Características clave de ESET PROTECT Advanced

Protección para Endpoint con la siguiente tecnología:

Característica	Descripción
Plataforma de administración Cloud y/o OnPermise	ESET PROTECT Cloud le permite administrar desde una ubicación central los productos ESET en estaciones de trabajo y servidores en un entorno de red con hasta 25.000 dispositivos desde una ubicación central. A través de la consola web de consola web de ESET PROTECT Cloud, puede implementar soluciones ESET, gestionar tareas, aplicar políticas de seguridad, controlar el estado del sistema y responder rápidamente a problemas o amenazas en equipos remotos Adicional, se encuentra disponible la consola ESET PROTECT OnPermise, esta aplicación le permite administrar los productos ESET en estaciones de trabajo del cliente, servidores y dispositivos móviles en un entorno dentro de una red desde una ubicación central. Con el sistema de administración de tareas integrado de ESET PROTECT, puede instalar las soluciones de seguridad de ESET en equipos remotos y responder rápidamente a problemas y detecciones nuevos.
Protección contra ataques de fuerza bruta	Como parte de la protección contra ataques de red, la protección contra ataques por fuerza bruta inspecciona el contenido del tráfico de red y bloquea los intentos de ataques para adivinar contraseñas. Se realiza un seguimiento de los intentos reiterados con la dirección IP de origen, y se crea una entrada de registro en la Lista negra de direcciones IP temporales, que ayuda a supervisar la situación Después de un período de tiempo determinado, la dirección IP de origen que funciona incorrectamente puede quitarse de la lista negra si la conexión es legítima Configurable en redes de gran tamaño
Bloqueador de exploits (Exploit Blocker)	Bloqueador de exploits está diseñado para fortalecer diferentes tipos de aplicaciones comúnmente explotadas como los navegadores web, los lectores de PDF, los clientes de correo electrónico y los componentes de Microsoft Office. Funciona controlando el comportamiento de los procesos en busca de actividad sospechosa que puede indicar un exploit. Cuando el Bloqueador de exploits identifica un proceso sospechoso, lo detiene inmediatamente y registra y envía los datos de la amenaza al sistema de nube ESET LiveGrid®. El laboratorio de investigación de ESET procesa los datos y los utiliza para proteger mejor a los usuarios frente a amenazas desconocidas y ataques de día cero (malware recientemente lanzado para el que no hay una solución configurada previamente).
Bloqueador de exploits de Java	El Bloqueador de exploits de Java es una extensión de la tecnología existente del Bloqueador de exploits. Controla Java y busca comportamientos similares a los exploits. Las muestras bloqueadas pueden informarse a analizadores de malware, para que puedan crear firmas para bloquearlos en diferentes capas (bloqueo de URL, descarga de archivo, etc.).
	Desde 1990, ESET trabaja con algoritmos de aprendizaje automático para detectar y bloquear amenazas. En 1998, se incorporaron redes neurales al motor de detección del producto ESET.

Aprendizaje automático	El aprendizaje automático incluye detecciones de AND, en las que se usan modelos basados en el aprendizaje automático para trabajar de manera efectiva con o sin conexión a la nube. Asimismo, los algoritmos de aprendizaje automático son una parte fundamental del orden inicial y de la clasificación de muestras entrantes, así como de su ubicación en el "mapa de seguridad cibernética" imaginario. ESET ha desarrollado su propio motor de aprendizaje automático interno. Usa el poder combinado de las redes neurales (como aprendizaje profundo y memoria extendida a corto plazo) y un grupo seleccionado en forma manual de seis algoritmos de clasificación. Esto le permite generar un resultado consolidado y contribuye a etiquetar correctamente la muestra entrante como limpia, potencialmente no deseada o maliciosa.
Protección contra ataques de red (IDS)	La protección contra ataques de red es una extensión del firewall personal que mejora la detección de explotaciones de vulnerabilidades conocidas al nivel de la red. La implementación de detecciones de explotaciones comunes en protocolos ampliamente usados como SMB, RPC y RDP, constituye otra capa importante de protección contra creciente malware, ataques dirigidos por la red y explotaciones de vulnerabilidades para las que aún no se ha lanzado o implementado una revisión.
Protección contra Ransomware (Ransomware Shield)	La Protección contra ransomware es una detección basada en el comportamiento del equipo y supervisa el comportamiento de las aplicaciones y los archivos de la manera en que suele hacerse para el ransomware o los codificadores de archivos. Si el comportamiento de una aplicación se considera malicioso o la exploración basada en reputación demuestra que una aplicación es sospechosa, se bloquea la aplicación y se detiene el proceso o se pide al usuario que la bloquee o admita.
Protección contra ataques basados en script	La protección contra ataques basados en script consta de una protección contra javascript en navegadores web y la protección contra Antimalware Scan Interface (AMSI) contra scripts en Powershell.
ESET LiveGrid	ESET LiveGrid® (creada en el sistema avanzado de alerta temprana ESET ThreatSense.Net) utiliza los datos que los usuarios de ESET enviaron de todo el mundo y los envía al laboratorio de investigación de ESET. Al proporcionar muestras sospechosas y metadatos from the wild, ESET LiveGrid® nos permite reaccionar inmediatamente ante las necesidades de nuestros clientes y mantener a ESET receptivo a las últimas amenazas. Los investigadores de malware de ESET usan la información para crear una instantánea precisa de la naturaleza y el alcance de amenazas globales, lo que nos ayuda a concentrarnos en los objetivos correctos. Los datos de ESET LiveGrid® tienen un rol importante al establecer las prioridades en nuestro procesamiento automático. Además, implementa un sistema de reputación que ayuda a mejorar la eficiencia general de nuestras soluciones antimalware. Un usuario puede verificar la reputación de los procesos y archivos en ejecución directamente desde la interfaz del programa o el menú contextual con información adicional disponible en ESET LiveGrid®. Cuando se inspecciona un archivo ejecutable en el sistema de un usuario, su etiqueta hash primero se compara con una base de datos de elementos de lista blanca y negra. Si se encuentra en la lista blanca, el archivo inspeccionado se considera limpio y también se lo marca para excluirlo en futuras exploraciones. Si se encuentra en la lista negra, se toman las medidas correspondientes en función de la naturaleza de la amenaza. Si no hay coincidencia, se explora el archivo completamente. En función de los resultados de la exploración, los archivos se clasifican como amenazas o no amenazas. Este enfoque tiene un impacto

	significativamente positivo en el rendimiento de la exploración. Este sistema de reputación permite la detección efectiva de muestras de malware incluso antes de proporcionar sus firmas al equipo del usuario mediante una base de datos de virus actualizada (algo que sucede varias veces al día).
Protección contra Botnet	La protección contra Botnet descubre malware explorando sus patrones y protocolos de comunicación de red. El malware Botnet cambia frecuentemente en contraste con los protocolos de red, que no han cambiado en los últimos años. Esta nueva tecnología ayuda a ESET a vencer el malware que intenta evitar la detección e intenta conectar su equipo con una red botnet.
UEFI Scanner	La exploración de interfaz de firmware extensible unificada (UEFI) es parte del sistema de prevención de intrusiones basado en el host (HIPS) que protege al firmware UEFI en su equipo. El firmware UEFI se carga en la memoria al comienzo del proceso de inicio. El código está en un chip de memoria flash soldado en la placa principal. Al infectarlo, los atacantes pueden implementar malware que sobrevive a las reinstalaciones y reinicios del sistema. El malware también puede pasar desapercibido fácilmente con soluciones antimalware, ya que la mayoría de ellos no explora esta capa.
Navegador seguro	Navegador seguro es una capa de protección adicional diseñada para proteger sus datos confidenciales durante la navegación en línea (por ejemplo, datos financieros durante transacciones en línea). ESET Endpoint Security 8 y posteriores contiene una lista incorporada de sitios web predeterminados que harán que se abra un navegador protegido. Puede agregar un sitio web o editar la lista de sitios web dentro de la configuración del producto. El navegador seguro se desactiva de manera predeterminada luego de la instalación.
Exploración de memoria avanzada	Exploración de memoria avanzada trabaja en conjunto con el bloqueador de exploits para fortalecer la protección contra malware diseñado para evadir la detección por los productos antimalware con el uso de ofuscación o cifrado. En los casos en los que la emulación o la heurística ordinarias no detecten una amenaza, la exploración de memoria avanzada puede identificar un comportamiento sospechoso y buscar amenazas cuando se manifiestan en la memoria del sistema. Esta solución es efectiva contra malware severamente ofuscado. A diferencia del bloqueador de exploits, la exploración de memoria avanzada es un método posterior a la ejecución, lo que significa que existe un riesgo de que se haya realizado alguna actividad maliciosa antes de la detección de una amenaza; sin embargo en caso de que hayan fallado otras técnicas de detección, ofrece una capa adicional de seguridad.
Sistema de prevención de intrusiones basado en el host (HIPS)	El Sistema de prevención de intrusiones basado en el host (HIPS) protege su sistema contra malware y actividades no deseadas que intentan perjudicar el equipo. El sistema HIPS utiliza el análisis avanzado de conducta combinado con las capacidades de detección del filtrado de red para monitorear los procesos activos, los archivos y las claves de registro. El HIPS es independiente de la protección del sistema de archivos en tiempo real y no es un firewall; solo monitorea los procesos activos en el sistema operativo.

Las siguientes tecnologías son productos incluidos dentro de ESET PROTECT Advanced adicionales a la protección para Endpoint:

Tecnología	Descripción
ESET Full Disk Encryption	ESET Full Disk Encryption (EFDE) es una función, que opera como complemento, propia de las consolas de administración remota de ESET: ESET Security Management Center y ESET PROTECT Cloud. La característica principal de EFDE es la administración del cifrado de disco completo de las estaciones de trabajo administradas de Windows y las estaciones de trabajo macOS, con una capa de seguridad adicional en el inicio de sesión de prearranque. EFDE es totalmente compatible con ESET Security Management Center, ESET PROTECT y con funciones de ESET PROTECT Cloud, como los grupos, las políticas, las tareas y los informes. EFDE utiliza tecnología patentada para proteger los datos de empresas de todos los tamaños. ESET Full Disk Encryption está validado por 140-2 con cifrado AES de 256 bit. Adicional, el administrador puede establecer atributos de contraseña obligatorios, número de reintentos de contraseñas y período de vencimiento. Desde una configuración de política, es posible otorgar a un usuario la opción de cambiar su contraseña cuando lo desee.
ESET LiveGuard Advanced	ESET LiveGuard Advanced (sandbox en la nube) es un servicio que proporciona ESET. Su finalidad es agregar una capa de protección diseñada específicamente para paliar las amenazas nuevas. Las muestras sospechosas que aún no se han confirmado como maliciosas y pueden incluir malware se envían automáticamente a la nube de ESET. Las muestras enviadas se ejecutan en un entorno aislado y nuestros motores de detección de malware avanzados las evalúan. Las muestras maliciosas y los mensajes de correo electrónico no deseado sospechosos se envían a ESET LiveGrid®. Los archivos adjuntos de correo electrónico se gestionan de forma independiente y pueden enviarse a ESET LiveGuard Advanced. Los administradores o los usuarios pueden definir el alcance de los archivos que se envían y el periodo de retención del archivo en la nube de ESET. ESET LiveGuard Advanced utiliza cuatro capas de detección independientes para garantizar la máxima velocidad de detección. Cada capa utiliza un enfoque diferente y da su veredicto sobre la muestra. La evaluación final es el resultado de toda la información sobre la muestra. Consulte la descripción general del proceso a continuación: https://help.eset.com/elga/es-ES/index.html?how_detection_layers_work.html