Kaspersky®
Endpoint Security
for Business

Protección frente a amenazas

Cualquier solución de seguridad solo es eficaz en la medida en que lo es el motor de prevención de amenazas en la que está integrada. La gestión de parches, el cifrado, el control de aplicaciones. Todas estas tecnologías proporcionan una valiosa seguridad adicional, pero no pueden ni van a compensar las deficiencias en la protección contra amenazas fundamental.

La protección contra amenazas se sitúa en el núcleo de cada una de nuestros productos, soluciones y servicios de seguridad. Nuestro enfoque adaptable a varios niveles se basa en una amplia gama de componentes, muchos de ellos únicos, desarrollados para luchar contra las diferentes formas de ciberamenazas en diferentes niveles. El resultado es un arsenal de tecnologías defensivas y proactivas antiamenazas de próxima generación que, de forma conjunta, permiten detectar, mitigar y evitar rápidamente las amenazas más sofisticadas y avanzadas de hoy en día, e incluso las del futuro.

Experiencia e investigación relacionadas con las amenazas

Protección de última generación basada en nuestro exclusivo enfoque HuMachine™, que aprovecha la combinación de los puntos fuertes del aprendizaje automático, la experiencia humana y la completa inteligencia sobre amenazas. Kaspersky Lab ha liderado siempre el terreno en el ámbito de la inteligencia sobre amenazas: hemos descubierto más APT que cualquier otro proveedor, y nuestro compromiso con la inversión en tecnologías de protección del futuro se refleja en el tamaño y la reputación global de nuestros equipos de investigación.

Kaspersky EDR: una auténtica herramienta de búsqueda de amenazas

La integración con Kaspersky Endpoint Detection & Response ofrece funciones de respuesta ante incidentes automatizadas. Este enfoque integral de EDR aumenta la visibilidad en toda su infraestructura de IT corporativa, y permite a los equipos de SOC tomar decisiones informadas sobre la mejor estrategia para mitigar tanto el malware de baja prioridad como la mayoría de amenazas sofisticadas. La funcionalidad de EPP y EDR trabaja de forma conjunta a través de un solo agente.

Protección a varios niveles con tecnologías avanzadas

Protección multidimensional que se consigue mediante una combinación de tecnologías de prevención de amenazas basadas en algoritmos de aprendizaje automático. En nuestra plataforma de seguridad de endpoints están incorporados elementos como el control de endpoints y el refuerzo de sistemas avanzados, incluidos el control de aplicaciones y el marcado en lista blanca, la detección del comportamiento, la corrección automatizada, la prevención de exploits y la protección antiransomware. También se proporciona protección contra ataques de PowerShell y sin archivos.

Capacidad de gestión para empresas

Dispone de capacidad para gestionar cientos y miles de endpoints a través de una única consola unificada, proporcionando así un control detallado y una visibilidad global de toda su infraestructura, tanto en el entorno local como en la nube. Los escenarios empresariales incluyen implementación automatizada, comprobación del estado e informes automatizados, todo ello con la compatibilidad plena con entornos jerárquicos y de aislamiento físico air-gap.

Funciones

Protección contra amenazas esencial

Protección contra amenazas de archivos

Un componente obligatorio de la seguridad antimalware que implementa una gama completa de tecnologías de protección contra amenazas basadas en archivos. Incluye análisis del subsistema de Windows para Linux (WSL).

Protección contra amenazas de correo electrónico

El correo electrónico es uno de los puntos de exposición más explotados por los cibercriminales. La protección contra amenazas de correo electrónico analiza los mensajes de correo electrónico entrantes y salientes en busca de objetos peligrosos.

Protección contra amenazas web

Para garantizar la seguridad y protección al trabajar con los recursos de Internet, se protegen los datos entrantes y salientes, y las URL se contrastan con las listas de direcciones web maliciosas o de phishing. La protección contra amenazas web también analiza el tráfico HTTPS para la intercepción temprana de las últimas amenazas (agentes de botnet, instaladores, ransomware, etc).

Protección contra amenazas de red

Analiza el tráfico de red entrante para identificar actividades típicas de los ataques de red. La protección contra la falsificación de direcciones MAC protege aún más su infraestructura, ayudando a identificar y bloquear los ataques donde las direcciones se cambian para poner en riesgo los endpoints e interceptar el tráfico dirigido a otros dispositivos de red.

Firewall

Restringe la actividad de la red asociada con el nodo protegido. Las reglas predefinidas cubren filtrado de paquetes de red y flujos de datos, así como las interacciones de red basadas en software.

Prevención de ataques de BadUSB

Algunos virus modifican el firmware de dispositivos USB para que el sistema operativo detecte el dispositivo como un teclado. La prevención de ataques de BadUSB implementa un procedimiento de autorización de teclado para identificar los dispositivos USB infectados que emulan un teclado. La aplicación permite el uso de teclados autorizados y bloquea los no autorizados.

Proveedor de protección AMSI (interfaz de análisis antimalware)

Permite a Kaspersky Endpoint Security analizar objetos enviados por aplicaciones de validación antimalware de terceros. Los resultados se envían a la aplicación solicitante, que puede entonces bloquear o eliminar el objeto.

Protección contra amenazas avanzadas

Kaspersky Security Network (KSN)

Una compleja infraestructura de nube recopila y analiza los datos relacionados con la ciberseguridad de millones de participantes voluntarios de todo el mundo, detecta el malware y proporciona la reacción más rápida posible a las nuevas amenazas.

Detección del comportamiento

Proporciona defensas proactivas, utilizando técnicas que incluyen el aprendizaje automático para identificar y extraer patrones de comportamiento sospechosos, protegiendo así su sistema contra ransomware. El cifrado de archivos local malicioso y el cifrado remoto de carpetas compartidas a través de la red se pueden identificar, detener y mitigar.

Prevención de exploits

Está dirigido específicamente contra el malware que aprovecha las vulnerabilidades de software en aplicaciones populares, mediante el reconocimiento de patrones de comportamiento típicos o sospechosos, frenando la explotación de raíz y evitando la ejecución de cualquier código malicioso.

Prevención de intrusiones basada en host (HIPS)

Asigna cada aplicación a uno de cuatro grupos de confianza predeterminados en función de los datos de KSN. Las aplicaciones del grupo más fiable se incluyen en listas blancas y se ejecutan sin ningún tipo de limitación. El resto se ejecuta con privilegios limitados y acceso limitado a los recursos críticos del sistema.

Motor de corrección

Recopila datos sobre la actividad sospechosa, lo que permite a Kaspersky Endpoint Security deshacer las acciones que el malware ha realizado en el sistema operativo.

Kaspersky Lab
Enterprise Cybersecurity:
https://www.kaspersky.es/enterprise-security
Noticias de ciberamenazas: **www.securelist.es**
Noticias de seguridad de IT: **business.kaspersky.com/**
Descubra nuestro exclusivo enfoque en:
www.kaspersky.com/true-cybersecurity

#truecybersecurity
#HuMachine

www.kaspersky.es