DYNAMIC THREAT DEFENSE

Solución basada en la nube que ayuda a detectar amenazas de zero-day o amenazas desconocidas mediante la ejecución de muestras sospechosas en un entorno aislado en la nube de ESET, donde se analiza su comportamiento, antes de permitirle acceder a tu red.

CURSO INTENSIVO

+5 puestos

Potente sandboxing basado en la nube

¿QUÉ ES?

- EDTD es una sandbox en la nube que se utiliza para ejecutar o "detonar" y analizar archivos sospechosos, fuera de la red de la empresa.
- No es un producto independiente; se complementa con los productos de seguridad de la familia endpoint de ESET y es una posibilidad más para ofrecer a tus clientes que deseen mejorar la seguridad de sus equipos.
- Se integra con todas las soluciones de empresa de ESET para Windows y se puede activar a través de ESET Security Management Center o en ESET Cloud Administrator.

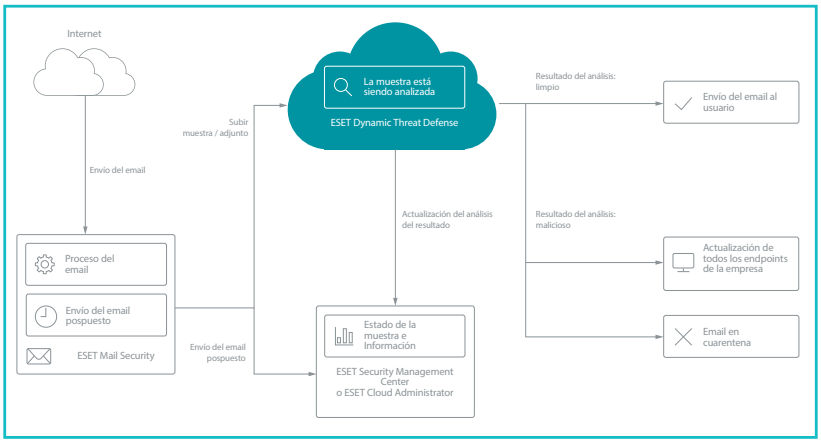
¿POR QUÉ LO NECESITO?

- Actualmente, existe un problema en la industria: las organizaciones siguen siendo víctimas de ataques zero-day, a pesar de utilizar una protección antimalware multicapa.
- EDTD proporciona una capa adicional de defensa fuera de la red de la empresa para ejecutar y analizar amenazas zero-day, como el ransomware, lejos del entorno de producción del cliente.
- Los recientes eventos con WannaCry, Petya o NotPetya mostraron que incluso las soluciones anti-malware específicas no eran capaces de detectar estas amenazas en los primeros días / horas.
- El malware sofisticado, Advanced Persistent Threats (APT), está diseñado y es actualizado frecuentemente para evadir la detección de las diferentes plataformas de protección multicapa para endpoints.
- Un solo incidente de ransomware puede inutilizar fácilmente a una empresa.

¿CÚALES SON LAS PRINCIPALES RAZONES DE VENTA?

PROTECCIÓN MULTICAPA

1. EDTD utiliza 3 modelos diferentes de aprendizaje automático cada vez que se envía un archivo.
2. A continuación, ejecuta la muestra en un sandbox completo que simula el comportamiento del usuario para engañar a las tácticas evasivas del malware.
3. Luego utiliza una red neuronal de aprendizaje para comparar el comportamiento observado con el de todas las muestras históricas de malware.
4. Finalmente, el motor de análisis de ESET se utiliza para separar todas las partes y analizar cualquier objeto inusual.



VISIBILIDAD TOTAL

Para cada muestra analizada, se puede ver la actividad y el resultado final en ESET Security Management Center o en ESET Cloud Administrator. Además de eso, los clientes con una licencia de más de 100 puestos obtienen un informe de comportamiento completo con información detallada sobre las muestras y su comportamiento observado durante el análisis en la zona de pruebas, todo en un formato fácil de entender, sin necesidad de ser un experto.
No solo te informamos de muestras que se enviaron a ESET Dynamic Threat Defense, sino también todo lo que se manda al Sistema de Protección contra Malware en la nube de ESET, llamado ESET LiveGrid®.

MOVILIDAD

Hoy en día, donde los clientes trabajan cada vez más de forma remota, ESET Dynamic Threat Defense se convierte en el nivel de protección fundamental, ya que analiza archivos para todos los usuarios sin importar dónde se encuentren. Lo mejor es que si se detecta algo malicioso, toda la empresa está protegida antes que el resto de usuarios de ESET LiveGrid.

VELOCIDAD INIGUALABLE

Cada minuto cuenta, y por eso ESET Dynamic Threat Defense analiza más del 90% de las muestras en menos de 5 minutos. Si una muestra ya se analizó con anterioridad, sólo se necesitarán unos segundos para que todos los dispositivos de su organización estén protegidos.

DYNAMIC THREAT DEFENSE

PREGUNTAS FRECUENTES

TENGO ESET ENDPOINT SECURITY. ¿POR QUÉ NECESITO ESET DYNAMIC THREAT DEFENSE?

- ESET Endpoint Security es una solución líder y la protección avanzada y eficaz que se necesita en el contexto actual en el que el delito cibernético crece rápidamente.
- Para protegerse contra las amenazas de zero-day, EDTD bloquea el acceso no solo a archivos maliciosos sino también a archivos sospechosos mientras se examinan. En lugar de intentar calcular lo que podría hacer el archivo, EDTD lo ejecuta en un sistema operativo real y usa inteligencia artificial y aprendizaje automático para ver lo que realmente hace y luego analiza su funcionamiento. Incluso si pudiéramos utilizar toda la potencia de procesamiento y los recursos del endpoint, esto llevaría mucho tiempo y el trabajo se interrumpiría.
- La respuesta simple es bloquear temporalmente el acceso al archivo y subcontratar ese análisis a un sistema dedicado mucho más poderoso capaz de analizar la muestra en minutos en lugar de días. Eso es EDTD.

TENGO ESET ENDPOINT QUE INCLUYE UN SANDBOX EN EL PRODUCTO. ¿POR QUÉ DEBO PAGAR POR OTRO SANDBOX?

EDTD es un entorno basado en la nube para ESET Endpoint y ESET Mail Security, desarrollada para detectar nuevos tipos de amenazas nunca vistos antes. EDTD maneja una amplia gama de tipos de archivos sospechosos y se ejecuta en un entorno seguro y aislado dentro de ESET HQ Cloud.

Combina el análisis estático del código y la inspección profunda de la muestra con aprendizaje automático, análisis en memoria e inteligencia artificial para la detección basada en el comportamiento. Toda esta potencia de procesamiento es adicional y es por eso que EDTD se vende como un extra opcional para los productos ESET Endpoint.

¿LIVEGRID NO HACE ESTO?

Las firmas de archivos maliciosos de LiveGrid protegen a toda su comunidad poco tiempo después de que se analiza la muestra original. Debido a que este sistema es compartido por decenas de millones de endpoints, las muestras entrantes deben ponerse en cola antes del análisis. Bloquear ese archivo para el usuario daría lugar a retrasos en la productividad, por lo que el dispositivo que envió la primera muestra a LiveGrid está completamente expuesta a ese archivo, hasta que reciba la actualización junto con el resto de la Comunidad LiveGrid.

Si bien otras tecnologías de ESET detendrán la mayoría de las amenazas, una avanzada podría afectar a ese primer usuario antes de que se analice en el entorno de pruebas de la nube. Ser paciente cero aquí significa que su sistema o red puede no estar protegido a tiempo.

Además, mientras que EDTD clasifica los archivos como Limpios, Sospechosos, Altamente Sospechosos o Maliciosos, LiveGrid utiliza un sistema más simple, Limpio o Malicioso, colocando lo que EDTD vería como Sospechoso y Altamente Sospechoso en su categoría Limpio. LiveGrid es más claro en este caso, pero no permite que el administrador del cliente adapte la Política de Endpoint según los roles o situaciones.

¿TENGO QUE PAGAR MÁS POR EDTD?

Sí, pero es una mejoría muy importante si se quiere potenciar la protección.

Con EDTD:

- Se analiza una gama más amplia de muestras de archivos, incluidos documentos, scripts, instaladores y otros tipos de archivos que se utilizan comúnmente para infectar a los dispositivos.
- Las muestras de EDTD tienen prioridad para los recursos sobre las muestras de LiveGrid.
- El 90% de las muestras de EDTD se analizan en cinco minutos.
- El ordenador que envía el archivo bajo examen estará protegido de ese archivo durante el análisis.
- Todos los ordenadores que utilicen la misma cuenta de ESET Business Account se actualizarán en unos minutos, antes que la comunidad LiveGrid.
- Tu servidor ESMC mostrará y registrará el estado y los resultados de las muestras enviadas a EDTD.

¿LOS ARCHIVOS QUE ENVIO AL EDTD ESTÁN ALMACENADOS EN AZURE?

Los archivos reales no se almacenan en Azure, solo el hash, que es un resultado irreversible de pasar los archivos a través de una función criptográfica. No se puede acceder al archivo real; intentar recrear el archivo a partir del hash sería como intentar convertir la salsa de tomate en un tomate.

PREGUNTAS PARA LOS CLIENTES:

- ¿Reducir el riesgo de infección por una amenaza de zero-day, como el ransomware, es una prioridad para tu negocio?
- ¿Tu empresa necesita el siguiente nivel de seguridad, pero carece de los recursos de IT para proporcionarlo?
- ¿Los diferentes roles en tu empresa necesitan diferentes niveles de protección?