Características clave de ESET PROTECT Entry

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 **50,000** 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.).

Aprendizaje automático (Machine Learning)	**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. 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.
Control Web	La sección Control Web permite configurar las opciones que protegen a su empresa del riesgo de responsabilidad legal. El Control Web puede regular el acceso a sitios Web que violan los derechos de propiedad intelectual. El objetivo es prevenir que los empleados accedan a páginas con contenido inapropiado o perjudicial o páginas que puedan tener un impacto negativo en la productividad.
Firewall bidireccional	El firewall controla todo el tráfico de red que sale del sistema y que ingresa a él. Para ello, permite o deniega las conexiones de red individuales según las reglas de filtrado especificadas. Brinda protección frente a ataques desde equipos remotos y bloquea ciertos servicios potencialmente amenazantes.
Tecnología Intel® Threat Detection	La **Tecnología Intel® Threat Detection** añade una **capa de detección, asistida por hardware**, para soluciones de seguridad, subiendo la barrera contra amenazas avanzadas. La Tecnología Intel® Threat Detection es una característica clave de la plataforma Intel que permite el perfilamiento y la detección a través de todo el stack del dispositivo. Los productos ESET incluyen una protección de ransomware mejorada usando la Tecnología Intel® Threat Defense en la siguiente lista de procesadores:
Detección y Respuesta automatizada	Mediante la plataforma de administración de ESET PROTECT podemos automatizar la ejecución de tareas a consecuencia de algún evento o característica en el Endpoint, por ejemplo, **Aislar el equipo de la red** si se detecta algún comportamiento de **Ransomware.** Otra característica clave de la plataforma de ESET PROTECT es poder identificar cada Endpoint de acuerdo a sus características (Hardware, Software, estado del producto o del sistema operativo, etc.) y de acuerdo a esto detonar la ejecución de distintas tareas automáticamente (Escaneos completos, apagar o reiniciar el Endpoint, actualizar, activar, etc.), o bien, asignar un perfil de políticas específico en la configuración del Antimalware.
Informes	Mediante la plataforma de ESET PROTECT podemos automatizar el envío de distintos reportes acerca de los Endpoints, por ejemplo: - Inventario de Hardware - Inventario de Software - Detecciones activas - Endpoints con más detecciones por semana - Reporte de versión de producto de todo el ambiente ESET

	- Endpoints con más problemas Estos informes pueden programarse diario, semanal, mensual, etc., con el fin de obtener dicha información de manera más ágil.
Gestión de usuarios avanzado	Desde ESET PROTECT podemos **crear y personalizar** a detalle los **usuarios y permisos** que tendrán dentro de la plataforma, tales como que grupo de Endpoints podrá ver, que funciones podrá utilizar o si tendrá permisos de escritura o lectura sobre ciertas secciones de la consola.
Notificaciones personalizadas	**Las notificaciones** son esenciales para hacer un seguimiento del estado general de su red. Cuando ocurra un nuevo evento (según la configuración de notificación), se le notificará por correo electrónico a la dirección de correo electrónico especificada, y podrá responder en consecuencia.
Integración con Active Directory	Desde ESET PROTECT podemos sincronizar el árbol completo de equipos y usuarios de nuestro Active Directory en la organización.
Integración con SysLog	Si tiene un servidor Syslog que se ejecuta en su red, puede **Exportar registros a Syslog** con el fin de recibir ciertos eventos (Evento de detección, Evento de firewall agregado, Evento de HIPS agregado, etc.) de los equipos de cliente que ejecutan, por ejemplo, ESET Endpoint Security.
Deployment Remoto	La consola de ESET PROTET le permite realizar una implementación rápida y ágil mediante distintos métodos de ejecución remoto, por ejemplo: - Usar la herramienta de **ESET Deployment Tool**: La ESET Remote Deployment Tool es una manera conveniente de distribuir el paquete del instalador creado por ESET PROTECT Cloud para implementar el agente de ESET Management y productos de seguridad de ESET de manera remota en equipos que pertenecen a una red. - Implementación mediante **GPO** o **SCCM**: Puede usar herramientas de administración como **Objetivo de política de grupo** (GPO), **Software Center Configuration Manager** (SCCM), Symantec Altiris o Puppet para la instalación remota del agente. **Puede crear un script de GPO/SCCM para la instalación del agente en Windows**
Gestión de dispositivos Android y iOS e iPads mediante el módulo de MDM	Desde la plataforma de **ESET PROTECT** puede administrar dispositivos móviles a través del componen integrado de **ESET Mobile Device Management** (MDM) y controlar las funciones de seguridad del dispositivo.
Creación de Grupos estáticos y Grupos dinámicos	

	Mediante la plataforma de gestión de ESET PROTECT puede crear grupos y sub grupos para dividir por área, sucursal, organización, etc. Y asignar políticas del producto de seguridad personalizadas para cada caso.