Kaspersky Security for Microsoft Office 365
Funcionamiento

Kaspersky Security for Microsoft Office 365 utiliza tecnología de última generación para proteger el correo contra spam, ataques al correo corporativo, phishing, ransomware y amenazas avanzadas.

Descubre cómo.

1. Se hace un registro rápido y sencillo en cloud.kaspersky.com
2. Se conecta Office 365 a la consola de gestión Online
3. Se activa la protección
4. El correo llega a la nube de Office 365
5. Kaspersky Security for Microsoft Office 365 analiza en busca de amenazas
6. El correo legítimo permanece en la bandeja de entrada del usuario; el correo malicioso o sospechoso se filtra en una carpeta invisible a la que solo puede acceder el administrador
7. El proceso de filtrado es rápido y eficiente
8. Los datos no se almacenan en Kaspersky Lab; los administradores eligen un centro de datos determinado para realizar el procesamiento

¿Cómo garantizamos la máxima protección?

Las tecnologías de seguridad de última generación filtran incluso las amenazas desconocidas antes de que el usuario pueda cometer un error.

Tecnología antispam de última generación

Los modelos de detección de Kaspersky Lab basados en el aprendizaje automático detectan incluso el spam sofisticado y desconocido y ahorran tiempo mediante la disminución del número de falsos positivos.

Detección multicapa basada en HuMachine

Identifica incluso el malware desconocido. Los archivos sospechosos se pueden ejecutar en un espacio seguro antes de moverlos a la bandeja de entrada.

Aprendizaje automático

Los algoritmos de aprendizaje automático han sido diseñados para identificar malware en conjuntos de correos con más de 200 millones de archivos maliciosos y más de mil millones de archivos limpios. Estos modelos de detección filtran malware de día cero y hasta entonces desconocido.

Inteligencia de amenazas del Big Data

Basada en Kaspersky Security Network, la inteligencia de amenazas global basada en la nube se actualiza constantemente. Cuenta con la experiencia humana de más de 200 expertos especializados en amenazas.

Filtrado de archivos adjuntos:

El filtrado de archivos adjuntos bloquea los archivos peligrosos antes de que se conviertan en un problema. El reconocimiento de tipo de archivo real filtra tanto el contenido peligroso como el contenido no deseado.

Antiphishing de última generación

El motor antiphishing de Kaspersky Lab basado en redes neuronales utiliza más de 1000 criterios para crear modelos de detección.