# MAIL SECURITY

## PARA MICROSOFT EXCHANGE SERVER

30 AÑOS DE INNOVACIÓN CONTINUA EN SEGURIDAD

BUSINESS

ENJOY SAFER TECHNOLOGY™

# MAIL SECURITY
## PARA MICROSOFT EXCHANGE SERVER

ESET Mail Security para Microsoft Exchange Server integra una potente protección antivirus y antispam que se asegura que todo contenido dañino proveniente del correo electrónico sea filtrado y eliminado.

Con nuestra solución, obtendrá una protección completa del servidor, incluso del sistema de archivos propio del servidor. Podrás aplicar políticas para contenido específico según el tipo de archivo real y monitorear el estado de seguridad o personalizar la configuración con la herramienta ESET Remote Administrator.

## Protección Antimalware y Antispam

| | |
|---|---|
| **Antivirus y Antispyware** | Explora todo el tráfico POP3, SMTP e IMAP entrante y saliente. Filtra las amenazas provenientes del correo electrónico, incluyendo el spyware en el nivel de la puerta de enlace.<br><br>**Exploración opcional basada en la nube:**<br>Crea listas blancas de archivos seguros según la base de datos de reputación de archivos en la nube, para lograr una mejor detección y una exploración más rápida. Solo se envía a la nube la información de archivos ejecutables y comprimidos; el envío se realiza en forma anónima. |
| **Antispam y Anti-Phishing** | Detiene el spam y los intentos de phishing, y ofrece altas tasas de bloqueo sin necesidad de establecer manualmente el nivel de confianza contra spam (SCL). Tras la instalación, el módulo antispam está listo para ejecutarse. No requiere ajuste manual de los parámetros ni de los niveles de confianza. |
| **Administración de la cuarentena local** | Los usuarios de correo pueden interactuar en forma directa, desde un navegador independiente, con los mensajes bloqueados y que no se entregaron por considerarse spam o por sospechar que contienen malware. Según los permisos establecidos por el administrador, el usuario puede clasificar los mensajes en cuarentena, realizar búsquedas y ejecutar acciones (por mensaje individual o grupal) desde un navegador Web. Las acciones dependen del motivo por el cual cada mensaje se puso en cuarentena. Permite enviar un informe por correo al usuario con un resumen de los mensajes en cuarentena y enlaces para ejecutar acciones. |
| **Exploración bajo demanda de la base de datos** | Los administradores pueden elegir qué bases de datos y buzones de correo explorar. Para limitar aún más las exploraciones, permite filtrar por la fecha de modificación de cada mensaje, lo que reduce a un mínimo los recursos del servidor dedicados a esta tarea. |
| **Reglas de procesamiento de mensajes** | Las reglas de procesamiento de mensajes ofrecen una amplia gama de combinaciones para manejarlos. Los parámetros evaluados incluyen campos estándar como sujeto, remitente, cuerpo y un encabezado específico del mensaje, pero también permiten hacer un procesamiento condicional basándose en los resultados anteriores del filtro antispam o del explorador antivirus. Se identifican los archivos alterados o protegidos por contraseña y se examina el interior de los archivos adjuntos para determinar el tipo de archivo real, más allá de la extensión pretendida. Las reglas se pueden cambiar según las acciones deseadas. |
| **Bloqueo de exploits** | Refuerza la seguridad de las aplicaciones como los navegadores Web, los lectores de PDF, los clientes de correo electrónico y los componentes de MS Office, que suelen ser un objetivo común de ataque. Monitorea la conducta de los procesos en busca de actividades sospechosas típicas de los exploits. Refuerza la protección ante ataques dirigidos y exploits desconocidos hasta el momento, (ataques zero-day). |
| **Exploración avanzada de memoria** | Monitorea la conducta de los procesos maliciosos y los explora cuando se muestran en memoria. De esta forma, se logra una prevención efectiva contra las infecciones, incluso ante los tipos más furtivos de malware. |
| **Sistema de prevención de intrusiones basado en el host (HIPS)** | Permite definir reglas para el registro del sistema, los procesos, las aplicaciones y los archivos. Suministra protección ante la manipulación indebida y detecta amenazas basándose en la conducta del sistema. |
| **Control de dispositivos** | Bloquea los dispositivos portátiles no autorizados e impide que se conecten al servidor. Crea reglas para grupos de usuarios con el objetivo de cumplir con las políticas corporativas. Permite advertir antes de bloquear: le notifica al usuario final que se bloqueó su dispositivo y le da la opción de acceder a él pero registrando la actividad. |

# Protección de infraestructuras complejas

| | |
|---|---|
| **Independencia de instantáneas** | Las actualizaciones y los módulos del programa de ESET se pueden almacenar fuera de la ubicación predeterminada, es decir que no se ven afectados cuando una máquina virtual revierte su configuración a una instantánea anterior. En consecuencia, no es necesario descargar las actualizaciones y los módulos cada vez que la máquina virtual revierte su instantánea: puede utilizar las mismas actualizaciones intactas y así evitar grandes descargas, lo que acelera el tiempo de recuperación de la instantánea. |
| **Soporte nativo para entornos de clúster** | Permite configurar la solución para replicar la configuración en forma automática cuando se instala en un entorno de clúster. Nuestro asistente intuitivo facilita la interconexión de los diversos nodos instalados de ESET Mail Security dentro de un clúster y los administra como si fueran uno solo, eliminando la necesidad de replicar manualmente los cambios de configuración a otros nodos del clúster. |
| **ESET Shared Local Cache** | La Caché local compartida de ESET compara los metadatos de cada archivo que se va a explorar con los metadatos ya almacenados, y saltea automáticamente los archivos no infectados incluidos en la lista blanca. Cada vez que encuentra un archivo nuevo aún no explorado, se agrega automáticamente a la caché.<br>Esto significa que los archivos ya explorados en una máquina virtual no se vuelven a explorar en forma reiterada en otras máquinas dentro del mismo entorno virtual, lo que genera un incremento significativo de la velocidad de exploración. Como la comunicación se realiza a través del mismo hardware físico, prácticamente no hay ningún retraso en la exploración y se ahorra una cantidad considerable de recursos. |
| **Proveedor de Instrumental de Administración de Windows (WMI)** | Brinda la posibilidad de monitorear las funcionalidades clave de ESET Mail Security a través del marco del Instrumental de Administración de Windows. Esto permite la integración de ESET Mail Server con software administrativo de terceros y herramientas SIEM, como el System Center Operations Manager de Windows, Nagios, entre otros. |

SOPORTE TÉCNICO LOCAL Y GRATUITO

Haga más con la ayuda de nuestros especialistas. Soporte técnico disponible cuando lo necesita, en su idioma.

# Usabilidad

| | |
|---|---|
| **Exclusiones de procesos** | El administrador puede definir los procesos que el módulo de protección en tiempo real debe ignorar; todas las operaciones con archivos que se atribuyan a estos procesos excluidos se considerarán seguros. Resulta útil en particular para procesos que suelen interferir con la protección en tiempo real, como la creación de backups o la migración en vivo de máquinas virtuales. Sin embargo, hay que tener en cuenta que los procesos excluidos pueden acceder a archivos u objetos no seguros sin accionar ninguna alerta. |
| **Microdefiniciones acumulativas** | Las actualizaciones regulares se descargan y aplican en forma acumulativa mediante paquetes pequeños.<br>Su propósito es conservar los recursos del sistema y el ancho de banda de Internet, sin ningún impacto notable en la velocidad de la infraestructura de red completa y de los servidores, ni en las demandas de las endpoints a la memoria del sistema o la CPU. |
| **Instalación basada en componentes** | Además de instalar los componentes obligatorios, ESET permite elegir entre los siguientes componentes adicionales:<br>– Protección del sistema de archivos en tiempo real<br>– Protección Web y de correo electrónico<br>– Control de dispositivos<br>– Interfaz gráfica de usuario (GUI)<br>– Recopilador de registros de ESET<br>– y más |
| **Administración Remota** | ESET Mail Security se administra en forma completa desde ESET Remote Administrator. Permite desplegar, ejecutar tareas, determinar políticas, recopilar registros y obtener notificaciones e información general de la seguridad de la red: todo a través de una única consola de administración basada en la Web. |
| **Recopilador de registros de ESET** | Reúne todos los registros relevantes necesarios para la solución de problemas, con la asistencia del soporte técnico de ESET. Luego agrupa los registros en un único archivo comprimido que se puede enviar por correo electrónico o subir a una unidad compartida de red para acelerar la resolución del problema. |
| **ESET License Administrator** | Permite manejar todas las licencias en forma transparente, desde un mismo lugar, a través de un navegador Web. Permite combinar, delegar y administrar todas las licencias de manera centralizada en tiempo real, incluso aunque no se esté usando ESET Remote Administrator. |