



Kaspersky® Security for Microsoft Office 365

Se envían 3.5 millones de emails por segundo. Un solo email es suficiente para arruinar su empresa

Kaspersky Security for Microsoft Office 365 utiliza heurística avanzada, aislamiento de procesos, aprendizaje de máquina y otras tecnologías de nueva generación para proteger los correos electrónicos contra ransomware, archivos adjuntos maliciosos, spam, phishing, estafas BEC (Business Email Compromise) y amenazas desconocidas. Nuestra solución de seguridad, al igual que Microsoft Office 365, se alberga en la nube, y como todas las soluciones de Kaspersky Lab, se basa en la seguridad más premiada y más probada del mundo¹. Mantenga el flujo de comunicación libre de ciberamenazas con **Kaspersky Security for Microsoft Office 365**.

Aumentar la productividad y reducir las amenazas antispam de nueva generación

El 50% de los emails enviados son spam. Reduzca tiempo, recursos y riesgos asociados al spam bloqueando los correos electrónicos no deseados antes de que lleguen a su bandeja de entrada. El servicio de nueva generación de Kaspersky Lab para la detección y el análisis utiliza el aprendizaje de máquina y la inteligencia en la nube en tiempo real de Kaspersky Security Network.

Protección antim malware gracias a la nube

El 99% de los malware se envía por correo electrónico o vía servidor web, mientras que el 66% se instala desde archivos adjuntos maliciosos². Pueden prevenir los ataques vía correo electrónico bloqueando los malware desconocidos y de día cero que se pueden encontrar en archivos Word, Excel, Power Point y otras aplicaciones.

Ya basta de ransomware, phishing y otras amenazas avanzadas

Las empresas son atacadas por ransomware cada 40 segundos, y el phishing por correo electrónico es un vector popular para estos ataques. El 78% de los usuarios comprende el riesgo de los emails enviados por remitentes desconocidos y, aún así, uno de cada dos usuarios hace click en ellos. Kaspersky Security for Microsoft Office 365 utiliza el aislamiento de procesos y el aprendizaje de máquina para filtrar las amenazas antes de que el usuario pueda cometer algún error.

Protección, integridad y control de los datos

Ya no hay que preocuparse de la privacidad. Desde el momento de su configuración, los administradores eligen el centro de datos asignado para el procesamiento del correo electrónico. Kaspersky Lab no guarda los emails de los clientes, los correos electrónicos sospechosos se trasladan a una carpeta a la que solo el administrador puede acceder a través de la consola de gestión de Kaspersky Microsoft Office 365.

Reducción de falsos positivos: ya no desaparecerán los emails

Muchos usuarios tienen el problema de que los emails legítimos se etiqueten como spam por error. Gracias a la disminución de falsos positivos y al control de lo que pasa con el correo electrónico sospechoso, Kaspersky Security for Microsoft Office 365 reduce las posibilidades de que esto ocurra. Los emails borrados se guardan en copias de seguridad, para poder buscarlos y restaurarlos si es necesario. Ya no habrá "correos desaparecidos".

Fácil de usar y económico

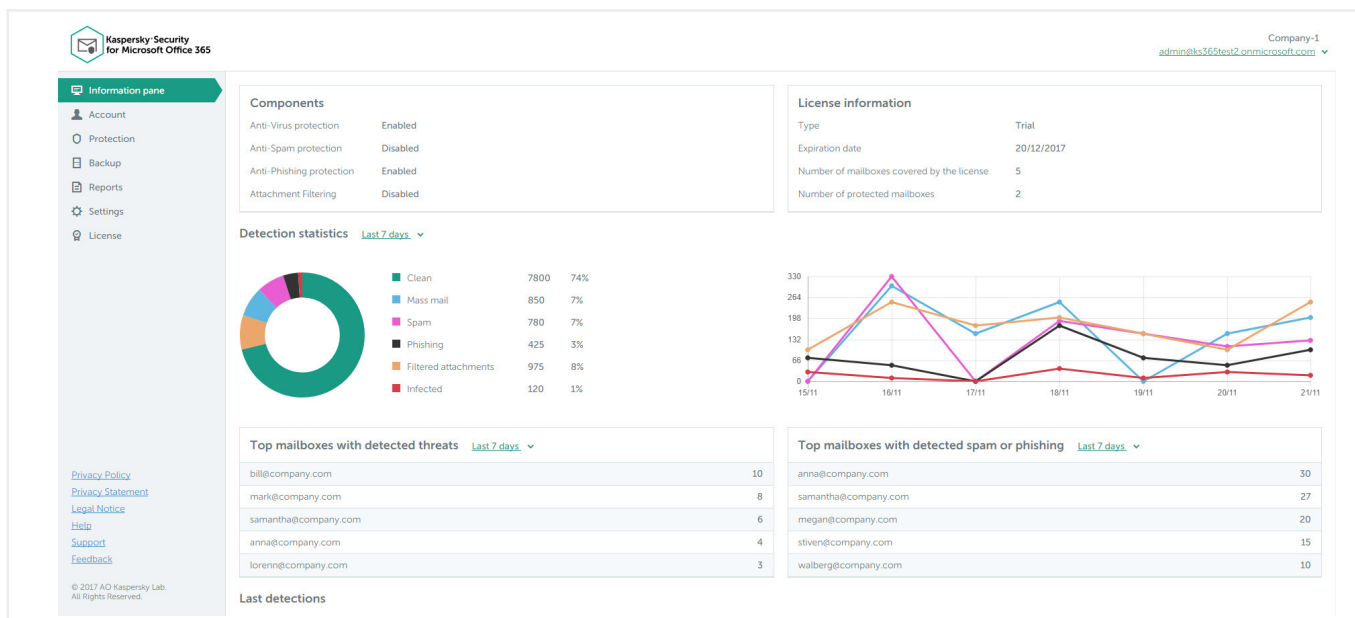
Una interfaz intuitiva y fácil de usar significa que no es necesario organizar una formación adicional para los empleados. Una sola consola de gestión se ocupa de todo y proporciona una visión única de las amenazas detectadas y de las estadísticas. Una política de uso única y sencilla otorga una protección integrada y no es necesario invertir en infraestructuras adicionales o instalar archivos distributivos para empezar.

¹ En 2016, los productos de Kaspersky Lab participaron en 78 test y reseñas independientes. Nuestros productos fueron los mejores en 55 ocasiones, y se clasificaron entre los 3 mejores de su categoría en 70 ocasiones. <https://latam.kaspersky.com/top3>

² Verizon Data Breach Investigation Report 2017 (Investigación de Brechas de datos de Verizon)

³ Boletín de seguridad de Kaspersky 2016. La revolución del ransomware

⁴ Friedrich-Alexander Universität: "FAU Researchers investigate user behavior when unknown messages are received online." (Investigación del comportamiento del usuario al recibir mensajes online desconocidos)



Tecnologías de nueva generación

Impulsado por Kaspersky Security Network

Kaspersky Security Network incluye el análisis de reputación y la función antiphishing gracias a sus datos sobre las últimas amenazas de spam. Esta tecnología analiza el tráfico casi en tiempo real para detectar, bloquear y eliminar las últimas amenazas, incluidos ransomware y ataques de día cero.

Heurística y aprendizaje de máquina

El sistema de detección automática basado en la heurística asegura incluso el descubrimiento de malware desconocido. El aprendizaje de máquina permite la detección rápida de las secuencias de ejecución, que indican la presencia de un ataque. Junto con los registros de aislamiento de procesos, el resultado final es un perfeccionamiento constante de los indicadores de detección y una consecuente protección de máximo nivel contra las últimas amenazas, minimizando al mismo tiempo los falsos positivos.

Prueba gratuita en cloud.kaspersky.com

Kaspersky Lab
 Noticias de ciberamenazas: <https://securelist.lat/>
 Noticias de seguridad TI: <https://latam.kaspersky.com/blog/category/business/>

#truecybersecurity
 #HuMachine

<https://latam.kaspersky.com/>

© 2017 AO Kaspersky Lab. Todos los derechos reservados. Las marcas registradas y sus servicios son propiedad de sus respectivos propietarios.

Juntos es aún mejor

Kaspersky Business Hub – Una sola consola para gestionar la protección de su empresa. Interfaz intuitiva, gestión sencilla y protección superior para diferentes dispositivos y herramientas de productividad, todo desde un solo lugar.

A través de **Kaspersky Business Hub** se gestionan los siguientes productos:

- Kaspersky Endpoint Security Cloud
- Kaspersky Security for Microsoft Office 365

Kaspersky Security for Microsoft Office 365 features

- Gestión centralizada
- Política de uso sencilla
- Tablero de amenazas para informes y estadísticas
- Eliminación de archivos adjuntos no deseados
- Reconocimiento de tipo de archivo verdadero: reconocimiento preciso del tipo de archivo, independientemente de su extensión
- Antispam, antimalware y antiphishing
- No se necesita infraestructura adicional

