



FICHA DE SERVICIO

THREAT INTELLIGENCE

Feeds e informes de inteligencia únicos elaborados
por profesionales de referencia del sector

Progress. Protected.

¿Por qué añadir ESET a tu stack de CTI?

Comprender el panorama actual de amenazas y las tácticas empleadas por los ciberdelincuentes proporciona una ventaja crucial en materia de conocimiento. Esta visión permite a las empresas **reforzar sus sistemas de defensa internos de forma eficaz**. Los datos de inteligencia de alta calidad son la piedra angular de cualquier estrategia sólida de inteligencia sobre ciberamenazas (CTI).

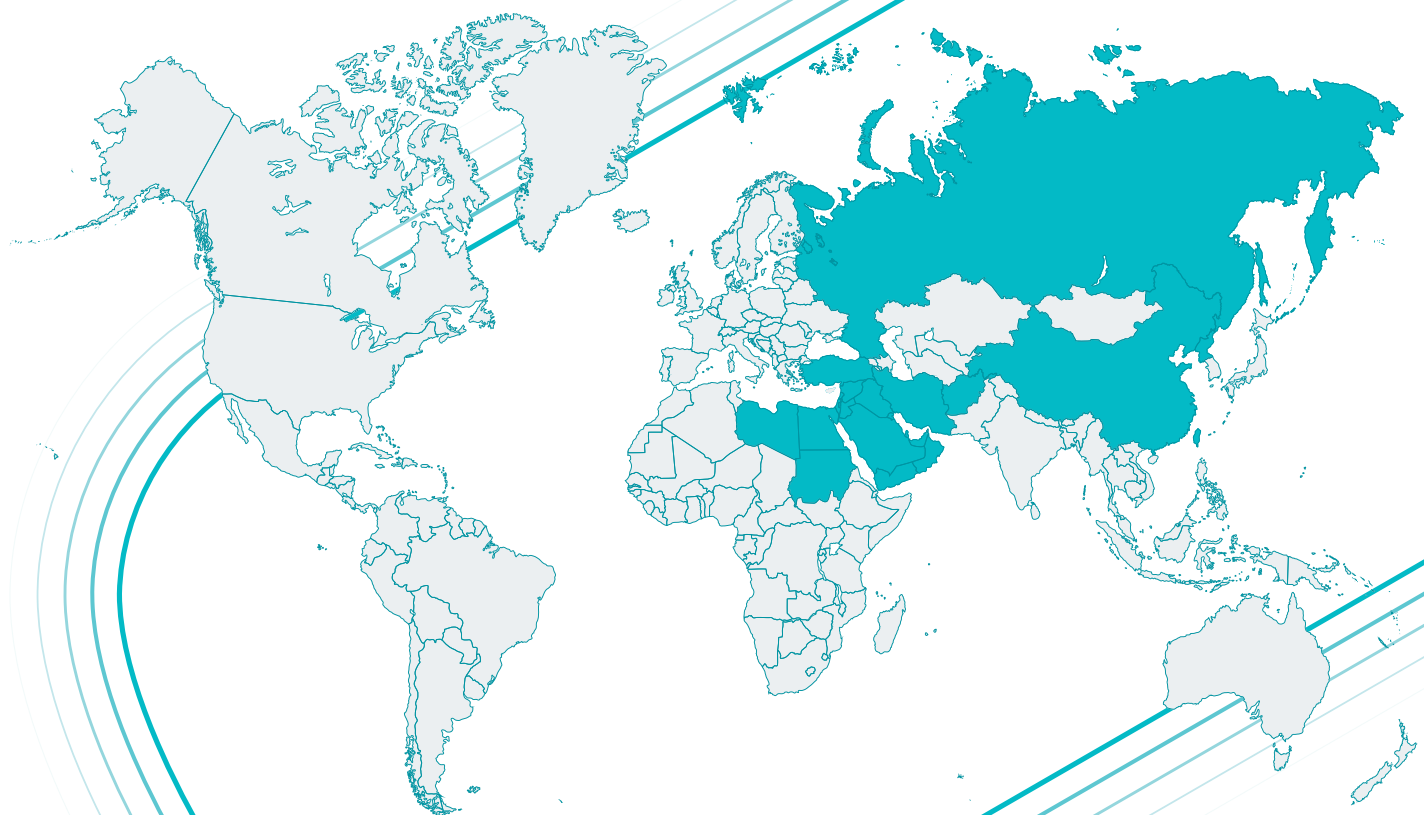
Desde hace más de 35 años, ESET es una empresa de capital privado, sin deudas y en crecimiento constante. Nuestro éxito se basa en un enfoque de "prevención primero" impulsado por IA y reforzado por experiencia humana. En el centro de nuestras operaciones está nuestra **inteligencia sobre amenazas exclusiva, respaldada por una amplia red de I+D dirigida** por investigadores

reconocidos en el sector. Nos tomamos el tiempo necesario para comprender de verdad las ciberamenazas, lo que nos permite defendernos de ellas con eficacia.

Por muy avanzadas que sean tus soluciones de CTI actuales, integrar **ESET en tu stack aportará un valor inigualable**. Nuestros completos feeds de inteligencia de amenazas, informes APT e informes de eCrime garantizan que te mantengas a la vanguardia frente a las amenazas emergentes, reforzando tus defensas existentes con información procesable e investigación de vanguardia.

Aprovecha la telemetría exclusiva de ESET

La presencia global de ESET, construida durante décadas, nos proporciona una **biblioteca de inteligencia rica y diversa** procedente de millones de nodos. A diferencia de muchos competidores, nuestra telemetría es especialmente sólida en regiones consideradas "**más interesantes**" desde un punto de **vista geopolítico** en el ámbito de la ciberdefensa. Esta cobertura única se traduce directamente en una inteligencia superior. Al aprovechar la telemetría de ESET, **obtaines acceso a información de alta calidad y procesable** que mejora tus capacidades de detección y respuesta ante amenazas.

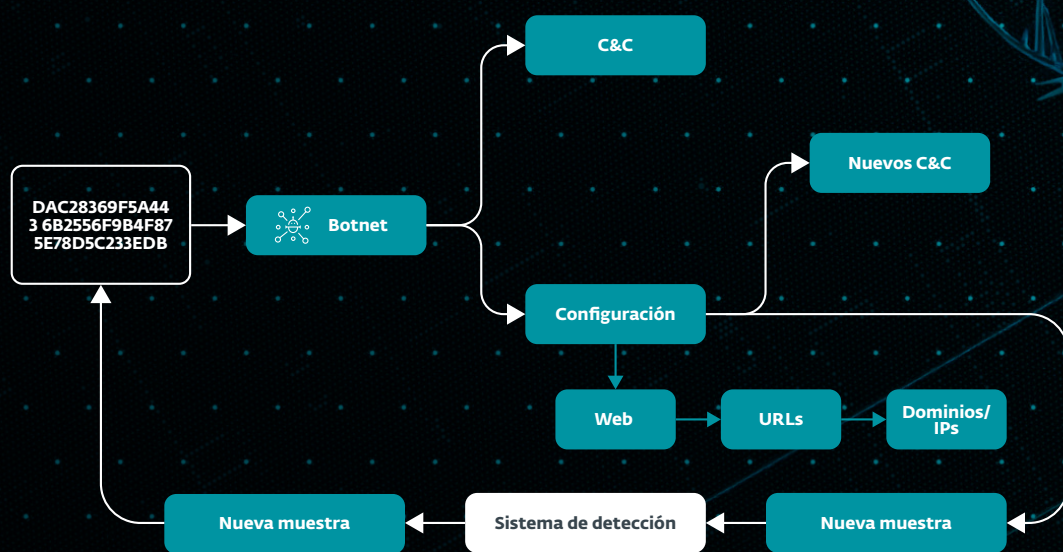


Inteligencia única y enriquecida para obtener información procesable

La inteligencia de amenazas no consiste solo en recopilar indicadores y presentarlos: ESET va mucho más allá. Empleamos tecnología avanzada y una amplia experiencia para procesar y enriquecer nuestra inteligencia sobre amenazas, garantizando que aporte un valor real a tu negocio.

- 1. Telemetría integral:** Nuestra inteligencia parte de una amplia gama de telemetría generada por ESET LiveSense, nuestra tecnología de seguridad multicapa integrada dentro de la plataforma ESET PROTECT. Esto garantiza una recopilación de datos amplia y profunda desde fuentes diversas.
- 2. Métodos de recopilación diversos:** Además de LiveSense, utilizamos varios métodos de recopilación y monitorización, como honeypots, sensores, recursos OSINT, rastreo web (tanto en la web visible como en la profunda) y Threat Tracking. Esto genera un volumen considerable de datos de alta calidad.
- 3. Procesamiento avanzado:** Una vez recopilados, todos los datos se procesan a través de nuestros robustos sistemas backend, que utilizan IA para clasificar y analizar la información de forma automática. Esto garantiza que solo se muestre la información más relevante y útil.
- 4. Análisis experto:** Más allá del procesamiento automatizado, nuestro equipo cualificado de analistas e investigadores de inteligencia sobre amenazas desempeña un papel crucial. Estudian y analizan continuamente a los distintos actores de amenazas, sus motivaciones, TTP (tácticas, técnicas y procedimientos) y herramientas. Esta verificación humana añade una capa adicional de profundidad y precisión a nuestra inteligencia, yendo más allá de lo que el machine learning y la automatización pueden lograr por sí solos.





Las muestras que recibimos mediante telemetría se someten a un análisis conductual y estructural en profundidad. Este proceso genera indicadores útiles adicionales que enriquecen aún más nuestra inteligencia de amenazas. Al examinar minuciosamente cada muestra, extraemos información valiosa que mejora la calidad y eficacia general de nuestra inteligencia, ofreciéndote una comprensión más completa del panorama de amenazas.

Seguridad superior gracias a los informes APT detallados

Redactados en un lenguaje claro y procesable para mejorar la postura de seguridad de tu empresa, nuestros informes APT ofrecen información detallada sobre campañas de malware, su distribución y los actores implicados. Accede a nuestro servidor MISP y a ESET LiveAI, y reserva sesiones en directo con los principales expertos en inteligencia de amenazas de ESET para obtener una inteligencia completa y procesable.

NUESTRA MEJOR INVESTIGACIÓN AL ALCANCE DE TU MANO

Nuestro equipo de investigación es muy conocido en el sector de la seguridad digital gracias a nuestro galardonado blog [WeLiveSecurity](#). La excelente investigación del equipo y los resúmenes de actividad APT están disponibles, junto con mucha más información detallada. Los clientes de ESET obtienen un acceso anticipado y exclusivo a todo el contenido de WeLiveSecurity.

CONTENIDO SELECCIONADO Y PRÁCTICO

Los informes ofrecen mucho contexto sobre lo que está ocurriendo y por qué. Gracias a esto, las empresas pueden prepararse con antelación ante lo que pueda venir. Y lo que es importante, nuestros expertos se aseguran de que el contenido sea fácil de entender.

TOMA DECISIONES CRUCIALES CON RAPIDEZ

Todo esto ayuda a las empresas a tomar decisiones cruciales y ofrece una ventaja estratégica en la lucha contra el crimen digital. Aporta una comprensión de lo que ocurre en el "lado oscuro de Internet" y proporciona un contexto crucial, para que tu empresa pueda hacer preparativos internos con rapidez.

ACCESO A UN ANALISTA DE ESET

Todos los clientes que contraten el paquete APT Reports Premium también tendrán acceso a un analista de ESET durante un máximo de cuatro horas al mes. Esto ofrece la oportunidad de tratar los temas con más profundidad y ayudar a resolver cualquier cuestión pendiente.



ESET LiveAI utiliza IA avanzada y experiencia en APT para ofrecer información y medidas de protección bajo demanda frente a los ciberataques. Disponible como chatbot, responde a consultas de seguridad, ofrece resúmenes de APT, recopila IOC y TTP, y genera reglas YARA para una comprensión y prevención rápidas de las amenazas.

		Informes APT	Informes APT Advanced	Informes APT Ultimate
Resumen quincenal de actividad	Informes que resumen la actividad de todos los grupos APT cubiertos anteriormente (dos informes al mes)	✓	✓	✓
Informes de análisis de amenazas	Análisis técnico personalizado o periódico de las amenazas más frecuentes (aproximadamente 30 al año)	✓	✓	✓
Panorámica mensual	Recopilación mensual de información con una visión general ejecutiva de las amenazas	✓	✓	✓
Resumen mensual	Índice y resumen ejecutivo de los informes y acontecimientos del mes	✓	✓	✓
Acceso anticipado a WeLiveSecurity	Acceso anticipado a los informes sobre amenazas y a una selección de artículos de WeLiveSecurity	✓	✓	✓
Feed de IOC de APT	Acceso completo al feed STIX/TAXII que contiene los IOC de los informes	✓	✓	✓
Acceso al servidor MISP	Acceso completo al servidor MISP de ESET, que contiene toda la información disponible en los informes	✗	✓	✓
ESET LiveAI	Acceso a ESET LiveAI, que proporciona información y resúmenes de los informes APT disponibles	✗	✓	✓
Acceso a analistas	Acceso a analistas a través de diversas plataformas, como MS Teams y correo electrónico, limitado a cuatro horas al mes (no acumulables, incluido el tiempo de preparación)	✗	✗	✓

De los indicadores a la inteligencia: supera al eCrime

Los informes de eCrime de ESET Threat Intelligence proporcionan información detallada sobre el ransomware y las operaciones de ciberdelincuencia en un sentido más amplio. Obtén visibilidad sobre las herramientas, la infraestructura y las estrategias de monetización de los atacantes, respaldada por la investigación y la telemetría globales de ESET. Ve más allá de los IOC para acceder a inteligencia contextual que refuerza la defensa proactiva y la toma de decisiones estratégicas.

Qué diferencia a los informes ESET eCrime

DEFENSA PROACTIVA

Obtén inteligencia no solo sobre los grupos de eCrime, sino también sobre los afiliados que realmente llevan a cabo los ataques. Descubre cómo operan y anticipáte a sus próximos movimientos para mantenerte un paso por delante.

EFICIENCIA OPERATIVA

Utiliza información clara y depurada procedente de incidentes reales para eliminar el ruido. Facilita que tu equipo detecte amenazas, responda más rápido y enfoque la búsqueda donde realmente importa.

VISIBILIDAD EXCLUSIVA

Ve más allá de los feeds públicos de amenazas con una visión más profunda de las tácticas de monetización, la infraestructura y el comportamiento de los afiliados, respaldada por la investigación y la telemetría de ESET.

		Informes eCrime	Informes eCrime Advanced
Resumen de actividad MENSUAL	- Las últimas campañas de ransomware e infostealers, resumidas en información clara y estratégica - A quién se dirigen, cómo se desarrollan los ataques y qué falló - Lecciones clave, IOC y recomendaciones para reforzar la resiliencia	✓	✓
Análisis técnico PERIÓDICAMENTE	- Análisis en profundidad de actores de amenazas concretos (p. ej. FIN7) - Cadena de ataque completa: desde el acceso inicial hasta el robo de datos - Tácticas, herramientas e infraestructura de los ciberdelincuentes; mapeo con MITRE ATT&CK®; indicadores de compromiso (IOC)	✓	✓
Resumen mensual MENSUAL	- Visión general, lista para dirección, de la actividad reciente de ransomware/infostealers - Tendencias clave, incidentes destacados y amenazas emergentes - Ayuda a la dirección a evaluar el riesgo y fijar prioridades sin complejidad técnica	✓	✓
Feed de eCrime	- IOC recientes y depurados sobre bandas de ransomware, sus afiliados y campañas de infostealers - Disponible en el formato estándar STIX/TAXII	✓	✓
ESET LiveAI	- Utiliza la información de eCrime para responder preguntas relacionadas con amenazas - Ayuda a interpretar los incidentes y el comportamiento de los ciberdelincuentes - Facilita el acceso inmediato a la inteligencia sobre amenazas para equipos y responsables de la toma de decisiones	✗	✓
Acceso al servidor MISP	- Integración directa con inteligencia sobre amenazas seleccionada - Ingesta automática de IOC para reforzar las defensas - Agiliza los flujos de trabajo, acelera la detección y respalda la respuesta a incidentes	✗	✓

Feeds de datos claros y concisos

Mejora tu visión del panorama de amenazas con la telemetría única de ESET. Ofrecemos feeds de datos altamente depurados en JSON y STIX 2.1, que se integran sin fricciones en herramientas SIEM, TIP o SOAR. A diferencia de muchos proveedores de inteligencia sobre amenazas, prestamos muchísima atención a que **nuestros feeds estén meticulosamente filtrados y evaluados** para garantizar su relevancia. Esto permite que los sistemas de seguridad existentes realicen acciones automáticas cuando sea necesario, ofreciendo a los analistas de inteligencia de amenazas una visión completa del panorama de amenazas global.

- Datos completos en metadatos, detallados y seleccionados, con un índice de falsos positivos muy bajo
- Garantizamos datos de tamaño reducido, altamente relevantes, deduplicados y con puntuación de confianza
- Son el resultado de un filtrado avanzado, con información aportada por los investigadores de ESET
- Líderes del mercado, especialmente en datos de botnets
- Requisitos de mantenimiento reducidos gracias a un contenido debidamente seleccionado
- Feeds en tiempo real: solo IOC (indicadores de compromiso) recientes y prevalentes

FEED DE DATOS MALICIOSOS

Información en tiempo real sobre muestras de malware recién descubiertas, sus características e IOC. Incluye hashes de archivo, marcas de tiempo y tipos de amenaza para ayudarte a bloquear archivos maliciosos antes de que causen daño.

FEED DE RANSOMWARE

Datos en tiempo real sobre familias de ransomware activas y muestras prevalentes. Permite un bloqueo proactivo para prevenir filtraciones y costosas interrupciones.

FEED DE BOTNETS

Impulsado por el rastreador de botnets de ESET, este feed incluye tres subfeeds: botnets, C&C y objetivos. Proporciona detalles de detección, hashes de archivo, marcas de tiempo de la última comunicación, archivos descargados, IP, protocolos e información sobre los objetivos.

FEED DE IOC DE APT

Información sobre amenazas persistentes avanzadas basada en la investigación de ESET. Exportado desde el servidor MISP interno de ESET y alineado con los informes sobre APT. Disponible como parte de los informes o como feed independiente.

FEED DE PUA Y ADWARE

ESET cuenta con más de dos décadas de experiencia en la clasificación de PUA (aplicaciones potencialmente no deseadas), lo que otorga a su inteligencia una profundidad y precisión inigualables. Los feeds de adware proporcionan información en tiempo real sobre el adware activo y amenazas similares, permitiendo un bloqueo proactivo antes de que causen impacto.

FEED DE APLICACIONES PUA DE USO DUAL

Rastrea herramientas legítimas (p. ej., RMM) utilizadas indebidamente por atacantes, ayudándote a anticiparte a este uso indebido mientras se reduce el ruido gracias a datos específicos y de baja redundancia.

FEED DE DOMINIOS

Ofrece datos sobre dominios maliciosos, incluyendo el nombre de dominio, la dirección IP y la fecha asociada. Los dominios se clasifican por gravedad, lo que te permite priorizar acciones como el bloqueo de dominios de alto riesgo.

FEED DE URL

Un feed depurado de URL específicas con información detallada sobre cada dirección y los dominios que la alojan. Incluye únicamente hallazgos de alta confianza, respaldados por explicaciones claras y legibles para las URL marcadas.

FEED DE IP

Recibe datos procesables sobre IP maliciosas. La estructura refleja la de los feeds de dominios y URL. Utilízalo para identificar amenazas comunes, bloquear IP de alta gravedad, monitorizar las de menor riesgo e investigar más a fondo usando datos adicionales para evaluar el posible daño.

FEED DE AMENAZAS PARA ANDROID

Ofrece información en tiempo real sobre las amenazas de Android más prevalentes y sus IOC, permitiendo un bloqueo proactivo. Creado a partir de la telemetría de ESET, se actualiza casi en tiempo real con deduplicación diaria.

FEED DE INFOTEALERS DE ANDROID

Un feed especializado dentro de las amenazas de Android, con detalles sobre muestras de infostealers actuales y datos relacionados. Obtén información sobre familias activas y bloquéalas de forma proactiva antes de que causen daño.

FEED DE URL DE ESTAFAS

Anticípate a las estafas con datos en tiempo real sobre URL fraudulentas. Cubre tiendas electrónicas, estafas de inversión, estafas de citas y estafas de criptomonedas. Creado a partir de todas las fuentes de URL de ESET casi en tiempo real; la deduplicación se produce cada 24 horas.

FEED DE CRIPTOESTAFAS

Anticípate a las criptoestafas con actualizaciones en tiempo real sobre dominios, URL y datos asociados de estafas. Procedente de la extensa telemetría de ESET, ofrece información temprana y específica para ayudarte a bloquear proactivamente las amenazas y proteger tus activos.

FEED DE ARCHIVOS ADJUNTOS MALICIOSOS EN CORREOS

El correo electrónico es un objetivo prioritario de los ataques. Este feed ofrece datos en tiempo real sobre archivos adjuntos de correo maliciosos, procedentes de la extensa telemetría de escaneo de correo de ESET.

FEED DE URL DE PHISHING

Ofrece información en tiempo real sobre URL de phishing activas procedentes de la base de datos específica de ESET. Actualizado continuamente con deduplicación diaria, este feed te ayuda a detectar y bloquear sitios fraudulentos antes de que comprometan datos sensibles.

FEED DE SMISHING

Ofrece información oportuna sobre phishing por SMS (smishing), incluyendo dominios, URL e indicadores relacionados. Procedente de la extensa telemetría de ESET, se actualiza casi en tiempo real con deduplicación diaria.

FEED DE ESTAFAS POR SMS

Protégete frente a las estafas por SMS con un feed en tiempo real sobre dominios y URL maliciosos. Actualizado casi en tiempo real a partir de la extensa telemetría de ESET y deduplicado a diario, te ayuda a identificar y bloquear amenazas sofisticadas.

FEED DE ECRIME

Obtén datos claros y procesables sobre operaciones de cibercrimen y eCrime habilitado por malware, monitorizando desde bandas de ransomware y sus afiliados hasta campañas de infostealers, para que tu equipo pueda pasar de reaccionar a defender proactivamente tu empresa.

Descubre el poder de ESET Threat Intelligence

Programa una demo con nosotros hoy mismo y descubre el valor inigualable que ESET Threat Intelligence puede aportar a tu empresa. Con una tasa de renovación del 100 %, nuestros clientes satisfechos son un testimonio de la eficacia de nuestras soluciones. Deja que te mostremos cómo podemos reforzar tus defensas de ciberseguridad.

¿Aún no estás listo para una llamada de demostración?

Empieza creando [una cuenta de prueba](#) en el portal de ESET Threat Intelligence para explorar los feeds y los informes.

Esto es ESET

Ciberseguridad diseñada para ofrecer confianza y control

ESET ofrece soluciones de ciberseguridad diseñadas específicamente para que las empresas y los particulares puedan alcanzar la independencia digital en un mundo cada vez más impulsado por la IA.

Con sede en la Unión Europea y de propiedad privada, ESET desarrolla tecnologías propias de ciberseguridad basadas en la inteligencia artificial y modelos de IA soberanos diseñados para proteger el ecosistema digital y la infraestructura de IA.

Cada solución que crea ESET se basa en más de 35 años de experiencia en ciberseguridad, incorporando la experiencia humana, el criterio y los valores humanos a cada decisión. Combinado con un enfoque proactivo centrado en la prevención, ESET protege frente a las ciberamenazas convencionales y las impulsadas por IA. Basándose en el rigor científico y con el respaldo de 11 centros de I+D repartidos por todo el mundo, ESET impulsa continuamente la investigación y la innovación para ofrecer una ciberseguridad sencilla y siempre supervisada por expertos. Sus tecnologías son validadas de forma constante por las principales empresas de pruebas independientes.

ESET protege a millones de usuarios y empresas en 178 países. Guiada por su compromiso con una IA responsable y la confianza de los clientes, ESET protege el progreso que la tecnología hace posible.

ESET EN CIFRAS

+1.000M

de usuarios protegidos
en todo el mundo

+500k

clientes de empresa

178

países

11

centros de I+D en todo
el mundo

ALGUNOS DE NUESTROS CLIENTES



protegidos por ESET
desde 2017: más de 9.500
dispositivos



protegidos por ESET desde
2019: 1.200 dispositivos
y 2.700 buzones de correo

Canon

Canon Marketing Japan Group

protegidos por ESET desde
2016: más de 23.000
dispositivos



socio de seguridad de ISP
desde 2008: 2 millones
de clientes

RECONOCIMIENTOS



Ganador de los premios **al mejor endpoint para empresas y al mejor endpoint para pequeñas empresas** en los SE LABS Awards 2025



Nombrado **«Customers' Choice»** en el informe **«Voice of the Customer»** de Gartner® Peer Insights™ sobre plataformas de protección de endpoint de 2026

FROST & SULLIVAN

Nombrado **«líder»** en el informe «Frost Radar: Endpoint Security 2025», lo que demuestra su excelencia en crecimiento e innovación

Gartner y Peer Insights™ son marcas comerciales de Gartner, Inc. y/o sus filiales. Todos los derechos reservados. El contenido de Gartner Peer Insights consiste en las opiniones de usuarios finales individuales basadas en sus propias experiencias, y no debe interpretarse como declaraciones de hechos, ni representa las opiniones de Gartner o sus filiales. Gartner no respalda a ningún proveedor, producto o servicio representado en este contenido, ni ofrece ninguna garantía, expresa o implícita, con respecto a este contenido, sobre su exactitud o integridad, incluida cualquier garantía de comerciabilidad o idoneidad para un fin determinado.