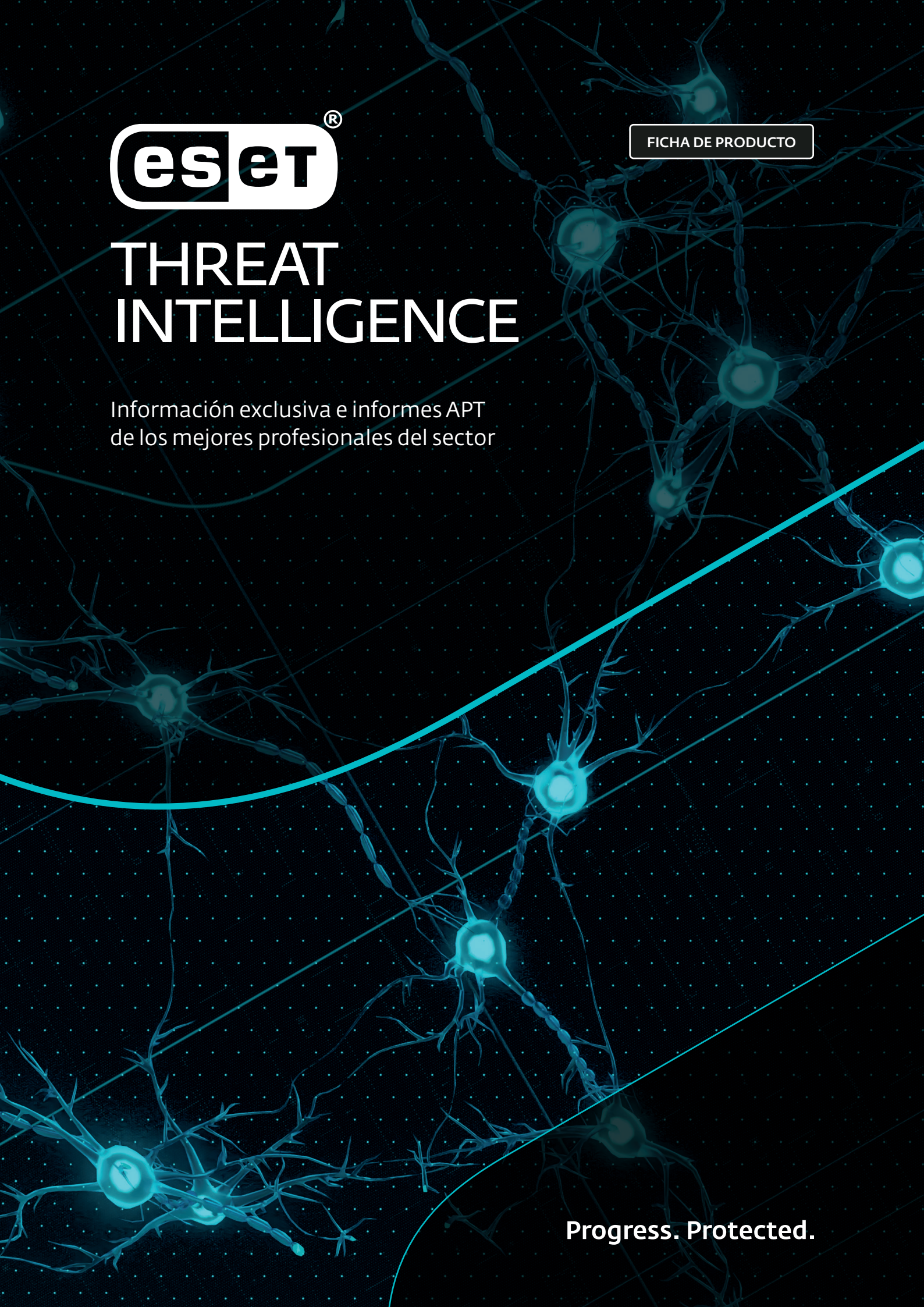
FICHA DE PRODUCTO

THREAT INTELLIGENCE

Información exclusiva e informes APT
de los mejores profesionales del sector



Progress. Protected.

Obtén una perspectiva única sobre el panorama de las ciberamenazas

OBTÉN UNA PERSPECTIVA ÚNICA

ESET recopila inteligencia sobre amenazas de una gran variedad de fuentes y cuenta con una experiencia inigualable sobre este terreno que te ayudará a hacer frente a los ataques de ciberseguridad cada vez más sofisticados.

ADELÁNTATE A LA COMPETENCIA

ESET vigila específicamente aquellos lugares donde hemos detectado grupos APT que tienen como objetivo empresas de países orientales: Rusia, China, Corea del Norte, Irán. Conocerás las nuevas amenazas antes que nadie.

TOMA DECISIONES CRUCIALES, MÁS RÁPIDO

Anticípate a las amenazas y toma decisiones más rápidas y acertadas gracias a los informes exhaustivos y feeds de ESET.

MEJORA TU NIVEL DE SEGURIDAD

Gracias a la información de inteligencia de ESET, podrás mejorar tus capacidades de detección y corrección de amenazas, bloquear APTs y ransomware y mejorar tu arquitectura de ciberseguridad.

AUTOMATIZA LA INVESTIGACIÓN DE AMENAZAS

La tecnología de ESET detecta amenazas constantemente, en múltiples capas, desde antes del arranque hasta en el estado de inactividad. Benefíciate de la telemetría en todos los países donde ESET detecta amenazas emergentes.

Ventajas de ESET

Experiencia humana respaldada por aprendizaje automático. Nuestro sistema de reputación, LiveGrid está compuesto por 110 millones de sensores en todo el mundo, y es verificado por nuestros centros de I+D.

EXPERIENCIA HUMANA RESPALDADA POR MACHINE LEARNING

El uso del aprendizaje automático para automatizar decisiones y evaluar posibles amenazas es una parte vital de nuestra estrategia. Pero solo es tan eficaz como el personal que hay detrás del sistema. La experiencia humana es primordial para proporcionar la información sobre la inteligencia de amenazas, porque los ciberdelincuentes suelen ser adversarios inteligentes.

FUERTE REPUTACIÓN SISTEMA - LIVEGRID®

Los productos ESET Endpoint contienen un sistema de reputación en la nube que proporciona información relevante sobre las amenazas más recientes y archivos seguros. Nuestro sistema de reputación, LiveGrid®, está formado por 110 millones de sensores en todo el mundo verificados por nuestros centros de I+D. Esto proporciona a los clientes el máximo nivel de confianza al visualizar la información y los informes en su consola.

PROCEDENCIA DE LA UE, PRESENCIA MUNDIAL

Con sede en la Unión Europea, ESET lleva más de 30 años en el sector de la seguridad, cuenta con 22 oficinas en todo el mundo, 13 centros de I+D y está presente en más de 200 países y territorios. Esto nos permite ofrecer a nuestros clientes una perspectiva global de las tendencias y amenazas más recientes.

Informes sobre Amenazas Persistentes Avanzadas (APT)

NUESTRA MEJOR INVESTIGACIÓN A TU ALCANCE

Nuestro equipo de investigación es muy conocido en el sector de la seguridad digital, gracias a nuestros reconocidos blogs We Live Security y PROTEGERSE. El equipo ofrece excelentes investigaciones y resúmenes de actividades APT, además de información mucho más detallada. Los clientes de ESET obtienen un adelanto exclusivo de todo el contenido de We Live Security y PROTEGERSE.

CONTENIDOS PRÁCTICOS Y ELABORADOS

Los informes aportan información contextual sobre lo que está ocurriendo y por qué. Gracias a ello, las empresas pueden prepararse de antemano para lo que pueda venir. Y lo que es más importante, nuestros expertos se aseguran de que el contenido sea fácil de entender.

TOMA DECISIONES CRUCIALES CON RAPIDEZ

Todo ello ayuda a las empresas a tomar decisiones cruciales y proporciona una ventaja estratégica en la lucha contra la delincuencia digital. Aporta una comprensión de lo que está ocurriendo en el "lado malo de Internet" y proporciona un contexto crucial, para que la empresa pueda prepararse internamente con rapidez.

ACCESO A UN ANALISTA DE ESET

Cada cliente que solicite el paquete APT Reports Premium tendrá también acceso a un analista de ESET durante un máximo de cuatro horas al mes. Esto ofrece la oportunidad de tratar temas con mayor detalle y ayudar a resolver cualquier problema pendiente.

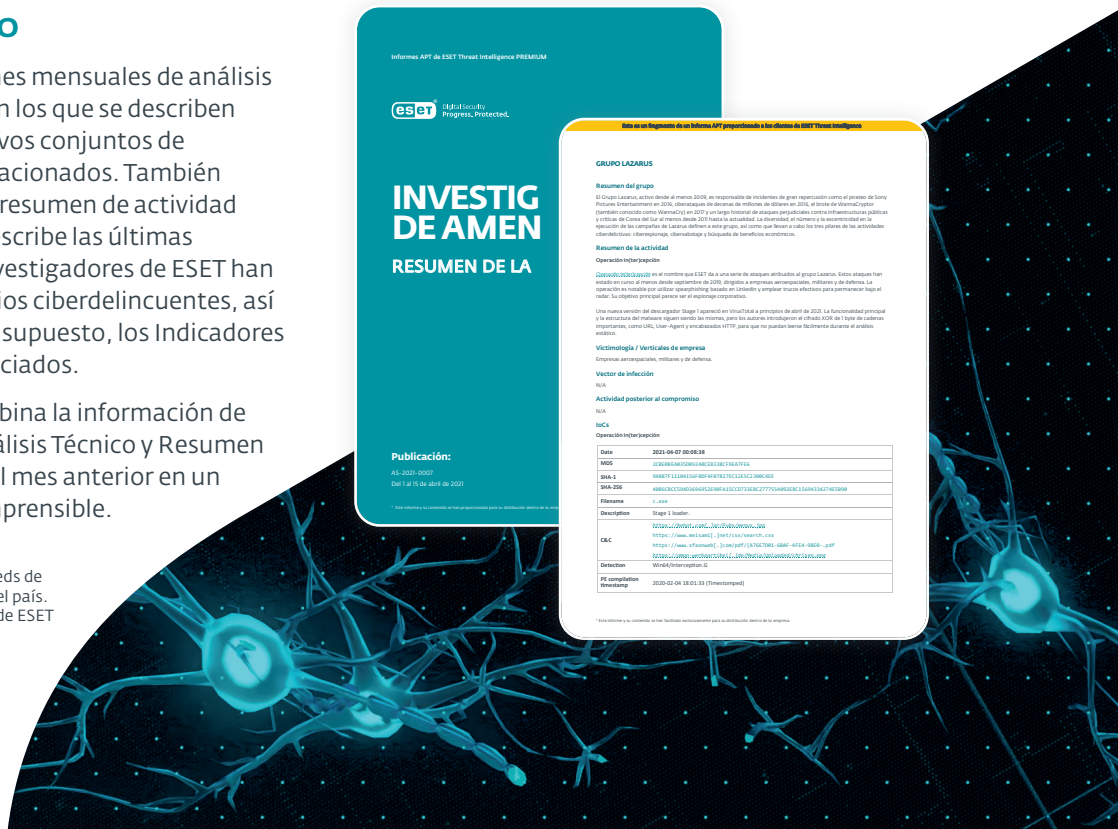
CON LOS INFORMES DE APT, OBTENDRÁS

- Acceso a análisis privados y exhaustivos
- Informes de síntesis APT
- Un resumen mensual para los directivos de alto nivel
- Acceso directo a un profesional de ciberseguridad de ESET
- Acceso a nuestro servidor MISP

ANÁLISIS PROFUNDO

El paquete incluye informes mensuales de análisis técnico en profundidad en los que se describen campañas recientes, nuevos conjuntos de herramientas y temas relacionados. También obtendrás un informe de resumen de actividad cada dos semanas que describe las últimas campañas APT que los investigadores de ESET han estado rastreando de varios ciberdelincuentes, así como sus objetivos y, por supuesto, los Indicadores de Compromiso (IoC) asociados.

El resumen mensual combina la información de todos los informes de Análisis Técnico y Resumen de Actividad publicados el mes anterior en un formato más breve y comprensible.



La disponibilidad de los informes y feeds de ESET Threat Intelligence varía según el país. Contacta con tu representante local de ESET para obtener más información.

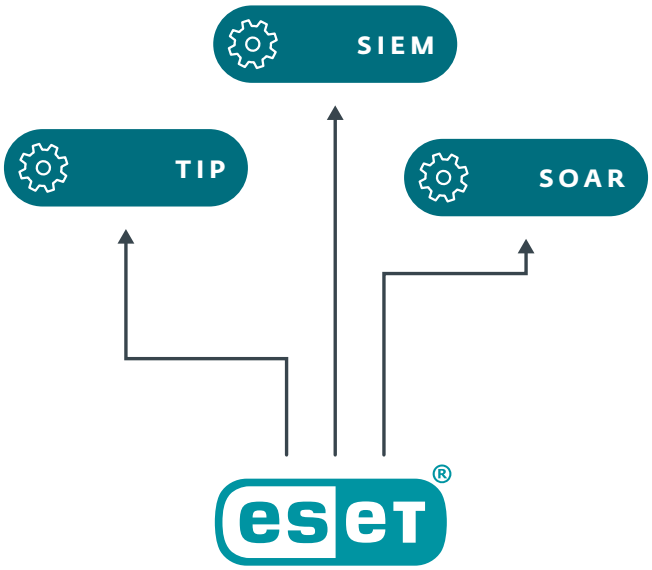
Integra ESET Threat Intelligence en tu sistema

Integrar la telemetría de ESET es sencillo y enriquecerá tu TIP, SIEM o SOAR

Disponemos de una **API completa con toda la documentación**

Suministramos datos en **formatos estandarizados**, como JSON y STIX a través de TAXII, para que la integración en cualquier herramienta sea posible

Para IBM QRadar, Anomali, ThreatQuotient y Logpoint tenemos **manuales de integración paso a paso** para una implementación rápida y sencilla, y seguimos añadiendo otras



¿Cómo nace nuestra inteligencia sobre amenazas? **Ciclo de vida de la inteligencia de amenazas**

La creación de nuestra inteligencia es, de hecho, un ciclo que se refuerza a sí mismo.

Utiliza la amplia gama de telemetría generada por ESET LiveSense, nuestra tecnología de seguridad multicapa que se encuentra dentro de la plataforma ESET PROTECT.

La telemetría obtenida se complementa con diversas fuentes adicionales, como honeypots u OSINT.

A continuación, se procesa en nuestros potentes sistemas de seguimiento y procesamiento de malware mejorados con IA. Estos sistemas son capaces de descubrir y añadir mucha información contextual para enriquecer los datos de inteligencia.

Como elemento crucial, nuestros expertos en información sobre amenazas supervisan el producto final y se aseguran de que contenga siempre datos actualizados que te ayuden a tomar decisiones mejores y más rápidas.

Feeds de inteligencia propiedad de ESET

Enriquece tu visión del panorama mundial de amenazas basándote en una telemetría única. Los feeds de ESET provienen de nuestros centros de investigación en todo el mundo, proporcionando una imagen holística y permitiéndote bloquear rápidamente los IoC en tu entorno. Los feeds están en los formatos - JSON - STIX 2.1

FEED DE ARCHIVOS MALICIOSOS

Este feed proporciona información en tiempo real sobre muestras de malware recién descubiertas, sus características e IoC. Te ayuda a entender qué archivos maliciosos se están detectando y te permite bloquearlos de forma proactiva antes de que causen daños. El feed presenta dominios maliciosos, incluyendo hashes de archivos, marcas de tiempo, tipo de amenaza detectada y otra información detallada.

FEED DE DOMINIO

Este feed puede utilizarse para bloquear dominios considerados maliciosos. Incluye nombres de dominio, direcciones IP y las fechas asociadas a ellos. El feed clasifica los dominios en función de su gravedad, lo que te permite ajustar tu respuesta en consecuencia, por ejemplo, bloquear únicamente dominios de alta gravedad.

FEED IP

Este feed comparte las IP consideradas maliciosas y los datos asociados a ellas. La estructura de los datos es muy similar a la utilizada para los feeds de dominios y URL. El principal objetivo es entender qué IPs maliciosas prevalecen actualmente en la red, bloquear las IPs de mayor gravedad, detectar las de menor gravedad e investigar más a fondo.

FEED URL

De forma similar al Feed de Dominios, el Feed de URLs examina direcciones específicas. Incluye información detallada sobre datos relacionados con la URL, así como información sobre los dominios que las alojan. Toda la información se filtra para mostrar solamente resultados de alta confianza.

FEED BOTNET

Basado en la red de rastreo de botnets propiedad de ESET, el servicio Feed Botnet presenta tres tipos de subfeeds: botnet, C&C y objetivos. Los datos proporcionados incluyen elementos como detección, hash, última actividad, archivos descargados, direcciones IP, protocolos, objetivos y otra información.

FEED APT

Este feed está compuesto por información APT producida por la investigación de ESET. En general, el feed es una exportación del servidor MISP interno de ESET. Todos los datos que se comparten también están detallados en los informes APT. APT Feed también forma parte de APT Reports, pero puede adquirirse por separado.

Con los feeds de ESET, obtendrás

- ✓ DATOS ALTAMENTE ELABORADOS
- ✓ CONTENIDO PROCESABLE
- ✓ MÍNIMOS FALSOS POSITIVOS
- ✓ ACTUALIZACIONES FRECUENTES
- ✓ API COMPLETA

La disponibilidad de los informes y feeds de ESET Threat Intelligence varía según el país. Para obtener más información, contacta con tu representante local de ESET.

Acerca de ESET

Seguridad digital de última generación para las empresas

NO SOLO DETENEMOS LAS FILTRACIONES, SINO QUE LAS PREVENIMOS

A diferencia de las soluciones convencionales que se centran en reaccionar ante las amenazas después de que se hayan ejecutado, ESET ofrece un enfoque inigualable de prevención basado en IA respaldado por experiencia humana, reconocida Inteligencia de Amenazas y una extensa red de I+D liderada por investigadores de gran prestigio.Todo ello para la innovación continua de nuestra tecnología de seguridad multicapa.

Disfruta de una protección inigualable frente al ransomware, el phishing, las amenazas de día cero y los ataques dirigidos con nuestra galardonada plataforma de ciberseguridad XDR basada en la nube que combina funciones de prevención y detección proactiva de amenazas de última generación. Nuestras soluciones altamente personalizables incluyen soporte hiperlocal. Ofrecen un impacto mínimo en el rendimiento, identifican y neutralizan las amenazas emergentes antes de que puedan ejecutarse, garantizan la continuidad del negocio y reducen los costes de implementación y gestión.

En un mundo donde la tecnología permite el progreso, protege tu negocio con ESET.

ESET EN CIFRAS

1000M
de usuarios protegidos en todo el mundo

+400k
clientes de empresa

200
países y territorios

13
centros de I + D en el mundo

RECONOCIMIENTO DE LA INDUSTRIA

ESET es reconocido por más de 700 valoraciones recogidas en Gartner Peer Insights

ESET reconocida por su compromiso con la comunidad, recibe el premio Tech Cares 2023 de TrustRadius

RECONOCIMIENTO DE LOS ANALISTAS

En 2023, IDC situó a ESET entre los 5 principales proveedores de inteligencia de amenazas y destacó el papel de ESET Threat Intelligence.

ESET ha sido reconocida como 'Top Player', por cuarto año consecutivo, en el Cuadrante de Mercado de Protección contra Amenazas Persistentes Avanzadas (APT) 2023 de Radicati.

ESET es la principal empresa independiente de software de ciberseguridad, y se encuentra entre los 10 primeros de 354 colaboradores del marco de trabajo ATT&CK de MITRE.

CERTIFICADO DE SEGURIDAD ISO

ESET cumple la norma ISO/IEC 27001:2013, una norma de seguridad reconocida y aplicable internacionalmente en la implementación 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 CLIENTES

Protegido por ESET desde 2017, más de 9.000 equipos

Protegido por ESET desde 2016, más de 4.000 buzones de correo

Protegido por ESET desde 2016, más de 32.000 equipos

Distribuidor ISP desde 2008, 2 millones de clientes base

ALGUNOS DE NUESTROS PREMIOS

★★★★★

"LA IMPLEMENTACIÓN FUE MUY SENCILLA. CON LA COOPERACIÓN DEL EQUIPO TÉCNICO DE ESET, MUY BIEN CAPACITADO, PUDIMOS PONER EN MARCHA NUESTRA NUEVA SOLUCIÓN DE SEGURIDAD ESET EN POCAS HORAS".

Director de IT, Diamantis Masoutis S.A., Grecia, más de 6.000 puestos

★★★★★

"QUEDAMOS MUY IMPRESIONADOS CON EL SOPORTE Y LA ASISTENCIA QUE RECIBIMOS. ADEMÁS DE SER UN GRAN PRODUCTO, LA EXCELENTE ATENCIÓN Y ASISTENCIA QUE RECIBIMOS FUE LO QUE REALMENTE NOS LLEVÓ A MIGRAR TODOS LOS SISTEMAS DE PRIMORIS A ESET EN SU CONJUNTO."

Joshua Collins, Director de Operaciones del Centro de Datos, Primoris Services Corporation, EE.UU., más de 4.000 puestos