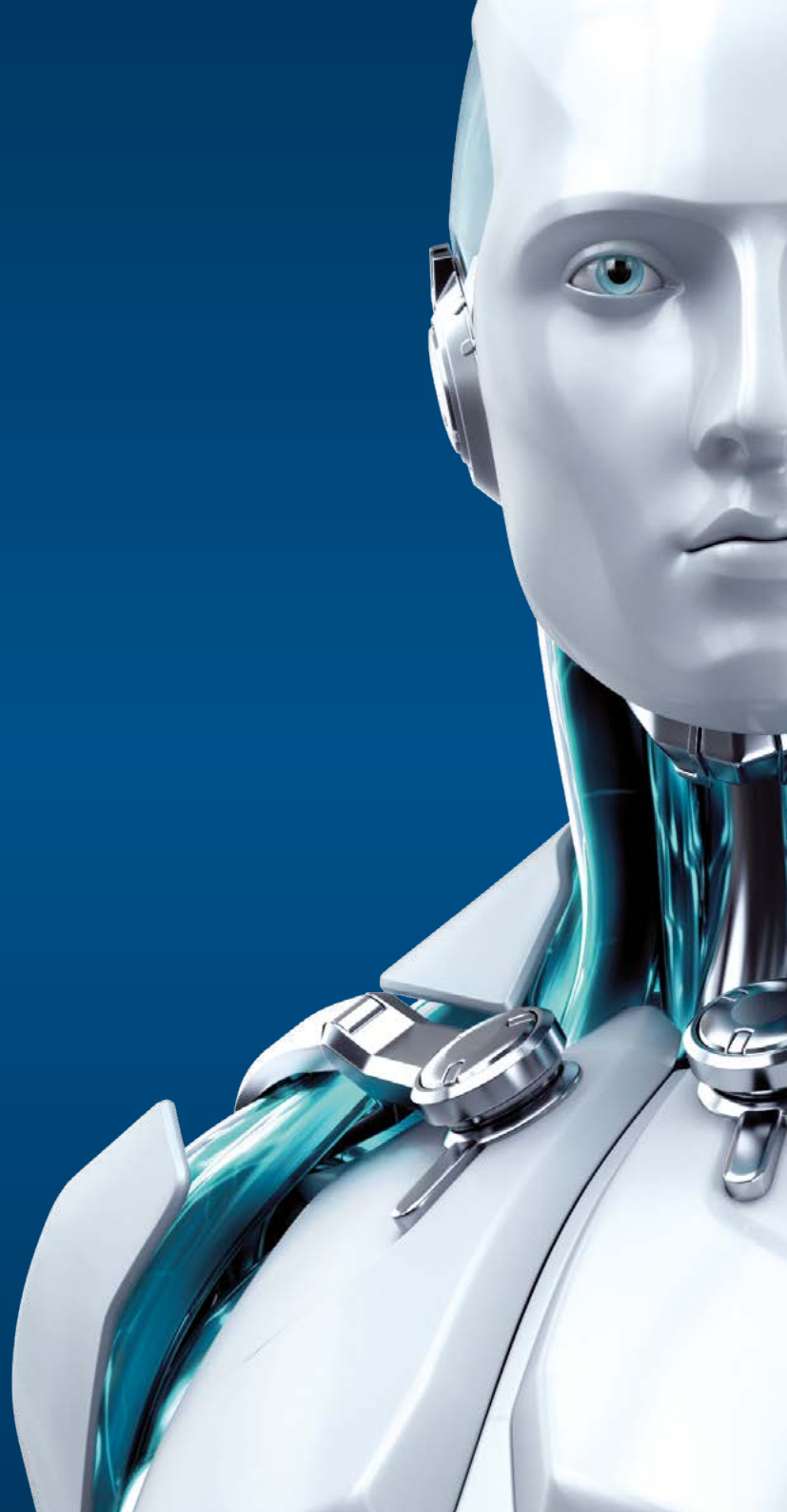
ENDPOINT SECURITY

PARA ANDROID



ENJOY SAFER TECHNOLOGY™

ENDPOINT SECURITY
PARA ANDROID

ESET Endpoint Security para Android protege la flota móvil de su empresa con la tecnología proactiva ESET NOD32®.

Explora todas las aplicaciones, los archivos y las tarjetas de memoria en busca de malware. El sistema Anti-Theft protege los dispositivos físicos, permitiendo bloquearlos o borrar su contenido en forma remota si se pierden o se los roban. Los usuarios dejan de recibir llamadas y mensajes de SMS no deseados, y los administradores pueden impulsar políticas de seguridad a todos los dispositivos para asegurar el cumplimiento de normativas.

Protección de endpoints

Protección en tiempo real	Protege todas las aplicaciones y los archivos en tiempo real con la tecnología proactiva ESET NOD32®, optimizada para plataformas móviles. El sistema integrado de recolección de malware, ESET LiveGrid®, junto con la exploración avanzada, protegen los smartphones y las tabletas corporativas ante todas las amenazas.
Exploración bajo demanda	Proporciona la exploración y la desinfección confiables de la memoria integrada y de los medios intercambiables. La exploración se ejecuta en segundo plano y el usuario puede ponerla en pausa. También es posible programar la hora exacta para ejecutar una exploración.
Exploración durante la carga de la batería	Permite realizar la exploración completa fuera de las horas de mayor actividad, cuando el dispositivo se está cargando y la pantalla se encuentra bloqueada.
Anti-Phishing	Protege a los usuarios de los sitios Web falsos que intentan extraer contraseñas, información bancaria y otros datos confidenciales.
Protección ante la desinstalación	Impide que se desinstale la aplicación móvil a menos que se de la contraseña de administrador.
Filtrado de SMS y llamadas	Protege a los usuarios de las llamadas y los mensajes de SMS no deseados* provenientes de números ocultos, contactos o números telefónicos seleccionados, o durante períodos predefinidos.
	*Debido a los cambios que Google realizó en el sistema operativo Android (desde la versión 4.4 Kitkat), la funcionalidad de bloqueo de SMS no estará disponible.

Seguridad del dispositivo

Le proporciona al administrador opciones para ejecutar políticas de seguridad básicas en toda la flota de dispositivos móviles. La aplicación les notifica automáticamente al usuario y al administrador si la configuración actual del dispositivo no cumple con las políticas de seguridad corporativas y sugiere los cambios de configuración que se deberían hacer para remediarlo.

Configuración de la seguridad del dispositivo	Definir los requisitos sobre la complejidad de las contraseñas Establecer una cantidad máxima de intentos de desbloqueo tras la cual el dispositivo entrará automáticamente en la configuración de fábrica Establecer un vencimiento para el código de bloqueo de pantalla Establecer un temporizador para el bloqueo de pantalla Indicar a los usuarios que cifren el contenido de sus dispositivos móviles Bloquear el uso de la cámara integrada

Política de configuración de dispositivos: le permite al administrador monitorear la configuración predefinida del dispositivo para determinar si cumple con las normativas. Los administradores cuentan con la capacidad de supervisar el uso de la memoria, las conexiones Wi-Fi, el roaming de datos, el roaming de llamadas, las fuentes desconocidas (que no sean de la tienda Google Play), el modo de depuración de dispositivos USB, las transacciones NFC y el estado actual del dispositivo.

Anti-Theft

Activación por Comandos	Le permite al administrador accionar todos los comandos remotos desde ESET Remote Administrator, ya sea a través de un SMS con un código de verificación en dos fases o directamente desde la interfaz del producto en el equipo del administrador. Es de especial utilidad para empresas que no usan la administración remota o cuando el administrador se encuentra fuera de la oficina.
Bloqueo Remoto	Bloquea en forma remota los dispositivos perdidos o robados. Luego del bloqueo, ninguna persona sin autorización podrá acceder a los datos almacenados en el dispositivo. Una vez que se recupera el dispositivo, se envía un comando remoto de desbloqueo que lo habilita nuevamente para su uso.
Localización Remota	Encuentra remotamente el teléfono y rastrea sus coordenadas de GPS.
Borrado Remoto	Elimina en forma segura todos los contactos, los mensajes y los datos almacenados en la memoria interna del dispositivo, así como en las tarjetas de memoria extraíbles. El procedimiento de desinfección avanzada asegura que no sea posible restaurar ninguna parte de la información borrada. Tras el borrado remoto, ESET Endpoint Security para Android permanece instalado en el dispositivo, por lo que aún es posible ejecutar cualquier otro comando de Anti-Theft.
Alarma Remota	Al activarse, suena una alarma en el dispositivo, incluso aunque el volumen esté en silencio. Al mismo tiempo, el dispositivo perdido se bloquea automáticamente.
Restablecimiento remoto de la configuración predeterminada de fábrica	Elimina todos los datos en el dispositivo a los que se puede tener acceso; para ello, se destruyen todos los encabezados de los archivos y se restablece la configuración predeterminada de fábrica.
Mensaje personalizado	El administrador puede enviar un mensaje personalizado a un dispositivo determinado o a un grupo de dispositivos. El mensaje se muestra como si fuera una ventana emergente, por lo que el usuario no podrá pasarla por alto.
Información sobre el bloqueo de pantalla	El administrador puede definir un mensaje personalizado (nombre de la empresa, dirección de correo electrónico, frase) para que se muestre incluso cuando el teléfono se encuentra bloqueado. De esta manera, quien haya encontrado el teléfono podrá llamar a un número predefinido.
Tarjeta SIM de confianza	Cuando se inserta una tarjeta SIM no autorizada, el dispositivo se bloquea automáticamente y se envía la información sobre la tarjeta al administrador.
Contactos de administradores	Contiene una lista con los números telefónicos de los administradores, protegida por una contraseña de administrador. Los comandos de SMS que se usan para controlar los dispositivos solo pueden enviarse desde estos números de confianza. Asimismo, se usan estos números cuando hay que enviar notificaciones relacionadas con las acciones del Anti-Theft.

SOPORTE TÉCNICO GRATUITO LOCAL.

Haga más con la ayuda de nuestros especialistas.

Soporte técnico disponible cuando lo necesita, en su idioma.

Control de aplicaciones

Les ofrece a los administradores la opción de monitorear las aplicaciones instaladas, de bloquear el acceso a aplicaciones definidas y de indicarles a los usuarios que deben desinstalar determinadas aplicaciones.

Configuración del control de aplicaciones	Permite definir manualmente las aplicaciones que se van a bloquear. Bloqueo basado en categorías: por ej., juegos, medios sociales, etc. Bloqueo basado en permisos: por ej., aplicaciones que rastrean la ubicación, que acceden a la lista de contactos, etc. Bloqueo según la fuente: aplicaciones instaladas desde otras fuentes que no sean las tiendas predeterminadas de descarga de aplicaciones móviles. Establece excepciones para las reglas de bloqueo de aplicaciones: lista blanca de aplicaciones. Establece una lista de las aplicaciones instaladas que son obligatorias.
Auditoría de aplicaciones	Rastrea las aplicaciones y sus accesos a los datos personales y corporativos organizádolas por categorías, lo que le permite al administrador monitorear y controlar los accesos de las aplicaciones.

Usabilidad y administración

Importar o exportar la configuración	Si los dispositivos móviles no se administran desde ESET Remote Administrator, el administrador puede compartir la configuración de un dispositivo móvil a otro exportándola a un archivo e importándola en cualquier dispositivo donde se ejecute la aplicación cliente.
Centro de notificaciones	El usuario puede acceder a todas las notificaciones que requieran atención desde un mismo lugar, así como obtener la información necesaria para resolver el problema. Esto ayuda al usuario a cumplir con las normas corporativas.
Administración local	El administrador puede configurar y administrar el dispositivo en forma local si la empresa no usa ESET Remote Administrator. Todas las configuraciones de la aplicación están protegidas por una contraseña de administrador, lo que mantiene a la aplicación bajo el control completo del administrador todo el tiempo.
Identificación mejorada de dispositivos	Durante el proceso de registro de nuevos dispositivos, los teléfonos móviles se incluyen en una lista blanca para que solo los dispositivos autorizados puedan conectarse con ESET Remote Administrator. Esto simplifica la identificación individual de los dispositivos: por nombre, descripción y código IMEI.
Asistentes de configuración	Los asistentes para configuraciones posteriores a la instalación inicial están disponibles para funcionalidades seleccionadas, lo que simplifica todo el proceso cuando la configuración del dispositivo se implementa localmente.
Administración remota	Las endpoints con ESET pueden administrarse totalmente desde ESET Remote Administrator. 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.
ESET License Administrator	Le permite manejar 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.