



# DYNAMIC THREAT DEFENSE

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

CYBERSECURITY  
EXPERTS ON YOUR SIDE



# ¿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 y 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 por 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.

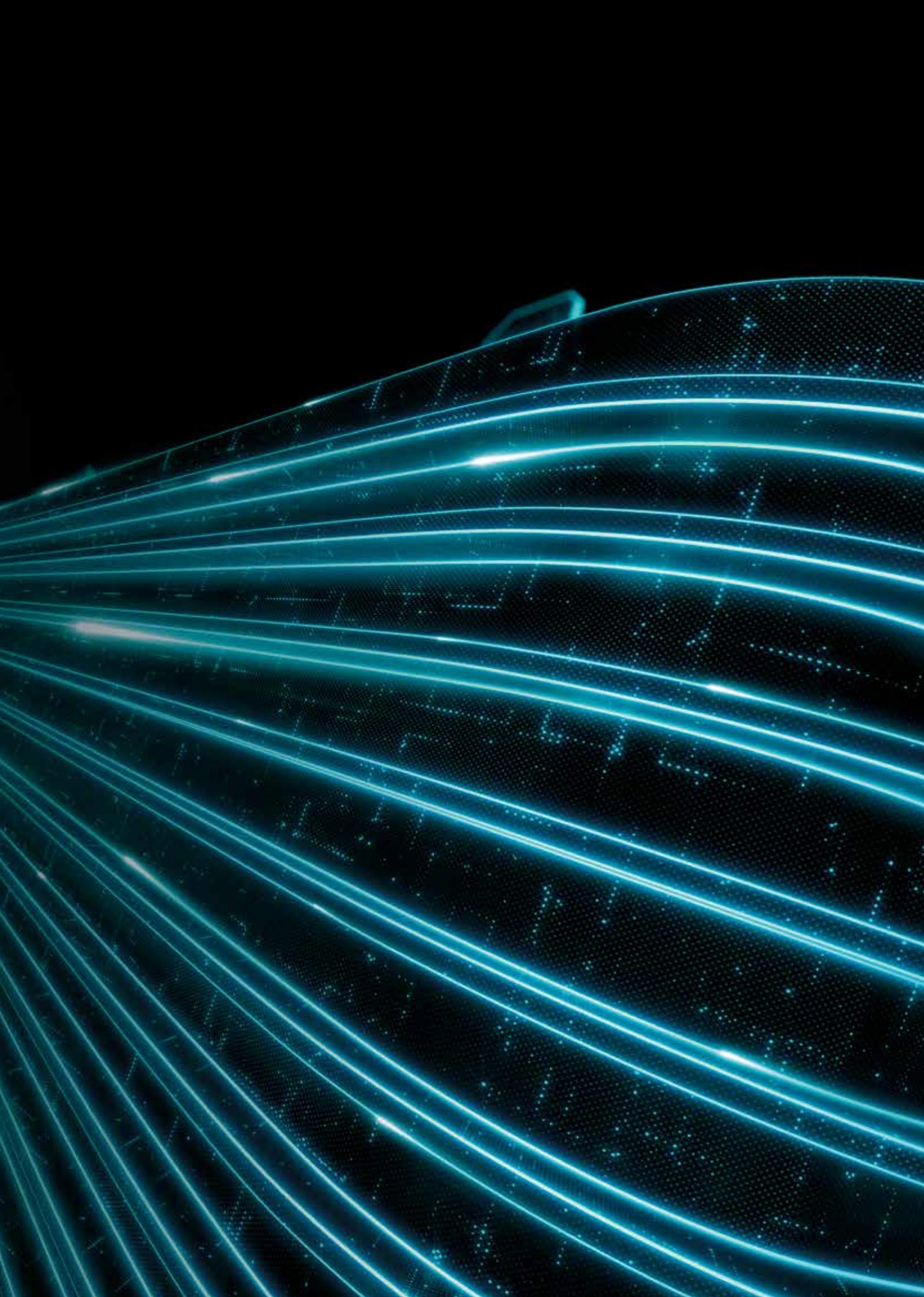
## ATAQUES DIRIGIDOS Y FUGAS DE INFORMACIÓN

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 comprometidas 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.

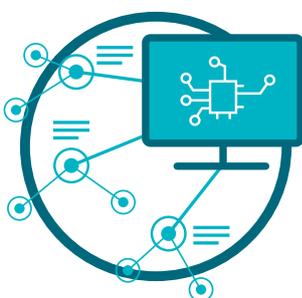


# Nuestros productos y tecnologías se apoyan en tres pilares



## 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.



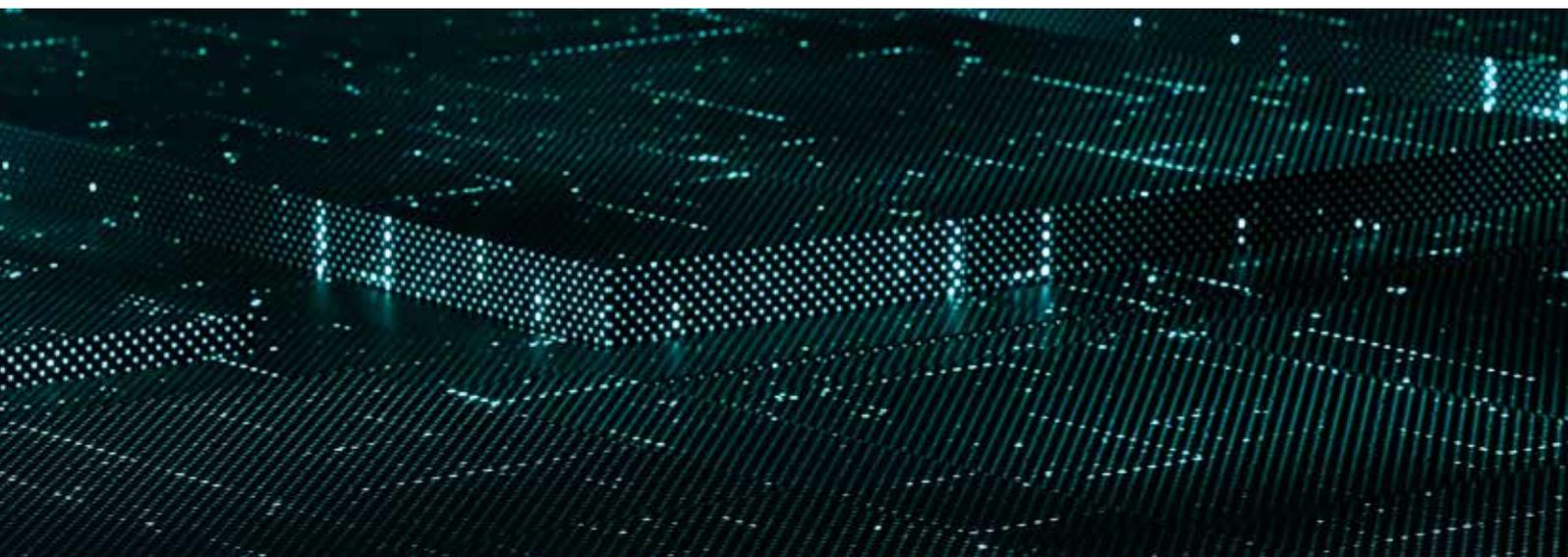
## MACHINE LEARNING

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.





# 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 Directorio Activo.
- ✓ Cambia automáticamente los ajustes de configuración con tan solo mover un usuario de un grupo a otro.



# Archivos desconocidos o sospechosos

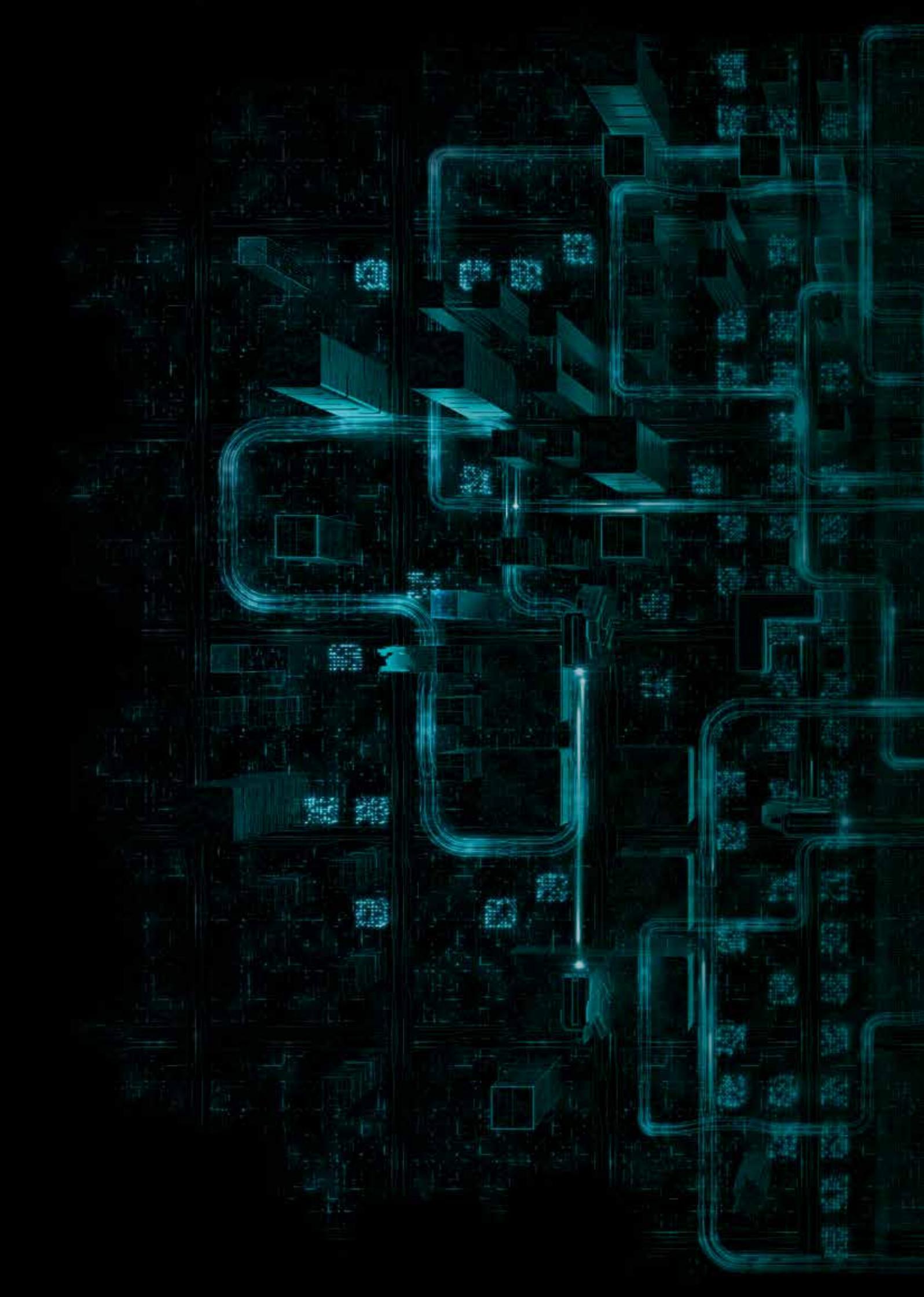
## CASO DE USO

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.





# 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 endpoint 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 PROTECT On-Prem.

## PROTECCIÓN DEL CORREO

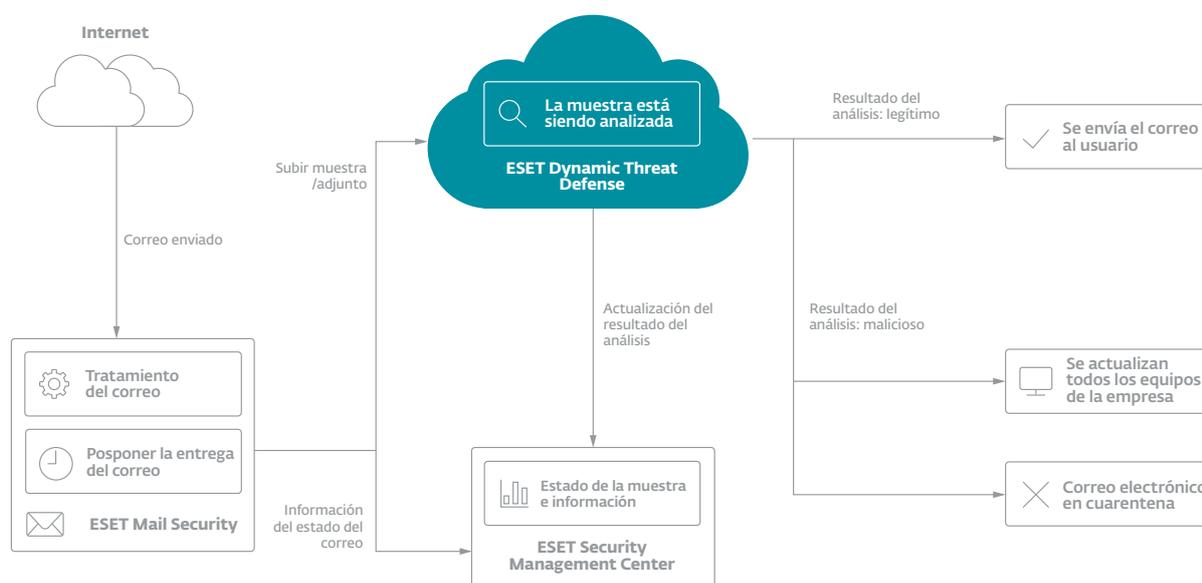
ESET Dynamic Threat Defense no solo funciona con archivos, sino que también funciona directamente con ESET Mail Security para garantizar que no lleguen correos maliciosos a tu empresa. Para garantizar la continuidad de la empresa, solo se pueden enviar para su inspección a ESET Dynamic Threat Defense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

Durante más de 30 años, ESET® ha desarrollado software y servicios de seguridad informática líderes en el sector, ofreciendo una protección inmediata y completa para las amenazas cambiantes de ciberseguridad para empresas y consumidores de todo el mundo.

ESET es una empresa privada. Sin deudas ni préstamos, somos libres de hacer lo que haya que hacer para ofrecer la máxima protección a todos nuestros clientes.

## ESET EN CIFRAS

<b>+110M</b> de usuarios en todo el mundo	<b>+400k</b> clientes de empresa	<b>+200</b> países y territorios	<b>13</b> centros de I+D en el mundo
---	--	--	--

## ALGUNOS DE NUESTROS CLIENTES



protegidos con ESET desde 2017,  
con más de 14 000 endpoints



protegidos por ESET desde 2016,  
más de 9 000 endpoints



protegidos con ESET desde 2016,  
con más de 4 000 buzones de correo



Colaborador de seguridad de ISP desde 2008,  
con una base de 2 millones de clientes

# ¿Por qué elegir ESET?



ESET cumple la norma [ISO/IEC 27001:2013](#), una norma de seguridad reconocida y aplicable internacionalmente en el despliegue y la gestión de la seguridad de la información. La certificación es otorgada por el organismo de certificación acreditado por [SGS](#) y demuestra el cumplimiento total de ESET de las mejores prácticas de la industria.

## ALGUNOS DE NUESTROS PREMIOS MÁS IMPORTANTES



## RECONOCIMIENTO DE LOS ANALISTAS

### Gartner

ESET fue nombrado el único Challenger en 2019 en el Gartner Magic Quadrant para plataformas de protección de endpoints, por segundo año consecutivo.

### FORRESTER®

ESET recibió la calificación de «Strong Performer» en el Forrester Wave(TM): Suites de seguridad de endpoints, tercer trimestre de 2019.

### THE RADICATI GROUP, INC. A TECHNOLOGY MARKET RESEARCH FIRM

ESET recibió la calificación de «Top Player» en el informe 2019 Radicati Endpoint Security según dos criterios: funcionalidad y visión estratégica.

Gartner Inc, Magic Quadrant para plataformas de protección de endpoints, Peter Firstbrook, Lawrence Pingree, Dionisio Zumerle, Prateek Bhajanka, Paul Webber, 20 de agosto de 2019. Gartner no respalda a ningún proveedor, producto o servicio descrito en sus publicaciones de investigación. Los estudios publicados por Gartner recogen solo las opiniones de la organización de investigación de Gartner y no deben considerarse declaraciones de hechos. Gartner excluye cualquier garantía, explícita o implícita, en relación con este estudio, incluidas las garantías de comercialización o idoneidad para un uso en concreto.

Gartner Peer Insights es una plataforma gratuita de revisión y calificación por pares diseñada para los responsables de la toma de decisiones de software y servicios empresariales. Las reseñas pasan por un estricto proceso de validación y moderación para garantizar la autenticidad de la información. Las reseñas de Gartner Peer Insights representan las opiniones subjetivas de usuarios basadas en sus propias experiencias y no representan los puntos de vista de Gartner o sus asociados.

