



DYNAMIC THREAT DEFENSE

Previene las amenazas zero-day con una potente sandbox en la nube

**EXPERTOS EN
CIBERSEGURIDAD
A TU LADO**



¿Qué es una sandbox de seguridad en la nube?

Una sandbox de seguridad en la nube es un entorno de análisis aislado en el que se ejecuta un programa sospechoso y se observa, registra y analiza su comportamiento de forma automatizada.

ESET Dynamic Threat Defense proporciona una capa adicional de seguridad para los productos ESET como el Mail Security o la gama Endpoint usando nuestra tecnología sandbox en la nube para detectar nuevos tipos de amenazas nunca antes vistos. Esta sandbox consiste en múltiples tipos de sensores que completan el análisis estático de código, la inspección profunda de la muestra utilizando machine learning, el análisis en memoria y la detección según su comportamiento.

¿Por qué una sandbox de seguridad en la nube?

RANSOMWARE

El ransomware ha sido una preocupación constante para las empresas a nivel mundial desde la aparición de Cryptolocker en 2013. A pesar de que el ransomware ha existido desde hace mucho tiempo, nunca fue una amenaza que preocupara especialmente a las empresas. Sin embargo, una única incidencia de ransomware puede hacer que una empresa se quede inoperativa con el cifrado de sus archivos más importantes. Cuando una empresa experimenta un ataque de ransomware y se da cuenta de que las copias de seguridad no son suficientemente recientes, inmediatamente siente que la única opción que tiene es pagar el rescate.

Nuestra sandbox de seguridad en la nube proporciona una capa de defensa adicional fuera de la red de la empresa para evitar que el ransomware se ejecute en un entorno de producción.

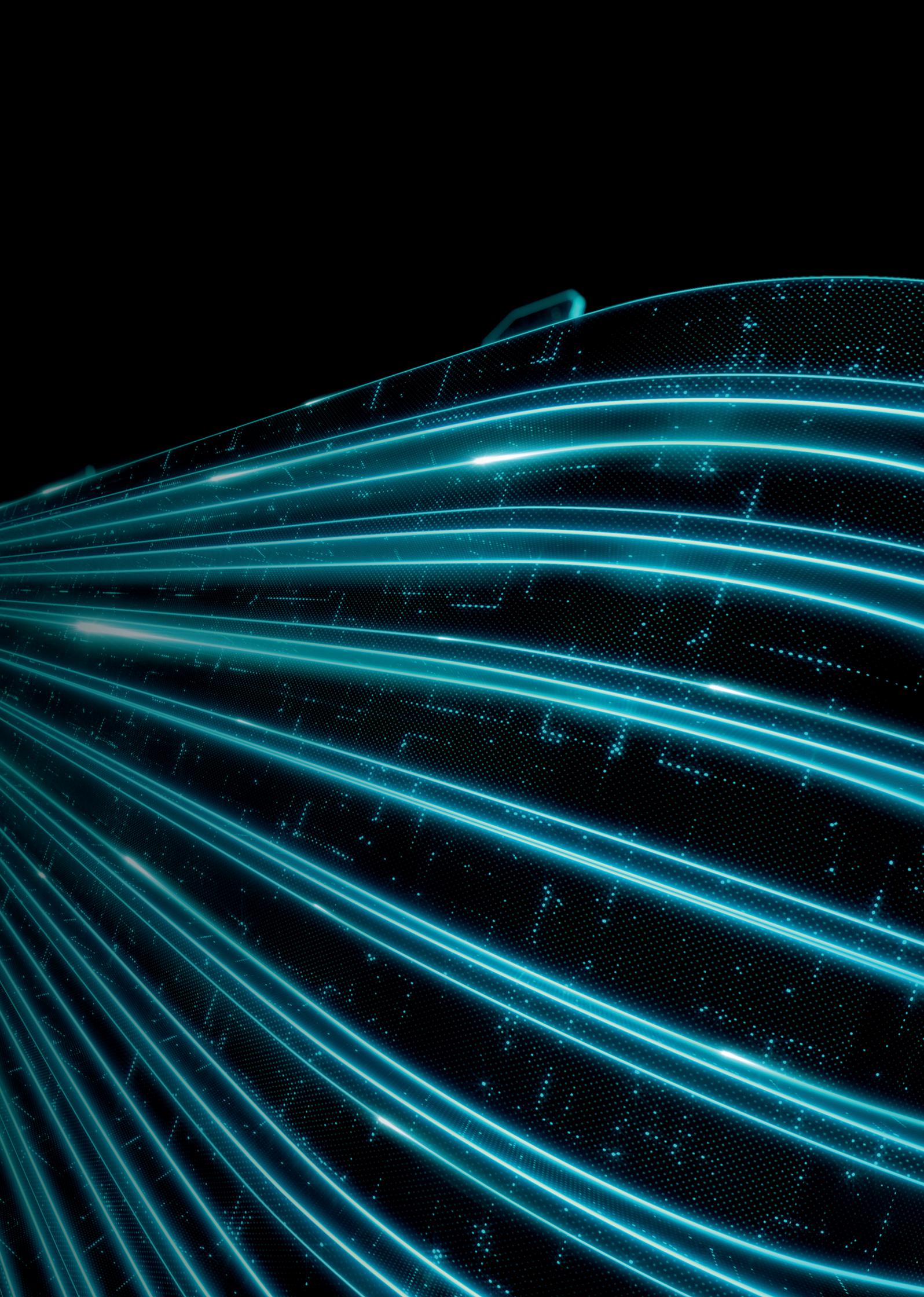
ATAQUES DIRIGIDOS Y FUGAS DE INFORMACIÓN

El panorama actual de la ciberseguridad se encuentra en constante evolución con nuevos métodos de ataque y amenazas nunca antes vistas. Cuando se produce un ataque o fuga de información, las empresas se suelen sorprender de que sus defensas hayan sido puestas en riesgo o ni siquiera son conscientes de que se ha producido el ataque. Una vez se percatan, las empresas implementan las medidas para evitar de forma reactiva que este ataque vuelva a suceder. Sin embargo, esto no las protege del próximo ataque, que podría usar otro vector totalmente nuevo.

La estrategia de utilizar como medida de defensa una sandbox de seguridad en la nube es mucho más efectiva que simplemente observar la apariencia de la posible amenaza porque va más allá de la mera apariencia y en cambio se fija en qué hace esta posible amenaza. Esto contribuye a ser mucho más conclusivo para determinar si se trata de un ataque dirigido, una amenaza persistente o si en cambio es benigno.

Un producto de sandbox de seguridad en la nube proporciona una capa de defensa adicional fuera de la red de la empresa.

Una sandbox de seguridad en la nube va más allá de la mera apariencia y en cambio se fija en qué hace esta posible amenaza.

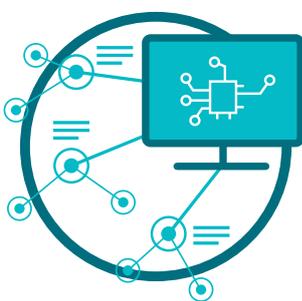


Nuestros productos y tecnologías se apoyan en tres pilares



ESET LIVEGRID®

Siempre que aparece una amenaza zero-day como por ejemplo un ataque de ransomware, el archivo se envía a nuestro sistema de protección contra el malware en la nube LiveGrid®, donde se ejecuta la amenaza y se monitoriza el comportamiento. Los resultados de este sistema se proporcionan a todos los equipos globalmente en pocos minutos sin necesidad de hacer nada por parte del administrador de sistemas y sin tener que actualizar los productos ESET.



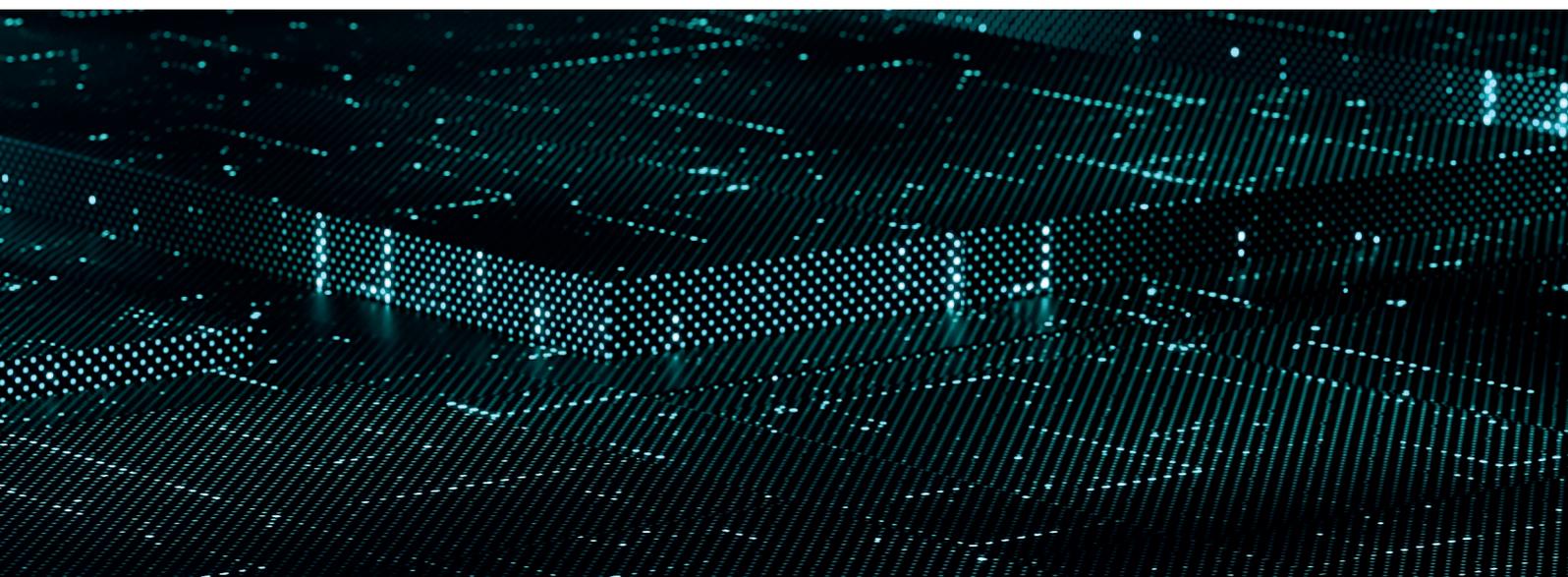
MACHINE LEARNING

Utiliza la potencia combinada de redes neuronales y algoritmos seleccionados cuidadosamente para determinar correctamente las muestras que llegan como seguras, potencialmente no deseadas o maliciosas.



EXPERIENCIA HUMANA

Líderes en investigación de malware a nivel mundial compartiendo su experiencia y conocimientos para garantizar la mejor respuesta frente a amenazas en todo momento.



ESET marca la diferencia

PROTECCIÓN MULTICAPA

Con Dynamic Threat Defense, ESET usa tres modelos diferentes de machine learning cuando se envía un archivo. Posteriormente, ejecuta la muestra en una sandbox que simula el comportamiento del usuario engañando a las técnicas antievasión. Después, se utiliza una red neuronal de aprendizaje profundo para comparar el comportamiento observado frente a los datos de comportamiento históricos. Finalmente, la última versión del motor de análisis de ESET se utiliza para apartarlo todo y analizarlo en busca de cualquier anomalía.

VISIBILIDAD COMPLETA

Cada muestra analizada se añade a la lista de la consola ESET Security Management Center con diversa información sobre la muestra en sí y su origen. Toda la información se muestra de una forma fácil de entender. No solo mostramos las muestras enviadas a ESET Dynamic Threat Defense, sino todo lo enviado al sistema de protección contra el malware en la nube, ESET Live Grid®.

MOVILIDAD

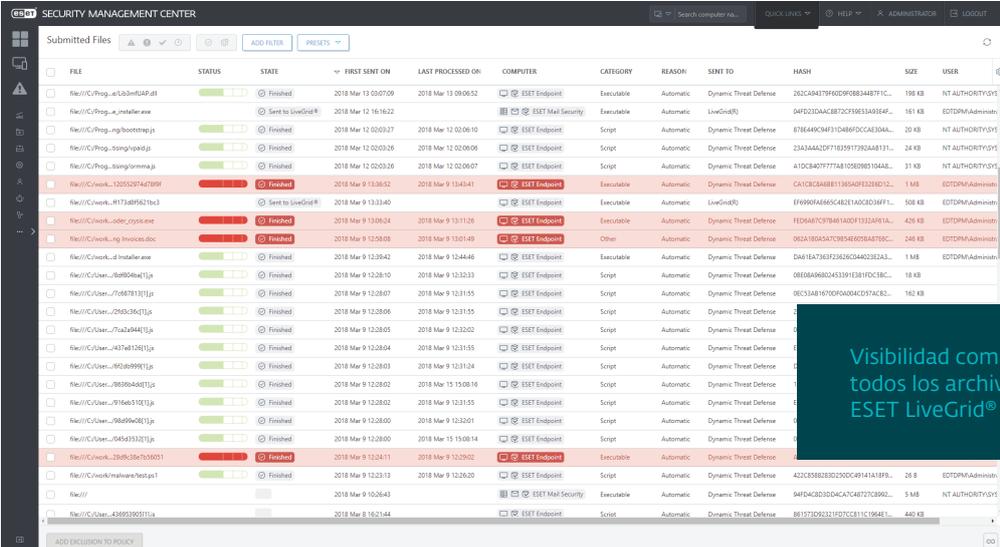
Hoy en día los clientes están en constante movimiento y por eso ESET Dynamic Threat Defense es capaz de analizar archivos sin importar dónde se encuentren los usuarios. Lo mejor es que si se detecta algún elemento malicioso, toda la empresa está protegida.

VELOCIDAD INIGUALABLE

Cada minuto cuenta y por eso ESET Dynamic Threat Defense puede analizar la mayoría de muestras en menos de 5 minutos. Si una muestra ya fue analizada anteriormente, en solo unos segundos se comprueba que todos los dispositivos de la empresa estén protegidos.

DE TOTAL CONFIANZA

ESET lleva en el sector de la seguridad informática más de 30 años y continuamos evolucionando nuestra tecnología para mantenernos a un paso por delante de las últimas amenazas. Esto nos ha llevado a ganarnos la confianza de más de 110 millones de usuarios en todo el mundo. Nuestra tecnología se encuentra examinada constantemente y validada por análisis de terceros que demuestran la gran eficacia de nuestra estrategia para detener las últimas amenazas.



FILE	STATUS	STATE	FIRST SENT ON	LAST PROCESSED ON	COMPUTER	CATEGORY	REASON	SENT TO	HASH	SIZE	USER
file://C:/Prog..._a13b1b1AP.dll	Finished	Finished	2018 Mar 13 03:07:09	2018 Mar 13 09:06:52	ESET Endpoint	Executable	Automatic	Dynamic Threat Defense	262C84879F609F08B3487F1C...	109 KB	NT AUTHORITY\SYSTEM
file://C:/Prog..._a13b1b1AP.dll	Sent to LiveGrid®	Finished	2018 Mar 12 16:16:22		ESET Mail Security	Executable	Automatic	LiveGrid®	04F033D0AC8F72CF9E3A58E4F...	161 KB	ESETDRM\Administrador
file://C:/Prog..._ngbootstraj.js	Finished	Finished	2018 Mar 12 02:03:27	2018 Mar 12 02:06:10	ESET Endpoint	Script	Automatic	Dynamic Threat Defense	878E448C84F31D486FDCA3D0A...	20 KB	NT AUTHORITY\SYSTEM
file://C:/Prog..._ssingipad.js	Finished	Finished	2018 Mar 12 02:03:26	2018 Mar 12 02:06:06	ESET Endpoint	Script	Automatic	Dynamic Threat Defense	23A3A4A2D9F7835917782A48131...	24 KB	NT AUTHORITY\SYSTEM
file://C:/Prog..._ssingipad.js	Finished	Finished	2018 Mar 12 02:03:26	2018 Mar 12 02:06:07	ESET Endpoint	Script	Automatic	Dynamic Threat Defense	A1DC8407777810560F528012...	31 KB	NT AUTHORITY\SYSTEM
file://C:/work..._1205520746780F	Finished	Finished	2018 Mar 9 13:36:52	2018 Mar 9 13:43:41	ESET Endpoint	Executable	Automatic	Dynamic Threat Defense	C41C8C848811365A0F328012...	1 MB	ESETDRM\Administrador
file://C:/work..._#173d9f9621ba3	Sent to LiveGrid®	Finished	2018 Mar 9 13:33:40		ESET Endpoint	Executable	Automatic	LiveGrid®	8F990FA685C482EAC2C38FF...	508 KB	ESETDRM\Administrador
file://C:/work..._code_csys.exe	Finished	Finished	2018 Mar 9 13:09:24	2018 Mar 9 13:11:28	ESET Endpoint	Executable	Automatic	Dynamic Threat Defense	FD2487C37641A0291332A1013...	428 KB	ESETDRM\Administrador
file://C:/work..._ng_invoices.doc	Finished	Finished	2018 Mar 9 12:58:08	2018 Mar 9 13:01:49	ESET Endpoint	Other	Automatic	Dynamic Threat Defense	962A18D4347C9E548058A878C...	248 KB	ESETDRM\Administrador
file://C:/work..._d_installer.exe	Finished	Finished	2018 Mar 9 12:58:42	2018 Mar 9 12:44:46	ESET Endpoint	Executable	Automatic	Dynamic Threat Defense	D461E4783F9292620C44023E2A3...	1 MB	ESETDRM\Administrador
file://C:/User..._8d8048411.js	Finished	Finished	2018 Mar 9 12:38:10	2018 Mar 9 12:31:33	ESET Endpoint	Script	Automatic	Dynamic Threat Defense	08E08A980245339E81F0C38C...	18 KB	
file://C:/User..._7d8b78131.js	Finished	Finished	2018 Mar 9 12:38:07	2018 Mar 9 12:31:55	ESET Endpoint	Script	Automatic	Dynamic Threat Defense	08C34818170F040A04C825ACB...	162 KB	
file://C:/User..._2983-36461.js	Finished	Finished	2018 Mar 9 12:38:06	2018 Mar 9 12:31:55	ESET Endpoint	Script	Automatic	Dynamic Threat Defense			
file://C:/User..._75a3a9461.js	Finished	Finished	2018 Mar 9 12:38:05	2018 Mar 9 12:32:02	ESET Endpoint	Script	Automatic	Dynamic Threat Defense			
file://C:/User..._437e11391.js	Finished	Finished	2018 Mar 9 12:38:04	2018 Mar 9 12:31:55	ESET Endpoint	Script	Automatic	Dynamic Threat Defense			
file://C:/User..._8f586991.js	Finished	Finished	2018 Mar 9 12:38:03	2018 Mar 9 12:31:24	ESET Endpoint	Script	Automatic	Dynamic Threat Defense			
file://C:/User..._862664811.js	Finished	Finished	2018 Mar 9 12:38:02	2018 Mar 9 15:08:16	ESET Endpoint	Script	Automatic	Dynamic Threat Defense			
file://C:/User..._9166b5101.js	Finished	Finished	2018 Mar 9 12:38:02	2018 Mar 9 12:31:55	ESET Endpoint	Script	Automatic	Dynamic Threat Defense			
file://C:/User..._98896061.js	Finished	Finished	2018 Mar 9 12:38:00	2018 Mar 9 12:32:01	ESET Endpoint	Script	Automatic	Dynamic Threat Defense			
file://C:/User..._045d35321.js	Finished	Finished	2018 Mar 9 12:38:00	2018 Mar 15 15:08:14	ESET Endpoint	Script	Automatic	Dynamic Threat Defense			
file://C:/work..._28a5-356105001	Finished	Finished	2018 Mar 9 12:34:11	2018 Mar 9 12:39:02	ESET Endpoint	Executable	Automatic	Dynamic Threat Defense			
file://C:/work..._malwarenext1.js	Finished	Finished	2018 Mar 9 12:33:13	2018 Mar 9 12:36:20	ESET Endpoint	Script	Automatic	Dynamic Threat Defense	42CC586203200C48141A189...	26 B	ESETDRM\Administrador
file://	Finished	Finished	2018 Mar 9 10:26:43		ESET Mail Security	Executable	Automatic	Dynamic Threat Defense	84F04C8202D4C4C48727C89A...	5 MB	NT AUTHORITY\SYSTEM
file://C:/User..._436923930511.js	Finished	Finished	2018 Mar 8 16:21:44		ESET Endpoint	Script	Automatic	Dynamic Threat Defense	86157202321F07C8E11C1064E...	440 KB	

Visibilidad completa: accede a todos los archivos enviados a ESET LiveGrid®

Casos de uso

Ransomware

CASO DE USO

El ransomware tiende a acceder a las cuentas de correo de los usuarios a través del correo electrónico.

SOLUCIÓN

- ✓ ESET Mail Security envía automáticamente los documentos adjuntos de correo electrónico sospechosos a ESET Dynamic Threat Defense.
- ✓ ESET Dynamic Threat Defense analiza la muestra y envía el resultado de nuevo a Mail Security normalmente en unos 5 minutos.
- ✓ ESET Mail Security detecta y elimina automáticamente los documentos adjuntos con el contenido malicioso.
- ✓ El documento adjunto malicioso nunca llega al destinatario.

Protección granular para diferentes perfiles de empresa

CASO DE USO

Cada perfil de la empresa requiere diferentes niveles de protección. Los desarrolladores o empleados de sistemas necesitan diferentes restricciones de seguridad que el gerente de la empresa o el CEO.

SOLUCIÓN

- ✓ Configura una única política por equipo o por servidor en ESET Dynamic Threat Defense.
- ✓ Aplica automáticamente una política diferente según un grupo de usuarios estáticos diferentes o un grupo de Active Directory.
- ✓ Cambia automáticamente los ajustes de configuración con tan solo mover un usuario de un grupo a otro.



Archivos desconocidos o cuestionables

CASO DE USO

En ocasiones los empleados o el departamento de sistemas reciben un archivo del que quieren comprobar su seguridad.

SOLUCIÓN

- ✓ Cualquier usuario puede enviar una muestra para su análisis directamente dentro de todos los productos ESET.
- ✓ ESET Dynamic Threat Defense analiza la muestra rápidamente.
- ✓ Si se descubre que un archivo es malicioso, todos los equipos de la empresa están protegidos.
- ✓ El administrador de sistemas tiene una visibilidad completa del usuario que envió la muestra y de si el archivo era legítimo o malicioso.



FILE BEHAVIOR REPORT ESET

STATUS Malicious

SHA-1 FED647C7B41A20F1332AF61A89EA9F85A54DF

SIZE 4387368

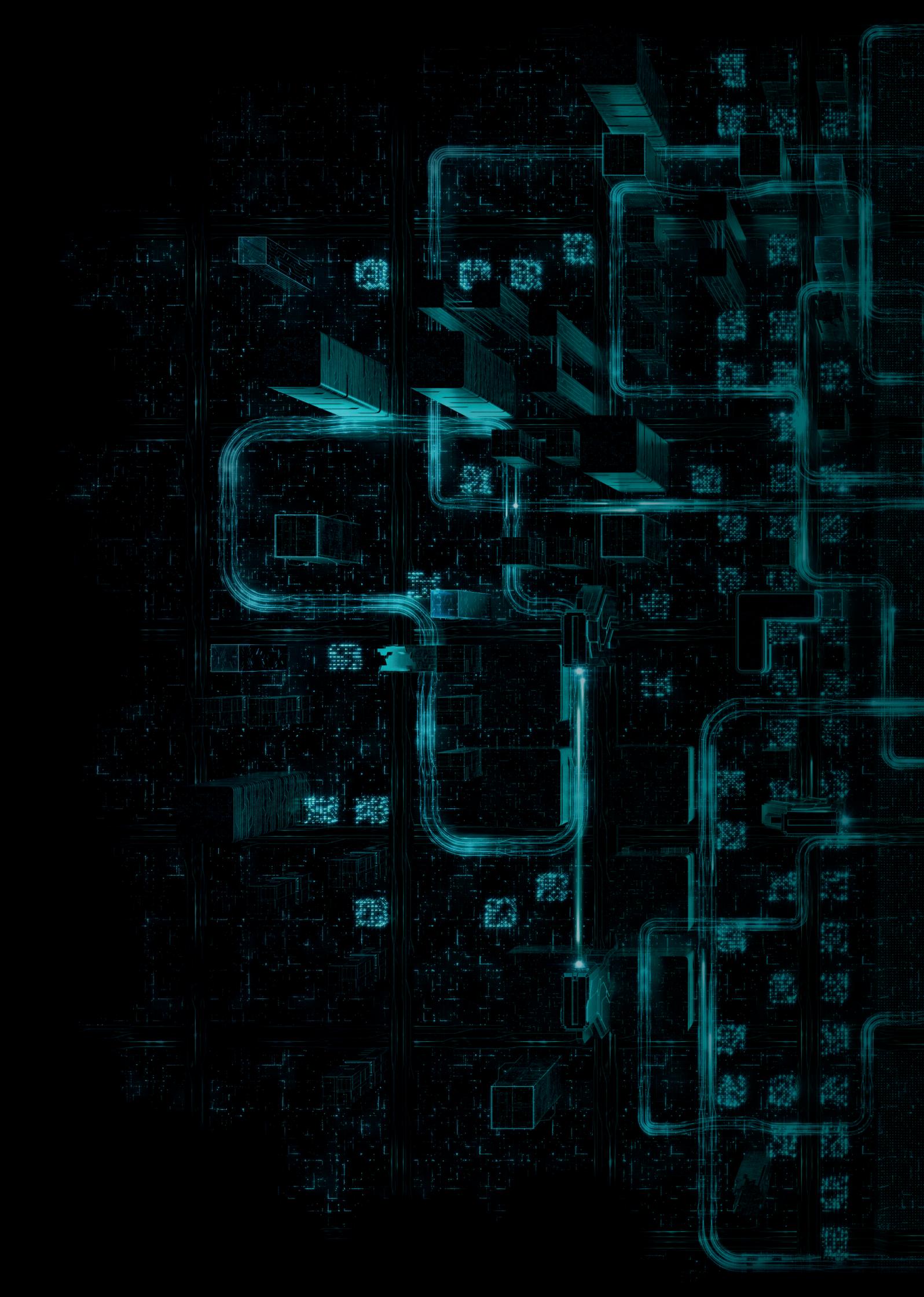
CATEGORY Executable

Detected Behaviors

BEHAVIOR	Malware detected after execution
EXPLANATION	Sample has been detected as malicious after execution
BENIGN CAUSES	Clean applications should not do this
MALICIOUS CAUSES	Malware detected with ESET scanning engine after execution
BEHAVIOR	New files created in the Windows folder
EXPLANATION	Sample has created new files in the Windows folder
BENIGN CAUSES	This is standard behavior for some installers
MALICIOUS CAUSES	Malware tried to hide its presence
BEHAVIOR	Analyzed sample copied
EXPLANATION	Sample has been copied to a different location
BENIGN CAUSES	This is standard behavior for some installers
MALICIOUS CAUSES	Malware tried to hide its presence
BEHAVIOR	Startup list modified
EXPLANATION	Sample has added a new entry to the Windows Startup application list
BENIGN CAUSES	This is standard behavior for some installers
MALICIOUS CAUSES	Malware wants to run after a system reboot
BEHAVIOR	Machine Learning detection
EXPLANATION	Sample behaves very similarly to known malware
BENIGN CAUSES	Clean applications should not do this
MALICIOUS CAUSES	Malware has been detected by Neural network Machine Learning
BEHAVIOR	New files in Program Files folder created
EXPLANATION	Sample has created new files in the Windows Program Files folder
BENIGN CAUSES	This is standard behavior for some installers
MALICIOUS CAUSES	Sample may be a Potentially Unwanted Application

ESET DYNAMIC THREAT DEFENSE





Características técnicas de ESET Dynamic Threat Defense

PROTECCIÓN AUTOMÁTICA

Cuando todo está configurado no se requiere ninguna acción por parte del administrador o el usuario. El producto para equipo o servidor decide automáticamente si la muestra es buena, mala o desconocida. Si la muestra es desconocida, se envía a ESET Dynamic Threat Defense para su análisis. Cuando termina el análisis, se comparte el resultado y los productos para escritorio responden en consecuencia.

PERSONALIZACIÓN TOTAL

ESET permite una configuración detallada de políticas por equipo para ESET Dynamic Threat Defense para que el administrador pueda controlar lo que se envía y qué debería ocurrir según el resultado recibido.

ENVÍO MANUAL

Un usuario o administrador puede enviar en cualquier momento muestras para su análisis a través de un producto ESET compatible y recibir el resultado completo. Los administradores verán quién lo envió y cuál fue el resultado directamente en la consola ESET Security Management Center.

PROTECCIÓN DEL CORREO

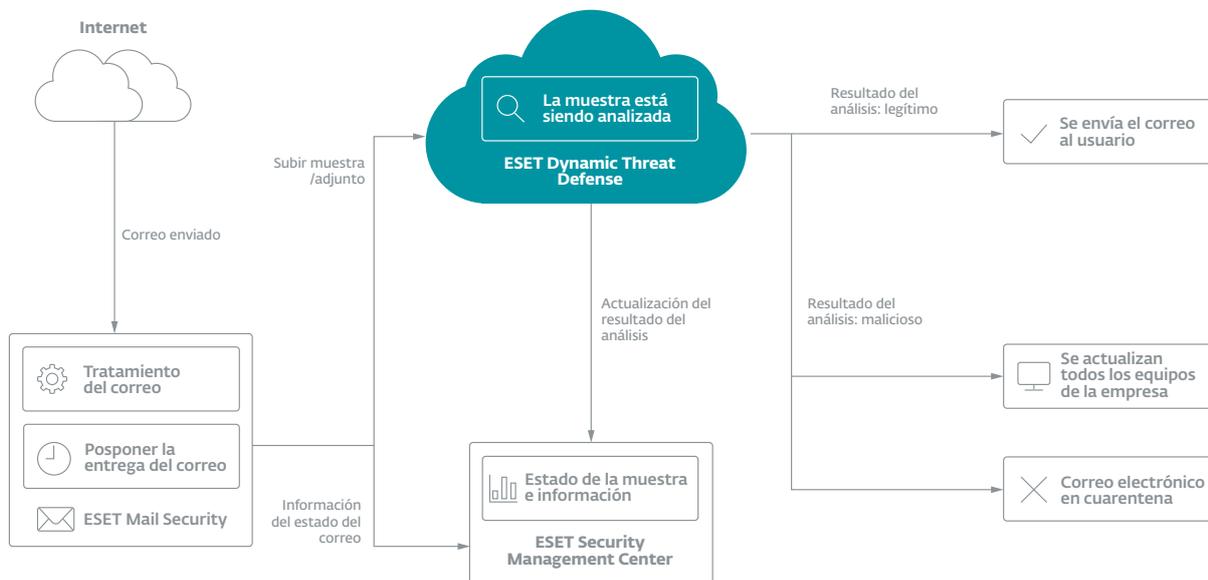
ESET Dynamic Threat Defense no solo funciona con archivos, sino que también funciona directamente con ESET Mail Security para garantizar que no lleguen correos maliciosos a tu empresa. Para garantizar la continuidad de la empresa, solo se pueden enviar para su inspección a ESET Dynamic Threat Defense los correos procedentes de fuera de la empresa.

“Lo más destacable es su fuerte ventaja técnica respecto a otros productos del mercado. ESET ofrece una seguridad fiable, lo cual implica que puedo trabajar en cualquier proyecto en cualquier momento sabiendo que los equipos están protegidos al 100%.”

Fiona Garland, analista de negocio en
Mercury Engineering, Irlanda; 1.300 puestos

Cómo funciona ESET Dynamic Threat Defense

Con ESET Mail Security



"Nuestra experiencia con ESET es más que satisfactoria, por lo que hemos renovado nuestras licencias para tres años más. Por tanto, sin ninguna duda, recomendamos las soluciones ESET a todas las empresas que quieran aumentar su nivel de seguridad."

Ernesto Bonhoure, director de sistemas informáticos;
Hospital Alemán, Argentina, 1.500+ puestos



Acercas de ESET

ESET, pieza clave en la seguridad de la información, ha sido nombrado el único Challenger en el Cuadrante mágico Gartner para plataformas de protección de equipos*

Durante más de 30 años, ESET ha desarrollado programas de seguridad informática y servicios líderes en el

sector, que proporcionan una protección exhaustiva al instante contra las amenazas a la seguridad informática en constante evolución para empresas y consumidores en todo el mundo.

ESET es una empresa privada. Sin deudas ni préstamos, tenemos la libertad de hacer lo necesario para la máxima protección de todos nuestros clientes.

ESET EN NÚMEROS

110m+
usuarios en
todo el mundo

400k+
clientes
empresa

200+
países y
territorios

13
centros
globales de
I+D

EMPLEADOS DE ESET

Más de un tercio de todos los empleados de ESET trabajan en Investigación y Desarrollo.



FACTURACIÓN DE ESET

En millones de €



*Gartner no promociona a ningún fabricante, producto o servicio que aparezca en sus artículos de investigación. Los artículos de investigación de Gartner representan la opinión de la empresa de investigación Gartner y no deberían interpretarse como exposición de hechos. Gartner niega cualquier responsabilidad, expresa o implícita, respecto a esta investigación, incluyendo toda garantía de comercialización o idoneidad para un objetivo determinado.

ALGUNOS DE NUESTROS CLIENTES

HONDA

Protegido por ESET desde 2011,
licencia prolongada x3, ampliada x2

Canon

Protegido por ESET desde 2016,
más de 14.000 equipos

Allianz

Suisse

Protegidos por ESET desde 2016
Más de 4000 buzones de correo

ATRÁPALO

Protegidos por ESET desde 2005,
licencia prolongada/ampliada x11

ALGUNOS DE NUESTROS PREMIOS MÁS IMPORTANTES



“Cash Converters necesita una solución segura y eficaz ante la sofisticación de los últimos virus divulgados. Seguiremos confiando en ESET, ya que ha reunido todos los requisitos para aportar un valor añadido a las soluciones de IT”.

David Polonio, CIO de Cash Converters

