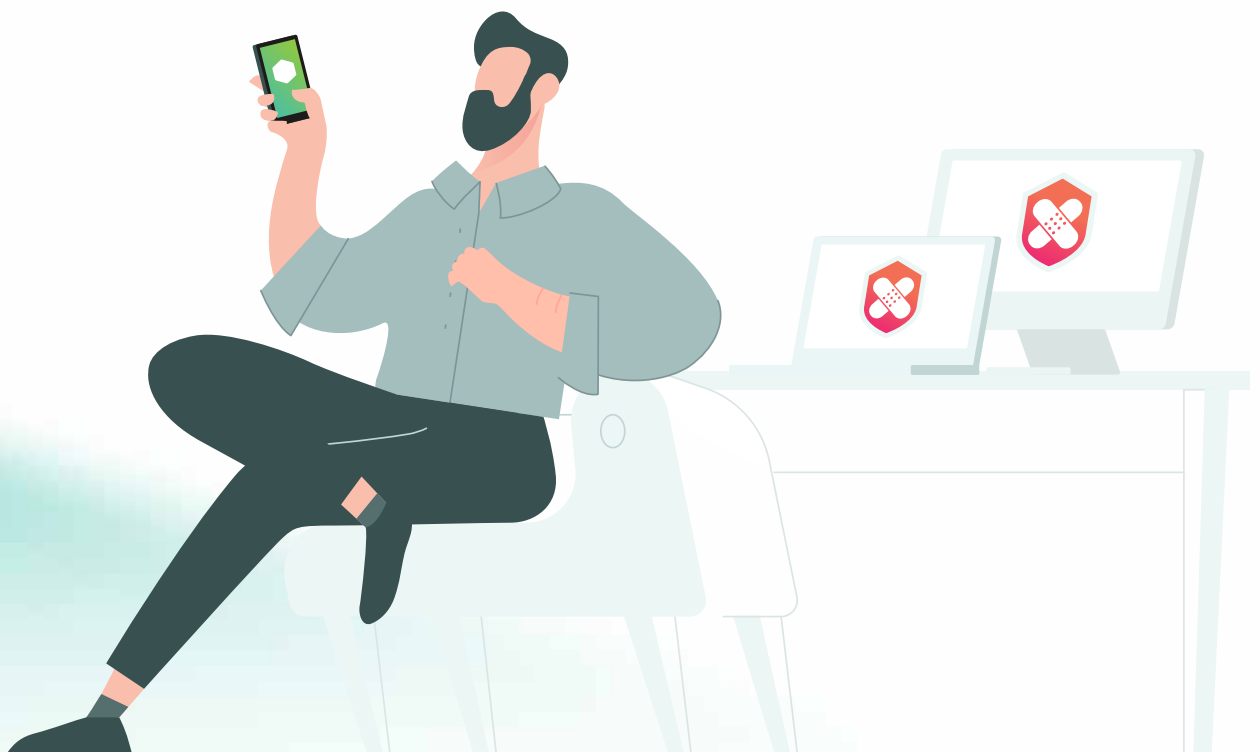
El cifrado basado en unidades de disco de FileVault (macOS) y de BitLocker (Windows) también se puede gestionar a través de la consola de Kaspersky Endpoint Security Cloud, así como gestionarse de forma remota si fuera necesario.

Casi todas las organizaciones recopilan y almacenan diferentes tipos de información personal identificable, datos financieros, documentos confidenciales y otros datos confidenciales en sus sistemas de IT. La divulgación o la pérdida de estos datos puede conllevar multas y acciones legales, y puede tener un impacto muy negativo en su negocio a nivel general. El cifrado de datos ayuda a garantizar que no se vean comprometidos en caso de que se produzca un fallo en el sistema o un robo del dispositivo.

---

## Gestión de parches para la puesta en marcha

No es para nada entretenido realizar la aplicación de parches a los dispositivos, pero es necesario para mantener una higiene cibernética. Es como lavarse los dientes: es aburrido, pero eficaz. Así que, ¿por qué no evita complicaciones y deja que se encargue de todo la gestión automática de parches programados que incluye **Kaspersky Endpoint Security Cloud Plus**?



## Detener el caos de la Shadow IT y tomar el control de la nube

Cloud Discovery le permite bloquear el acceso de los usuarios a recursos en la nube innecesarios, inapropiados y no autorizados, a fin de mantener la seguridad de sus datos y conseguir que sus compañeros se centren en sus tareas y sean productivos.

**Eche un vistazo a sus compañeros de trabajo: ¿podría adivinar quién está perdiendo tiempo en Facebook ahora mismo y quién está chateando en un servicio de mensajería instantánea?** Y, lo que es aún más importante, ¿sabría decir quién comparte datos corporativos en servicios de almacenamiento en la nube que usted desconoce? Exacto: no lo sabe. Por eso, la función Cloud Discovery, incluida en Kaspersky Endpoint Security Cloud, le ayuda a quitarse la venda de los ojos.

Cloud Discovery le permite bloquear el acceso de los usuarios a recursos en la nube innecesarios, inapropiados y no autorizados, a fin de mantener la seguridad de sus datos y conseguir que sus compañeros se centren en sus tareas y sean productivos. Con un par de clics, tendrá una visión completa del uso de la nube en su infraestructura, a través de un widget interactivo o un informe exportable. Con estas estadísticas, podrá gestionar el problema de la divulgación y el uso compartido de datos empresariales no controlados, así como el tiempo perdido en las redes sociales y en los servicios de mensajería.

La nuestra es la única solución basada en endpoints del mercado que ofrece esta tecnología de descubrimiento de la Shadow IT. La alternativa sería la adquisición de una solución de **agente de seguridad de acceso a la nube (CASB)** cara y complicada. Cloud Discovery le ayudará a detectar y a bloquear el uso de servicios de la nube no autorizados y la Shadow IT, como parte de sus defensas cibernéticas estándar, sin necesidad de conocimientos especiales.



---

# Security for Microsoft Office 365

Incluso con Cloud Discovery integrada, es posible que, como muchos negocios, tenga problemas de seguridad con Microsoft Office 365. Para ayudarle a controlar su nube, incluimos la protección para Office 365 totalmente gratis con **Kaspersky Endpoint Security Cloud Plus**. Con cada 10 licencias, ofrecemos la protección Kaspersky Security for Microsoft Office 365 para 15 buzones de correo/usuarios. **Nuestra solución de seguridad de Office 365 ofrece** protección avanzada y completa contra amenazas para los servicios de comunicación y colaboración de Microsoft Office 365, entre los que se incluyen:

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



---

## ¡Eche un vistazo y compruébelo de primera mano!

Para obtener más información sobre cómo **Kaspersky Endpoint Security Cloud Plus** puede ayudarle a proteger su negocio de la forma más sencilla y comprobarlo de primera mano, visite <https://cloud.kaspersky.com/>

---

Noticias de ciberamenazas: [www.viruslist.es](http://www.viruslist.es)  
Noticias de seguridad de IT: [business.kaspersky.com](http://business.kaspersky.com)  
Seguridad de IT para pymes: <https://www.kaspersky.es/small-to-medium-business-security>  
Seguridad de IT para grandes empresas: [kaspersky.es/enterprise-security](http://kaspersky.es/enterprise-security)

[www.kaspersky.es](http://www.kaspersky.es)

2020 Kaspersky Lab Iberia, España. Todos los derechos reservados.  
Las marcas registradas y logos son propiedad de sus respectivos dueños.



Seguridad probada, independiente y transparente. Nos comprometemos a construir un mundo más seguro en el que la tecnología nos mejore la vida. 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.

Más información en [kaspersky.es/transparency](http://kaspersky.es/transparency)



Probada.  
Independiente.  
Transparente.