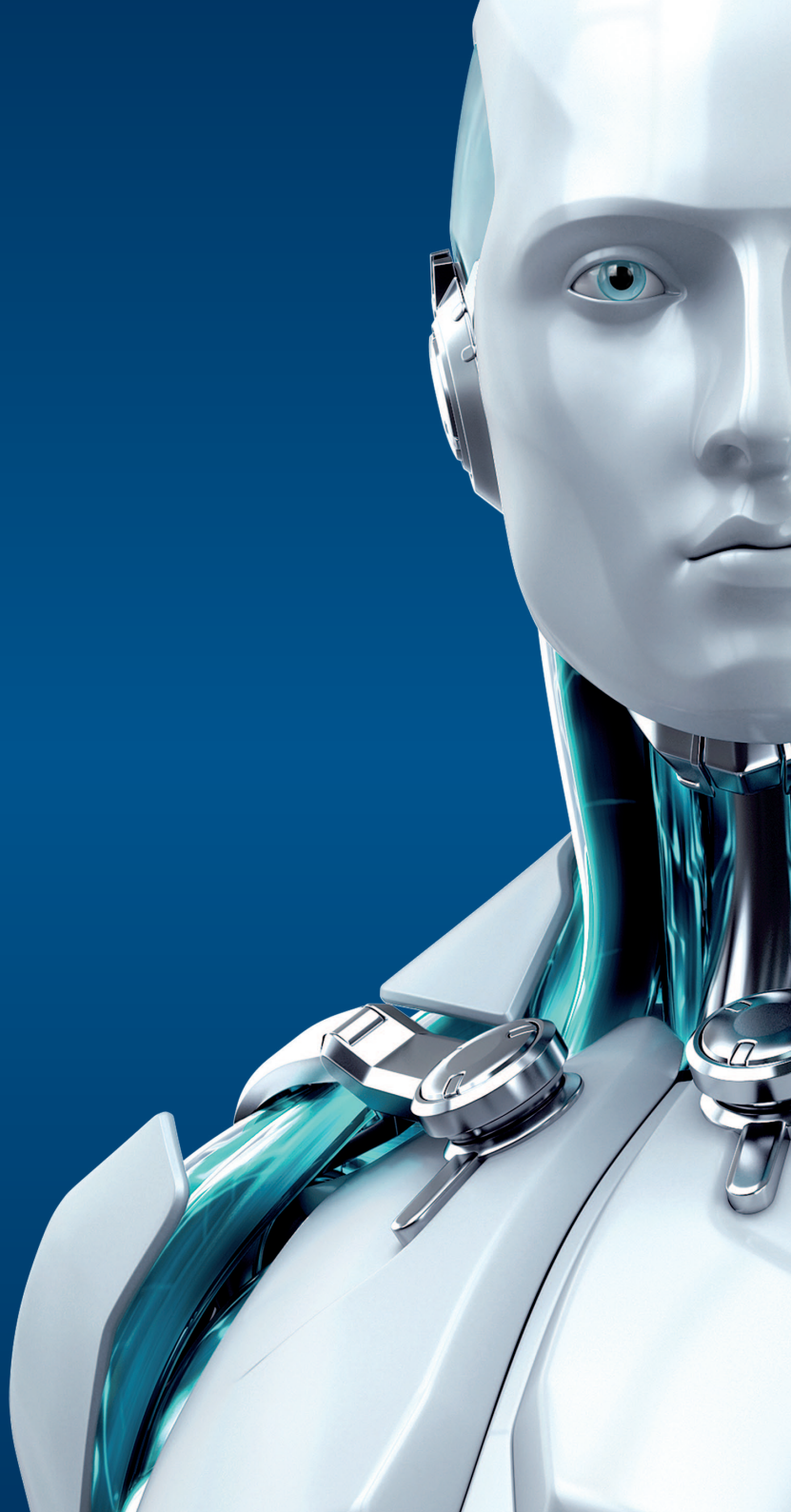
SECURITY
PARA MICROSOFT SHAREPOINT SERVER

ENJOY SAFER TECHNOLOGY™



ESET SECURITY PARA MICROSOFT SHAREPOINT SERVER

Mantiene SharePoint libre de amenazas analizando los ficheros dentro de su base de datos. Proporciona una protección totalmente integrada en el servidor.

Evita el malware y que usuarios no autorizados consigan romper la seguridad del sistema. Se puede administrar totalmente mediante ESET Remote Administrator 6.

Versiones compatibles de SharePoint:

Microsoft SharePoint Server 2016

Microsoft SharePoint Server 2013

Microsoft SharePoint Server 2010

Microsoft SharePoint Enterprise 2010

Microsoft Office SharePoint Server 2007

Protección del servidor SharePoint

Antivirus y antiespía	Elimina todo tipo de amenazas como virus, rootkits, gusanos y software espía. **Análisis potenciado en la nube opcional:** Crea una lista blanca de archivos legítimos basada en la reputación de archivos en la nube para una mejor detección y unos análisis más rápidos. Solo se envía a la nube información sobre ejecutables y ficheros y esa información no es atribuible a ningún usuario.
Análisis de la base de datos	El administrador puede decidir iniciar los análisis de la base de datos programados en las horas de menor actividad y automatizar la desinfección del equipo o forzar la inspección de varias versiones de documentos u objetos en cualquier ubicación de SharePoint. Las peticiones a la base de datos pueden dividirse en varias instancias de análisis múltiples para mejorar significativamente el tiempo de análisis bajo demanda.
Reglas de los objetos de la base de datos	Tanto para el análisis bajo demanda como para el análisis inicial, existen un conjunto de condiciones que permiten controlar los atributos, que van desde el tamaño del archivo o el contenido real del objeto analizado a la inspección del archivo, y permite una personalización ilimitada de cualquier encadenamiento deseado de reglas y las acciones a ejecutar posteriormente.
Soporte para virtualización	ESET Shared Local Cache almacena metadatos de los archivos ya analizados en el entorno virtual para que los archivos idénticos no sean analizados de nuevo y acelerar así la velocidad del análisis. Las actualizaciones de los módulos ESET y la base de firmas de virus se guardan fuera de la ubicación predeterminada, para no tener que descargarlas de nuevo cada vez que una máquina virtual es revertida a una snapshot anterior.
Bloqueo de exploits	Refuerza la seguridad de aplicaciones como navegadores web, lectores de documentos, clientes de correo electrónico o los componentes de MS Office cuyas vulnerabilidades son aprovechadas con frecuencia. Monitoriza los procesos en busca de actividades sospechosas típicas de los exploits. Refuerza la protección contra los ataques dirigidos y los exploits desconocidos, como por ejemplo los ataques zero-day.
Análisis avanzado de memoria	Monitoriza el comportamiento de los procesos maliciosos y los analiza cuando se ejecutan en la memoria. Esto permite una prevención efectiva de las infecciones, incluso de las especialmente diseñadas para evitar su detección.
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 Security para MS SharePoint 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.
Análisis de discos de almacenamiento	Te permite configurar fácilmente análisis bajo demanda de los servidores de almacenamiento de datos en red (NAS). En combinación con ESET Shared Local Cache instalado en la red, puede reducir drásticamente la cantidad de operaciones de entrada/salida en disco en las unidades en red.

Protección de acceso a la información

Detección de páginas fraudulentas	Te protege de los intentos de robo de información personal a través de páginas web fraudulentas.
Control de dispositivos	Bloquea el acceso a los equipos de tu empresa de dispositivos no autorizados tales como CD, DVD y dispositivos de almacenamiento USB. Te permite crear reglas para grupos de usuarios y así cumplir con las políticas de seguridad de tu empresa. Bloqueo flexible: notifica al usuario final que el dispositivo está bloqueado, permitiéndole la opción de acceder a él, creándose un registro de la actividad.

Opciones de análisis y actualización

Análisis en estado inactivo	No afecta al rendimiento del equipo, realizando un análisis total de forma preventiva cuando el ordenador no está siendo utilizado. Contribuye a acelerar los análisis posteriores utilizando la caché local.
Restaurar actualizaciones anteriores	Te permite volver a una versión previa de los módulos de protección y de la base de firmas de virus. Puedes detener las actualizaciones cuando desees, elegir una versión previa de forma temporal o posponer las actualizaciones hasta que se cambie manualmente.
Diferentes tipos de actualización	Permite la opción de descargar las actualizaciones desde tres tipos de servidores de actualización: antes del lanzamiento de la actualización (para usuarios beta), actualización estándar (recomendado para equipos que no son críticos) y actualización pospuesta (recomendado para equipos críticos en la empresa. Se actualizará aproximadamente doce horas después del lanzamiento estándar de la actualización).
Servidor local de actualizaciones	Ahorra ancho de banda descargando las actualizaciones solo una vez a un servidor "mirror" local. Los dispositivos móviles se actualizan directamente desde los servidores de ESET cuando el "mirror" local no está disponible. Soporta la actualización por protocolo seguro (HTTPS).

SOPORTE TÉCNICO GRATUITO EN ESPAÑOL

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

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.
Instrumental de administración de Windows (WMI)	Ofrece la posibilidad de monitorizar las funcionalidades clave de ESET Server Security a través del "Instrumental de administración de Windows". Esto permite la integración de ESET Server Security en programas de administración de terceros y herramientas SIEM, tales como Microsoft System Center Operations Manager, Nagios y otros.
Vista personalizable de la interfaz gráfica	La vista de la interfaz gráfica de usuario (GUI) que se le muestra al usuario puede establecerse como: completa, mínima, manual o silenciosa. El producto ESET puede hacerse totalmente invisible para el usuario final, incluyendo la opción de ocultar el icono de la barra de tareas o las ventanas de notificación. Ocultando totalmente la interfaz gráfica de usuario, el proceso "egui.exe" no se ejecuta en absoluto, lo cual da como resultado un menor consumo de recursos del producto ESET.
Instalación basada en componentes	Te permite elegir qué componentes instalar: -Protección del sistema de archivos en tiempo real. -Web y correo electrónico. -Control de dispositivos. -Interfaz gráfica de usuario (GUI). -ESET Log Collector. -ESET SysInspector. -Ayuda sin conexión a Internet.
Administración remota	Las soluciones ESET para servidores se pueden administrar totalmente mediante la herramienta 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:20161006