FICHA DE PRODUCTO

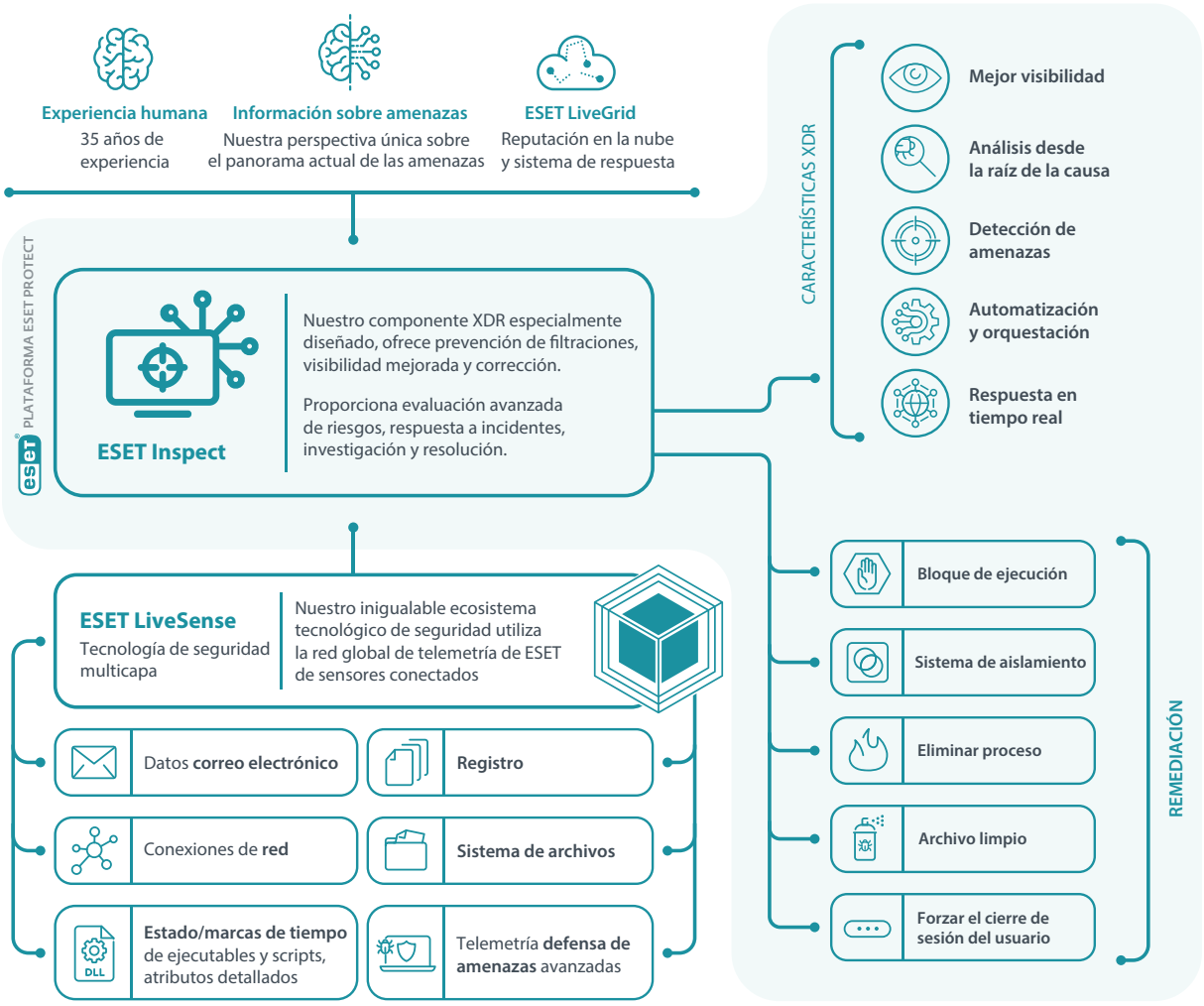
INSPECT

El componente XDR de la plataforma ESET PROTECT, ofrece prevención de filtraciones, visibilidad mejorada y reparación

¿Qué es una **solución de detección y respuesta (XDR)?**

ESET Inspect, el componente de la plataforma ESET PROTECT, es una herramienta para identificar comportamientos anómalos y filtraciones, evaluación de riesgos, respuesta a incidentes, investigaciones y reparación.

Permite a los responsables responder a incidentes, monitorizar y evaluar todas las actividades de la red y de los dispositivos conectados. También ayuda a automatizar las acciones correctivas inmediatas, en caso necesario. Las más de 800 reglas de detección (y en aumento) de ESET permiten una detección exhaustiva de amenazas.



Digital Security
Progress. Protected.

ESET marca la diferencia

PREVENCIÓN, DETECCIÓN Y RESPUESTA COMPLETAS

Permite un rápido análisis y corrección de cualquier problema de seguridad en tu red. La seguridad multicapa de ESET, en la que cada una de las capas envía datos a ESET Inspect, analiza grandes cantidades de datos en tiempo real para que ninguna amenaza pase desapercibida.

SOLUCIÓN DE UN FABRICANTE QUE DA PRIORIDAD A LA SEGURIDAD

ESET lleva más de 30 años luchando contra las ciberamenazas. Como empresa de base científica, lleva mucho tiempo a la vanguardia de desarrollos como el aprendizaje automático, la tecnología en la nube y ahora XDR.

MÁS VALE PREVENIR QUE CURAR

El enfoque de ESET respecto a la XDR está estrechamente relacionado con sus productos de prevención, que han sido premiados en varias ocasiones. Gracias a su compromiso de desarrollar tecnología de detección de alta calidad, la tecnología de prevención de ESET es líder mundial.

VISIBILIDAD DETALLADA DE LA RED

Con reglas de detección transparentes (ESET tiene más de 800 y seguimos aumentando), indicadores avanzados de peligro (IoC) y capacidad de búsqueda, una revisión exhaustiva de tu red te permitirá identificar cualquier cosa sospechosa.

FLEXIBILIDAD DE IMPLEMENTACIÓN

Te dejamos decidir cómo implementar tu solución de seguridad: ESET Inspect puede ejecutarse a través de tus propios servidores en local, o a través de una instalación basada en la nube, lo que te permite ajustar la configuración en función de tus objetivos de TCO y de la capacidad del hardware.

CREACIÓN AUTOMÁTICA DE INCIDENCIAS

Obtén una visibilidad perfecta con incidentes bien visualizados. ESET Inspect correlaciona grandes cantidades de datos para encontrar eventos desde la raíz de la causa y compilarlos en incidentes completos para que puedas resolverlos inmediatamente.

LISTO PARA EMPEZAR A TRABAJAR AHORA

La solución de ESET funciona de forma inmediata, pero es lo suficientemente potente para permitir la modificación granular por parte de detectores de amenazas experimentados.

MITRE ATT&CK

ESET Inspect hace referencia a sus detecciones en el programa MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™), que, con un solo clic, te ofrece información completa incluso sobre las amenazas más complejas.

SISTEMA DE REPUTACIÓN

El amplio filtrado de ESET permite a los expertos en seguridad filtrar todas las aplicaciones buenas conocidas utilizando el robusto sistema de reputación de archivos de ESET. Nuestro sistema de reputación contiene una base de datos de cientos de millones de archivos legítimos para garantizar que los equipos de ciberseguridad inviertan su tiempo en combatir las amenazas desconocidas y potencialmente maliciosas y no en los falsos positivos.

AUTOMATIZACIÓN Y PERSONALIZACIÓN

Ajusta fácilmente ESET Inspect al nivel de detalle y automatización que necesites. Elige el nivel de interacción deseado, y el tipo y la cantidad de datos que se van a almacenar, durante la configuración inicial y con la ayuda de los perfiles de usuario preestablecidos, y luego deja que el Modo de Aprendizaje elabore un mapa del entorno de tu empresa y sugiera exclusiones a los falsos positivos cuando sea necesario.

eset Digital Security
Progress. Protected.

Características de la solución

SISTEMA DE GESTIÓN DE INCIDENTES

Agrupa detecciones, equipos, ejecutables o procesos en unidades lógicas para ver posibles eventos maliciosos en una franja de tiempo, con acciones de usuario relacionadas. ESET Inspect sugiere automáticamente al encargado de responder a los incidentes todos los eventos y objetos relacionados que pueden ser de gran ayuda en las etapas de clasificación, investigación y resolución de un incidente.

OPCIONES DE RESPUESTA EN TIEMPO REAL

ESET Inspect viene provisto de acciones de respuesta fácilmente accesibles con un solo clic, como reiniciar y apagar un equipo, aislar los equipos del resto de la red, ejecutar un análisis bajo demanda, eliminar cualquier proceso en ejecución y bloquear cualquier aplicación en función de su valor hash. Además, gracias a la opción de respuesta en tiempo real de ESET Inspect, denominada Terminal, los profesionales de la seguridad pueden beneficiarse de todo el conjunto de opciones de investigación y reparación de PowerShell.

ANÁLISIS DESDE LA RAÍZ DE LA CAUSA

Visualiza fácilmente el análisis desde la raíz del problema, y el mapa de procesos completo, de cualquier cadena de eventos potencialmente maliciosos, profundiza en el nivel de detalle deseado y toma decisiones basadas en el amplio contexto proporcionado y en las explicaciones de las causas tanto benignas como maliciosas, elaboradas por nuestros expertos en malware.

API PÚBLICA

ESET Inspect cuenta con una API REST pública que permite acceder y exportar las detecciones y su reparación para permitir una integración efectiva con herramientas como SIEM, SOAR, herramientas de ticketing y muchas otras.

MÚLTIPLES INDICADORES DE COMPROMISO

Examina y bloquea módulos basados en más de 30 indicadores diferentes, incluyendo hash, modificaciones del registro, modificaciones de archivos y conexiones de red.

DETECCIÓN DE AMENAZAS

Utiliza la potente búsqueda IOC basada en consultas y aplica filtros a los datos sin procesar para clasificarlos en función de la popularidad de los archivos, reputación, firma digital, comportamiento u otra información contextual. La configuración de varios filtros permite la detección automatizada y sencilla de amenazas y la respuesta a incidentes, incluyendo la capacidad de detectar y detener APTs y ataques dirigidos.

ACCESO REMOTO SEGURO Y SIN COMPLICACIONES

La respuesta a incidentes y los servicios de seguridad son tan fluidos como la facilidad con la que se accede a ellos, tanto en lo que respecta a la conexión del responsable del incidente con la consola, como a la conexión con los equipos de destino. La conexión funciona a una velocidad prácticamente en tiempo real y con las máximas medidas de seguridad aplicadas, todo ello sin necesidad de herramientas de terceros.

AISLAMIENTO CON UN SOLO CLIC

Define políticas de acceso a la red para detener rápidamente los movimientos laterales de malware.
Aísla de la red un dispositivo comprometido con un solo clic en la interfaz de ESET Inspect. Además, elimina fácilmente los dispositivos del estado de contención.

DETECCIÓN DE ANOMALÍAS Y COMPORTAMIENTOS

Comprueba las acciones llevadas a cabo por un ejecutable y utiliza el sistema de reputación LiveGrid® de ESET para evaluar rápidamente si los procesos ejecutados son seguros o sospechosos. La monitorización de incidentes anómalos relacionados son posibles gracias a reglas específicas escritas para ser activadas por el comportamiento, no por simples detecciones de malware o firmas. La agrupación de ordenadores por usuario o departamento permite a los equipos de ciberseguridad identificar si el usuario está autorizado a realizar una acción específica o no.

ETIQUETADO

Asigna y deniega etiquetas para un filtrado rápido a objetos de ESET Inspect como ordenadores, alarmas, exclusiones, tareas, ejecutables, procesos y scripts. Las etiquetas se comparten entre los usuarios y, una vez creadas, pueden asignarse en cuestión de segundos.

DETECCIÓN DE INCUMPLIMIENTO DE LA POLÍTICA DE LA EMPRESA

Bloquea la ejecución de módulos maliciosos en cualquier ordenador de la red de tu empresa. La arquitectura abierta de ESET Inspect ofrece la flexibilidad necesaria para detectar los incumplimientos de las políticas que se aplican al uso de software específico como las aplicaciones torrent, el almacenamiento en la nube, la navegación Tor u otro software no deseado.

ARQUITECTURA ABIERTA E INTEGRACIONES

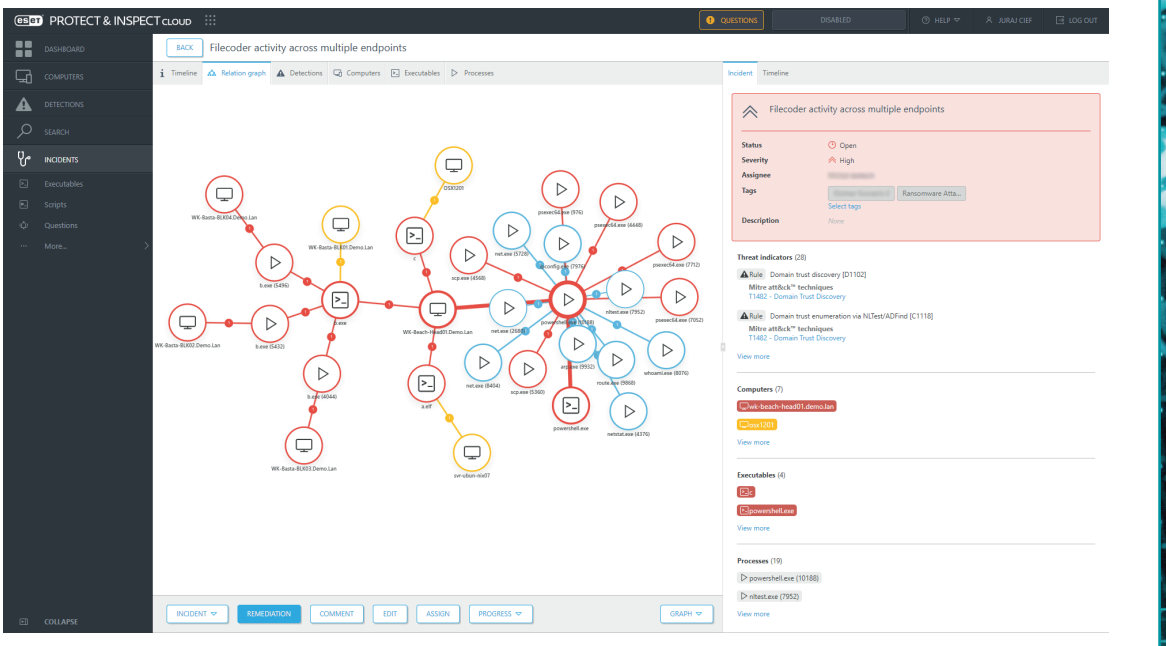
ESET Inspect proporciona una detección basada en el comportamiento y la reputación para los equipos de seguridad. Todas las reglas se pueden editar fácilmente mediante XML para permitir un ajuste preciso o crearse fácilmente para satisfacer las necesidades de entornos empresariales específicos, incluidas las integraciones SIEM.

PUNTUACIÓN AVANZADA

Prioriza la gravedad de las alarmas con una funcionalidad de puntuación que atribuye un valor de gravedad a los incidentes y permite al administrador identificar fácilmente los ordenadores con una mayor probabilidad de un incidente potencial.

OBTENCIÓN DE DATOS LOCALES

Examina datos completos sobre un proceso recién ejecutado,incluyendo la hora de ejecución, el usuario que lo ejecutó, el tiempo de permanencia y los dispositivos atacados. Todos los datos se almacenan localmente para evitar la fuga de datos sensibles.



Casos de uso

Detección del comportamiento y acciones recurrentes de los atacantes

PROBLEMA

En tu red, tienes usuarios que son reincidentes cuando se trata de malware. Los mismos usuarios siguen infectándose una y otra vez. ¿Es debido a un comportamiento imprudente? ¿O son el objetivo con más frecuencia que otros usuarios?

SOLUCIÓN

- ✓ Visualiza fácilmente los usuarios y dispositivos problemáticos.
- ✓ Completa fácilmente un análisis de las causas que han provocado el problema de seguridad para encontrar el foco de las infecciones.
- ✓ Remedia los vectores de infección encontrados, como el correo electrónico, web o dispositivos USB.

Detección y bloqueo de amenazas

PROBLEMA

Tu sistema de alerta temprana o tu centro de operaciones de seguridad (SOC) te proporciona una nueva alerta de amenazas. ¿Cuáles son tus siguientes pasos?

SOLUCIÓN

- ✓ Aprovecha el sistema de alerta temprana para recopilar datos sobre las nuevas o futuras amenazas.
- ✓ Busca en todos los equipos la existencia de una nueva amenaza.
- ✓ Bloquea la amenaza para evitar que se infiltre en una red o que se ejecute dentro de la estructura de la empresa.

eset® Digital Security
Progress. Protected.

Fácil instalación y respuesta sin la intervención del equipo de seguridad

PROBLEMA

No todas las empresas tienen equipos de ciberseguridad especializados y, por tanto, añadir e implementar las reglas de detección avanzadas puede ser complicado.

SOLUCIÓN

- ✓ Más de 300 reglas preconfiguradas incorporadas.
- ✓ Respuesta fácil y rápida para bloquear, eliminar o poner en cuarentena con un solo clic.
- ✓ Las soluciones y pasos a seguir se convierten en alarmas.
- ✓ Las reglas se pueden editar a través del lenguaje XML para permitir un fácil ajuste o creación de nuevas reglas.

Visibilidad de la red

PROBLEMA

Algunas empresas están preocupadas por determinadas aplicaciones que los usuarios utilizan en sus equipos. No solo deberías preocuparte por las instaladas de manera habitual, sino que también tendrías que revisar las móviles, que en realidad no se instalan. Pero, ¿cómo puedes controlarlas?

SOLUCIÓN

- ✓ Accede fácilmente y filtra todas las aplicaciones instaladas en los dispositivos.
- ✓ Visualiza y filtra todos los scripts de los dispositivos.
- ✓ Bloquea fácilmente todos los scripts no autorizados o las aplicaciones para que no se ejecuten.
- ✓ Notifica a los usuarios sobre las aplicaciones no autorizadas y desinstálalas automáticamente.

Detección profunda de amenazas - ransomware

PROBLEMA

Una empresa quiere herramientas adicionales para detectar el ransomware de forma proactiva, además de recibir notificaciones rápidamente si se detecta un comportamiento parecido a este tipo de malware en la red.

SOLUCIÓN

- ✓ Reglas de entrada para detectar aplicaciones cuando se ejecutan desde carpetas temporales.
- ✓ Introduce reglas para detectar archivos de MS Office (Word, Excel, PowerPoint) cuando ejecuten scripts adicionales o ejecutables.
- ✓ Alerta si alguna de las extensiones más comunes de ransomware se detecta en un dispositivo.
- ✓ Visualiza las alertas de Ransomware Shield de ESET Endpoint Security Solutions en la misma consola.

Entorno de investigación y remediación

PROBLEMA

La calidad de los datos depende de su entorno. Para tomar las decisiones adecuadas, necesitas saber cuáles son las alertas, en qué dispositivos tienen lugar y qué usuarios las activan.

SOLUCIÓN

- ✓ Identifica y agrupa los ordenadores de forma manual o automática con Directorio Activo.
- ✓ Permite o bloquea aplicaciones o scripts basados en el conjunto de ordenadores.
- ✓ Permite o bloquea aplicaciones o scripts basados en los usuarios.
- ✓ Recibe únicamente notificaciones de ciertos grupos.

ESET Digital Security
Progress. Protected.

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

ALGUNOS DE NUESTROS CLIENTES

MITSUBISHI MOTORS
Drive your Ambition

Protegido por ESET desde 2017, más de 9.000 equipos

Allianz Suisse

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

Canon Marketing Japan Group

Protegido por ESET desde 2016, más de 32.000 equipos

Distribuidor ISP desde 2008, 2 millones de clientes base

RECONOCIMIENTO

AV comparatives APPROVED Business Security JUL 2023

ESET recibió el premio Business Security APPROVED de AV-Comparatives en el Business Security Test en julio de 2023.

Leader SUMMER 2023

ESET consigue de manera consecutiva las mejores clasificaciones en la plataforma global de revisión de usuarios G2 y sus soluciones son apreciadas por clientes de todo el mundo.

The Radicati Group, Inc.
A TECHNOLOGY MARKET RESEARCH FIRM

ESET ha sido reconocida como "Top Player" por cuarto año consecutivo en el Cuadrante de Mercado de Amenazas persistentes avanzadas 2023 de Radicati.