



ENDPOINT SECURITY

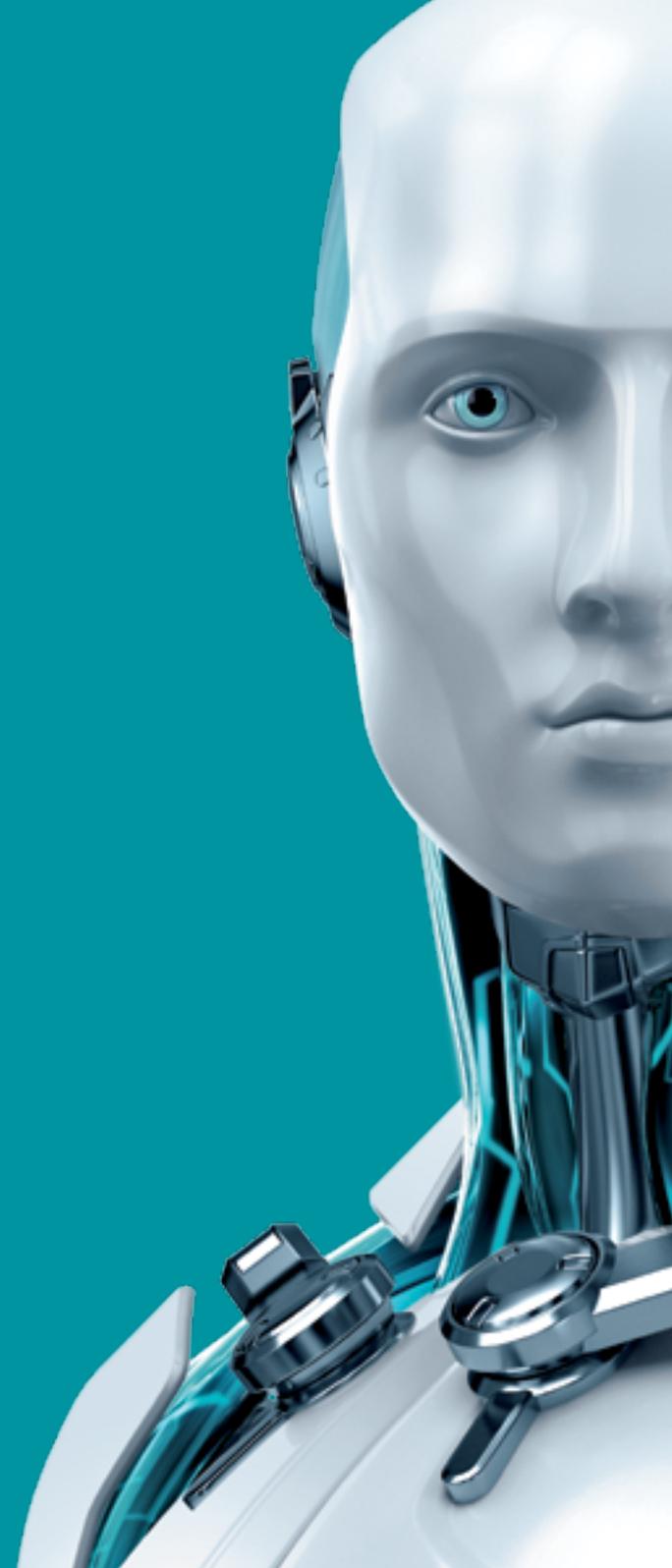
PARA WINDOWS

30

30 AÑOS DE
INNOVACIÓN
CONTINUA EN
SEGURIDAD



ENJOY SAFER TECHNOLOGY™





ENDPOINT SECURITY PARA WINDOWS

ESET Endpoint Security proporciona seguridad integral de TI para su empresa a través de múltiples capas de protección, entre las que se incluyen nuestra comprobada tecnología de detección ESET NOD32®, protección completa del acceso a los datos, y opciones de exploración y de actualización que se pueden ajustar en su totalidad.

Mantenga el rendimiento de su equipo al máximo gracias a la baja demanda de recursos del sistema, al soporte para la virtualización y a la exploración opcional basada en la nube.

Además, supervise todo sin esfuerzo con nuestra herramienta de administración remota, totalmente rediseñada y fácil de usar.

Protección para Endpoints

Antivirus & Antispyware

Elimina todos los tipos de amenazas, incluyendo virus, rootkits, gusanos y spyware.

Exploración opcional basada en la nube:

Creación de 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 de archivos comprimidos; el envío se realiza en forma anónima.

Soporte para virtualización

La Caché local compartida de ESET almacena metadatos sobre los archivos ya explorados dentro de cada entorno virtual con la finalidad de no volver a explorar los archivos idénticos nuevamente y, de esa forma, acelerar la velocidad de exploración.

Las actualizaciones de los módulos y de la base de datos de firmas de virus de ESET se almacenan fuera de la ubicación predeterminada, por lo tanto no se deben descargar cada vez que el estado de la máquina virtual se revierte a la instantánea predeterminada.

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.

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 los objetivos de ataque más comunes. 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, es decir, ataques zero-day.

Exploración avanzada de memoria

Monitorea la conducta de los procesos maliciosos y los explora cuando se muestran en memoria. Así se logra una prevención efectiva contra las infecciones, incluso ante los tipos más furtivos de malware.

Antispam del cliente

Filtra el spam y lo elimina, mientras explora los correos electrónicos entrantes en busca de malware. Soporte nativo para Microsoft Outlook (POP3, IMAP, MAPI).

Protección para múltiples plataformas

Las soluciones de seguridad de ESET para Windows son capaces de detectar amenazas para Mac OS y viceversa, de modo que suministran una mejor protección en entornos de plataformas múltiples.

Protección del acceso a los datos

Control Web	Limita el acceso a los sitios Web por categoría, por ej., juegos, redes sociales, compras, entre otros. Permite crear reglas para grupos de usuarios para cumplir con las normativas y políticas corporativas. Notifica al usuario final el bloqueo del sitio Web y da la opción de acceder pero registrando la actividad.
Anti-Phishing	Protege a los usuarios finales de los sitios Web falsos que intentan obtener información confidencial, como nombres de usuario, contraseñas o detalles bancarios y de tarjetas de crédito.
Firewall Bidireccional	Impide el acceso no autorizado a la red corporativa. Ofrece protección ante criminales informáticos y previene la exposición de datos. Le permite definir las redes de confianza y configura en forma predeterminada todas las demás conexiones (por ej., las conexiones a redes Wi-Fi públicas) en modo de seguridad "estricta". El asistente para la resolución de problemas lo guía a través de una serie de preguntas para identificar las reglas problemáticas o mismo para ayudarlo a crear reglas nuevas.
Protección contra vulnerabilidades	Mejora la detección de las Vulnerabilidades y Exposiciones Comunes (CVE) en los protocolos más utilizados, como SMB, RPC y RDP. Brinda protección contra las vulnerabilidades para las cuales aún no se publicó o desarrolló la revisión.
Protección ante botnets	Protege ante las infiltraciones por malware de tipo botnet, previniendo el envío de spam y evitando que se lleven a cabo ataques de red desde la endpoint.
Control de dispositivos	Bloquea el acceso al sistema para los dispositivos no autorizados (unidades de CD, DVD y USB). Permite crear reglas para grupos de usuarios para cumplir con las normativas y políticas corporativas. Notifica el bloqueo del dispositivo y da la opción de acceder pero registrando la actividad.

Opciones de exploración y actualización

Módulo de exploración en estado inactivo	Realiza las exploraciones completas en forma proactiva mientras el equipo no está en uso. Llena la caché local y ayuda a acelerar las exploraciones futuras.
Primera exploración tras la instalación	Suministra la opción de ejecutar una exploración bajo demanda de baja prioridad 20 minutos después de la instalación del programa, lo que asegura que el sistema esté protegido desde el comienzo.
Reversión de la actualización	Revierte el sistema a una versión previa de módulos de protección y de la base de datos de virus. Permite congelar las actualizaciones como lo desee: elija hacer una reversión temporal o demorar las actualizaciones hasta su modificación manual.
Actualizaciones postergadas	Permite realizar descargas desde 3 servidores especializados: actualizaciones previas a su lanzamiento (usuarios de versión beta), lanzamientos regulares (para sistemas no críticos) y lanzamientos postergados (para los sistemas críticos de empresas; 12 horas después del lanzamiento regular).
Servidor de actualización local	Ahorra el ancho de banda de la empresa, al descargar las actualizaciones una sola vez a un servidor local. Los usuarios móviles actualizan sus dispositivos desde el servidor de actualización de ESET cuando el mirror local no está disponible. Cuenta con soporte para canales de comunicación seguros (HTTPS).



SOPORTE
TÉCNICO
GRATUITO Y EN
IDIOMA LOCAL.

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

Usabilidad

RIP & Replace	<p>Durante la instalación de ESET Endpoint Solutions, la solución detecta si hay otros programas de seguridad y los desinstala.</p> <p>Es compatible con sistemas de 32 y de 64 bits.</p>
Visibilidad personalizable de la interfaz gráfica del usuario	<p>La visibilidad de la interfaz gráfica del usuario (GUI) en los equipos de los usuarios finales puede configurarse en: Completa, Mínima, Manual o Silenciosa.</p> <p>Es posible hacer que la solución de ESET sea totalmente invisible para el usuario final, incluyendo la eliminación del ícono en la bandeja y de las ventanas de notificaciones.</p> <p>Al ocultar la GUI por completo, el proceso "egui.exe" directamente no se ejecuta; esto genera que la solución de ESET consuma aún menos recursos del sistema.</p>
ESET License Administrator	<p>Permite el manejo de todas las licencias en forma transparente, desde un mismo lugar, a través de un navegador Web. Podrá combinar, delegar y administrar todas las licencias de manera centralizada en tiempo real, incluso aunque no esté usando ESET Remote Administrator.</p>
Soporte para pantallas táctiles	<p>Ofrece compatibilidad con pantallas táctiles y permite la visualización en pantallas de alta resoluciones. Más márgenes y reorganización completa de los elementos de la GUI.</p> <p>Acceso a las acciones básicas utilizadas con mayor frecuencia desde el menú en la bandeja.</p>
Bajo impacto en el sistema	<p>Ofrece protección comprobada a la vez que deja disponibles más recursos del sistema para los programas que los usuarios finales ejecutan con más frecuencia.</p> <p>Puede desplegarse en máquinas más viejas sin necesidad de actualizarlas, por lo que ayuda a extender la vida útil del hardware.</p> <p>El modo de alimentación a batería conserva la vida de la batería en equipos portátiles que se usan fuera de la oficina..</p>
Soporte para idiomas de derecha a izquierda	<p>Soporte nativo para idiomas de derecha a izquierda (por ej., árabe), garantizando la utilidad óptima para el usuario final.</p>
Administración remota	<p>Las soluciones ESET Endpoint Solutions pueden administrarse en su totalidad desde ESET Remote Administrator.</p> <p>Haga el despliegue, ejecute tareas, determine políticas, recopile registros y obtenga notificaciones e información general de la seguridad de la red: todo a través de una única consola de administración basada en la Web.</p>

Copyright © 1992 – 2017 ESET, spol. s r. o. ESET, el logotipo de ESET, la imagen del androide de ESET, NOD32, ESET Smart Security, SysInspector, ThreatSense, ThreatSense. Net, LiveGrid, el logotipo y/u otros productos mencionados de ESET, spol. s r. o., son marcas comerciales registradas de ESET, spol. s r. o. Windows® es una marca comercial del grupo de empresas Microsoft. Las demás empresas o productos aquí mencionados pueden ser marcas comerciales registradas de sus propietarios. Producido conforme a los estándares de calidad ISO 9001:2008.