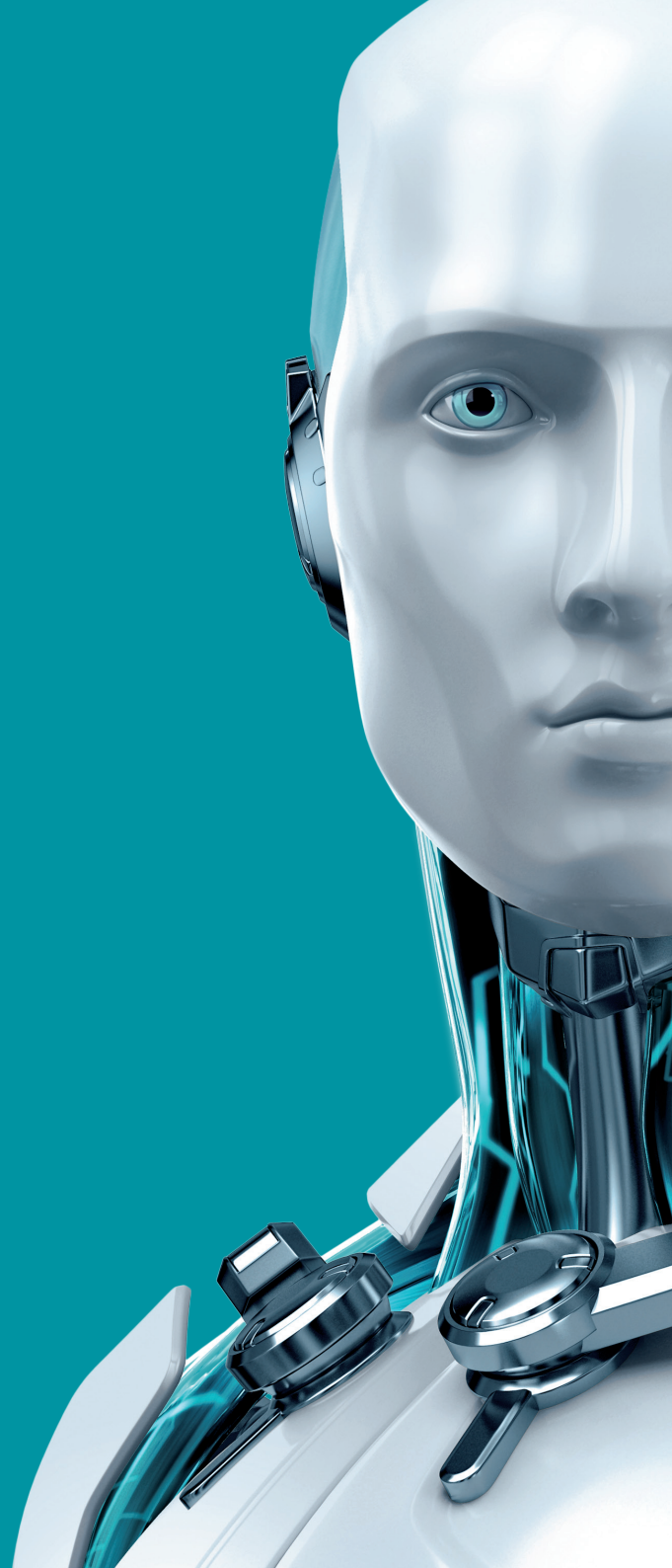
MAIL SECURITY

PARA MICROSOFT EXCHANGE SERVER

EMPRESAS

ENJOY SAFER TECHNOLOGY™



MAIL SECURITY
PARA MICROSOFT EXCHANGE SERVER

ESET Mail Security para Microsoft Exchange Server combina una protección antivirus con un antispam eficaz que garantiza el filtrado de todo el contenido malicioso en el correo electrónico a nivel del servidor. Además, el bajo consumo de recursos de ESET permite que tu servidor siga funcionando a máxima velocidad.

Con nuestro producto consigues una protección total del servidor, incluyendo el propio sistema de archivos. Puedes aplicar políticas para contenidos específicos en función del tipo de archivos y gestionar el estado de la seguridad o ajustar la configuración con la herramienta ESET Remote Administrator.

Anti-malware Protection and Antispam

Antivirus y antiespía	Elimina todo tipo de amenazas, tales como virus, rootkits, gusanos y software espía con un análisis opcional potenciado en la nube para obtener un mejor rendimiento y detección. **Análisis opcional potenciado en la nube:** Crea una lista blanca de archivos seguros utilizando la base de datos de reputación de archivos de ESET en la nube. Así, se obtiene una mayor rapidez en los análisis y se mejora la detección. Solo se enviará a la nube información sobre aplicaciones y archivos, en ningún caso se enviará información personal o confidencial, y únicamente si lo autorizas.
Antispam y Antiphishing	Bloquea el correo no deseado y los intentos de phishing con un alto nivel de detección sin necesidad de configurar manualmente el Nivel de Confianza de Spam (SCL). Después de la instalación, el módulo antispam está listo para funcionar sin necesidad de ajustar manualmente la configuración o los distintos niveles de protección.
Administración de la cuarentena local	Cada usuario de la cuenta de correo puede interactuar directamente, mediante su navegador de Internet, con el correo no deseado o los mensajes sospechosos de ser amenazas y a los que se les ha negado la entrega a la cuenta de correo. En función de los privilegios establecidos por el administrador, el usuario puede clasificar los mensajes en cuarentena, buscar en ellos y ejecutar acciones permitidas, mensaje a mensaje, o por grupo, mediante el navegador web. Las acciones varían en función del motivo por el cual fue enviado el mensaje a la cuarentena. Puede enviarse regularmente un informe por correo electrónico resumiendo los mensajes de la cuarentena con enlaces insertados para ejecutar acciones.
Análisis bajo demanda de la base de datos	Los administradores pueden elegir qué bases de datos y, en concreto, qué cuentas de correo serán analizadas. Estos análisis además se pueden limitar utilizando la modificación del sello temporal de cada mensaje para elegir qué debería analizarse, por lo que se reducen al mínimo los recursos del servidor dedicados a la tarea.
Reglas de proceso de mensajes	Las reglas de proceso de mensajes ofrecen un amplio rango de combinaciones por las que puede controlarse cada mensaje. Los parámetros evaluados incluyen campos estándar como el asunto, el remitente, el cuerpo y el encabezamiento específico del mensaje, pero también un procesamiento con condiciones avanzadas dependiendo de los filtros antispam anteriores o los resultados del análisis antivirus. Se detectan los archivos corruptos o protegidos por contraseña y se analizan internamente los archivos adjuntos para determinar el tipo real del archivo, no solo la extensión mostrada. Pueden cambiarse las reglas según las acciones deseadas.
Bloqueo de exploits	Fortalece la seguridad de aplicaciones tales como navegadores de Internet, lectores de documentos PDF, clientes de correo electrónico o componentes de MS Office, que son atacados con frecuencia. Monitoriza los procesos en busca de actividades sospechosas, típicas de los exploits. Refuerza la protección contra los ataques dirigidos y contra los ataques "zero-day".
Análisis avanzado de memoria	Monitoriza el comportamiento de todos los procesos y los analiza cuando se ejecutan en la memoria. Esto permite una prevención más efectiva contra las infecciones, incluso en el caso de que estén especialmente diseñadas para evitar su detección.
Sistema de prevención de intrusiones (HIPS)	Te permite controlar los procesos, archivos y claves de registro a través de reglas. Te protege frente a modificaciones no autorizadas y detecta las amenazas basándose en su comportamiento en el sistema.
Control de dispositivos	Bloquea el acceso de dispositivos no autorizados al servidor. Te permite crear reglas para grupos de usuarios y así cumplir con las políticas de seguridad de tu empresa. Permite el bloqueo flexible, que notifica al usuario final que el dispositivo está bloqueado, permitiéndole la opción de acceder a él, creándose un registro de la actividad.

Protección para infraestructuras complejas

Independiente de snapshots	Las actualizaciones y módulos del programa se pueden almacenar fuera de la ubicación predeterminada, para que no se vean afectados cuando se revierte la máquina virtual a un estado anterior. Como consecuencia, no tenemos que descargar las actualizaciones y módulos cada vez que revertimos una máquina y así el equipo puede utilizar estas actualizaciones intactas y evitar grandes descargas, dando como resultado un menor tiempo de recuperación de las máquinas virtuales.
Compatibilidad total para clústeres	Permite configurar el producto para que se copie automáticamente la configuración cuando se instala en entornos de clúster. Un asistente intuitivo facilita la interconexión de diversos nodos instalados de ESET Mail Security dentro de un clúster y así administrarlos como uno solo, eliminando la necesidad de copiar los cambios en la configuración de forma manual a los otros.
ESET Shared Local Cache	ESET Shared Local Cache almacena metadatos sobre los archivos ya analizados en el entorno virtual para que los archivos idénticos no sean revisados de nuevo y así acelerar el tiempo de análisis. Cuando se encuentra un archivo nuevo que no ha sido analizado, se añade automáticamente a la caché. Esto significa que los archivos ya analizados en una máquina virtual no son analizados de nuevo en otras máquinas dentro del mismo entorno virtual, acelerando mucho el tiempo de análisis. Como la comunicación ocurre en el mismo equipo físico, no se produce prácticamente retraso en el análisis, produciendo un ahorro considerable de recursos del sistema.
Instrumental de administración de Windows (WMI)	Ofrece la posibilidad de monitorizar las funcionalidades clave de ESET Mail Security a través del "Instrumental de administración de Windows". Esto permite la integración de ESET Mail Security en programas de administración de terceros y herramientas SIEM, tales como Microsoft System Center Operations Manager, Nagios y otros.

SOPORTE TÉCNICO GRATUITO EN ESPAÑOL

Cada licencia cuenta con el servicio de soporte técnico gratuito por parte de nuestros especialistas, proporcionado en español.

Requisitos del sistema

Compatible con los sistemas operativos Microsoft Windows® Server 2012 R2, 2012, 2008 R2, 2008, 2003.

Microsoft Windows® Small Business Server 2011, 2008, 2003.

Compatible con los servidores de correo Microsoft Exchange® Server 2013, 2010, 2007, 2003.

Compatible con ESET Remote Administrator 6.

Nota: no es compatible con versiones anteriores de ESET Remote Administrator.

Fácil de usar

Exclusiones de procesos	El administrador puede definir procesos para que sean ignorados por el módulo de protección en tiempo real. Todas las operaciones de archivos que pueden ser atribuidas a estos procesos con privilegios se consideran seguras. Esto es especialmente útil para procesos que a menudo interfieren con la protección en tiempo real, como las copias de seguridad o la migración a máquinas virtuales en funcionamiento. El proceso excluido puede acceder incluso a archivos u objetos potencialmente peligrosos sin activar ninguna alerta.
Actualizaciones incrementales	Las actualizaciones periódicas de firmas y módulos se descargan y aplican incrementalmente en pequeños paquetes. Con ello conseguimos utilizar menos recursos del sistema y ancho de banda de Internet sin provocar ninguna disminución destacable en la velocidad de toda la infraestructura de la red y servidores, o en la demanda de memoria o la utilización de la CPU de los equipos.
Instalación basada en componentes	Aparte de los componentes requeridos, ESET te permite elegir instalar solo aquellos componentes que necesitas: -Protección del sistema de archivos en tiempo real -Protección de la web y correo electrónico -Control de dispositivos -Interfaz gráfica de usuario (GUI) -ESET Log Collector -Y otros
Administración remota	ESET Mail Security puede ser administrado totalmente con ESET Remote Administrator. Puedes instalar el producto, ejecutar tareas, configurar políticas, recopilar registros, recibir notificaciones y obtener una supervisión general de la red de tu empresa, todo ello mediante una única consola de administración vía web.
ESET Log Collector	Es una herramienta simple que recopila todos los registros relevantes para solucionar las incidencias, con ayuda del departamento de soporte técnico de ESET, y los agrupa en un único fichero que se puede enviar por correo electrónico o subirse a una unidad de red compartida para acelerar el proceso de solución de incidencias.

Ficha v: 20170720