

kaspersky



Kaspersky Optimum Security

Mantenga la delantera respecto de las amenazas evasivas, con EDR¹ o MDR² que no agotarán sus recursos.



Kaspersky
Optimum
Security

El 30 % de los ciberataques exitosos utilizan herramientas legítimas del sistema

Kaspersky Incident Response Analyst Report, 2020



El número de ciberataques no deja de aumentar

Las amenazas evasivas de hoy en día están diseñadas para eludir la protección tradicional de endpoints, lo que se traduce en riesgos nuevos e importantes para todas las empresas. Si una amenaza no detectada alcanza su infraestructura, podría enfrentarse a importantes pérdidas, lo que repercutiría en los resultados finales de la empresa:

- Interrupción de procesos críticos para las empresas y pérdida de datos.
- Importantes daños a la reputación y pérdida de clientes
- Multas, sanciones y pérdida de ingresos.

El 45 % de los ataques se detectaron debido a archivos sospechosos o actividad sospechosa en endpoints, lo que evidencia que detectarlos es prioritario

Como se indicó anteriormente



Protección óptima

Los métodos de prevención automática son la base de cualquier protección de terminales, pero deben complementarse con herramientas avanzadas si el objetivo es poder hacer frente a las amenazas evasivas más peligrosas.

Kaspersky Optimum Security ofrece funciones de detección avanzada basadas en **aprendizaje automático** y de respuesta rápida; todo ello desde la nube. Su equipo ahora puede, con rapidez y precisión, hacer frente incluso a las amenazas que antes le quitaban el sueño.

El desafío

El ransomware, el malware y el spyware financiero se perfeccionaron para eludir la detección y es sencillo y accesible adquirirlos desde la Dark Web, lo que crea un perfecto huracán para las empresas de hoy.



Es necesario fortalecer la protección de los terminales

Estos últimos ataques **eluden la detección** al ocultarse dentro de herramientas de sistemas legítimos y otros métodos y tecnologías ya disponibles, y emplearlos para **obtener acceso, subsistir y realizar acciones maliciosas en su infraestructura de forma rápida y sin que los detecte**.

Además, se suma el trabajo remoto lo que coloca a los endpoints (que ya solían ser el punto de entrada a su infraestructura más atractivo) aún más en la mira.

La solución

Kaspersky Optimum Security ofrece una solución eficaz de detección y respuesta frente a amenazas, respaldada por una supervisión ininterrumpida de seguridad, respuestas automatizadas y búsqueda de amenazas, junto con la asistencia y la orientación de los especialistas de Kaspersky.



Inversión óptima

No deberá contratar a más personas, volver a capacitar al personal, ni atascarse con una implementación complicada: Kaspersky Optimum Security simplifica y ayuda a automatizar los procesos fundamentales de respuesta ante incidentes, según sus requisitos específicos.

Las opciones locales y en la nube y un conjunto escalable de herramientas de seguridad inmediatas le permiten a controlar la complejidad del sistema de TI, aumentar la productividad de los usuarios y reflejar los costos de implementación con claridad.



Los recursos disponibles son escasos

Para ofrecer el perímetro adicional que necesita, su organización debe desarrollar las funcionalidades adecuadas respecto de la respuesta ante incidentes.

Pero un proyecto de esta índole es muy costoso:

- Los costes del software y hardware pueden ser elevados.
- Las herramientas y los procesos fragmentados y compartimentados hacen que la eficacia de la seguridad se vea deteriorada.
- Se puede perder mucho tiempo en tareas rutinarias.



Balance óptimo

Logre el equilibrio óptimo entre simplificación y eficacia, inteligencia humana y automatización, eficiencia y funcionalidad, ¡todo ello sin poner en riesgo su protección!

Kaspersky Optimum Security le ayuda a reducir los riesgos de perder beneficios, clientes y reputación, y fortalece sus defensas frente a amenazas nuevas, desconocidas y evasivas. De este modo, estará preparado para enfrentarse a la rápida evolución del panorama actual de las amenazas.

Principales ventajas

- **Proteja su empresa frente al el riesgo real de daños e interrupciones** de la última ola de amenazas evasivas letales.
- **Desarrolle su propia** capacidad de respuesta ante incidentes con un conjunto de herramientas de detección y respuesta de terminales (EDR, por sus siglas en inglés) fácil de utilizar.
- **Mejore su capacidad de detección de forma sencilla** gracias a una detección y administración administradas potente y sin complicaciones.
- Reduzca considerablemente los riesgos de infección al **formar a sus empleados y sensibilizarlos en materia de seguridad**.
- Ahorre valiosos recursos gracias a la automatización de las **operaciones y la protección gestionada**.
- Ahorre tiempo y esfuerzos gracias a una solución cuyas diversas funciones se gestionan **en una única consola en la nube o en las instalaciones**.

El 55% de los ataques tardaron semanas o más en detectarse

Como se indicó anteriormente



Detección avanzada

- **Algoritmos de análisis del comportamiento basados en el aprendizaje automático** para detectar con rapidez y precisión los comportamientos sospechosos
- **Búsqueda automatizada de amenazas** basada en indicadores de ataque (IoA) patentados para encontrar amenazas complejas que están ocultas, con el respaldo de los especialistas de Kaspersky.
- Control adaptativo de anomalías para **ajustar de forma automática la configuración de las herramientas de reducción de la superficie de ataque** a los perfiles de los usuarios
- Detección en la nube, que incluye un **entorno de pruebas integrado en la nube**.

Principales funciones

Kaspersky Optimum Security ofrece una amplia gama de funciones esenciales para la protección frente a las amenazas evasivas, en cuyo núcleo se encuentran la capacidad de detección, análisis y respuesta.



Análisis sencillo

- Toda la información relacionada con un incidente se recopila automáticamente en **una única tarjeta de incidente**.
- **La visualización y el simple proceso** de investigación le permiten analizar de forma rápida y eficaz el incidente en un único entorno para decidir el curso de acción que debe seguirse.
- Al mismo tiempo, Kaspersky **prioriza e investiga todas las detecciones de indicadores de ataque para ofrecerle recomendaciones personalizadas**.



Respuesta automatizada

- **La función de respuesta** con un solo clic permite contener rápidamente un determinado incidente.
- **La respuesta asistida** basada en la experiencia de nuestros especialistas le permite hacer frente incluso a las amenazas más complejas y peligrosas.
- **La respuesta automatizada entre terminales** le permite encontrar las amenazas analizadas o importadas en toda la red y responder con eficacia.

Contenido

Elija cómo utilizar Kaspersky Optimum Security: como solución gestionada para lograr una protección ininterrumpida, como conjunto de herramientas EDR fáciles de usar o como mezcla de ambas, con el fin de aprovechar la experiencia y los conocimientos de los especialistas de Kaspersky a la vez que desarrolla sus propias capacidades de detección y respuesta. Kaspersky Optimum Security reúne varios productos en una única solución:



Kaspersky
Optimum Security



Optimum
Kaspersky
Endpoint Detection
and Response

Mejor visibilidad de las amenazas
Análisis de la causa raíz

Optimum
Respuesta
automatizada



Kaspersky
Security Awareness

Programas de formación en línea para mejorar las habilidades de los empleados en materia de ciberseguridad



Optimum
Kaspersky
Managed Detection
and Response

Control ininterrumpido de la seguridad
Detección automática de amenazas

Optimum
Escenarios de respuesta
guiada y remota



Equipo de
Threat Intelligence
Portal

Datos enriquecidos para la investigación

El 31 % de los ciberataques con éxito e se produjeron por medio de correos electrónicos maliciosos, lo que implica que muchos de ellos podrían haberse evitado con la ayuda de los propios empleados

Como se indicó anteriormente



Forme a los usuarios

La clave para reducir su superficie de ataque y la cantidad de incidentes es formar a sus empleados para que sean conscientes de las ciberamenazas que pueden desatar en su infraestructura por negligencia o por simple desconocimiento. **Kaspersky Security Awareness** proporciona los conocimientos y las habilidades que todos los empleados necesitan para ayudarles a proteger su infraestructura, logrando que trabajen activamente con usted para mantener un entorno ciberseguro.



Hashes

Manténgase al corriente con la información más reciente

Ayude a sus especialistas en ciberseguridad a analizar y comprender las amenazas de forma más exhaustiva y rápida con la información más reciente sobre archivos, hashes, IP y URL asociadas a las amenazas. Obtenga esta información complementaria sin coste adicional en el portal **Kaspersky Threat Intelligence Portal**, muy fácil de utilizar.



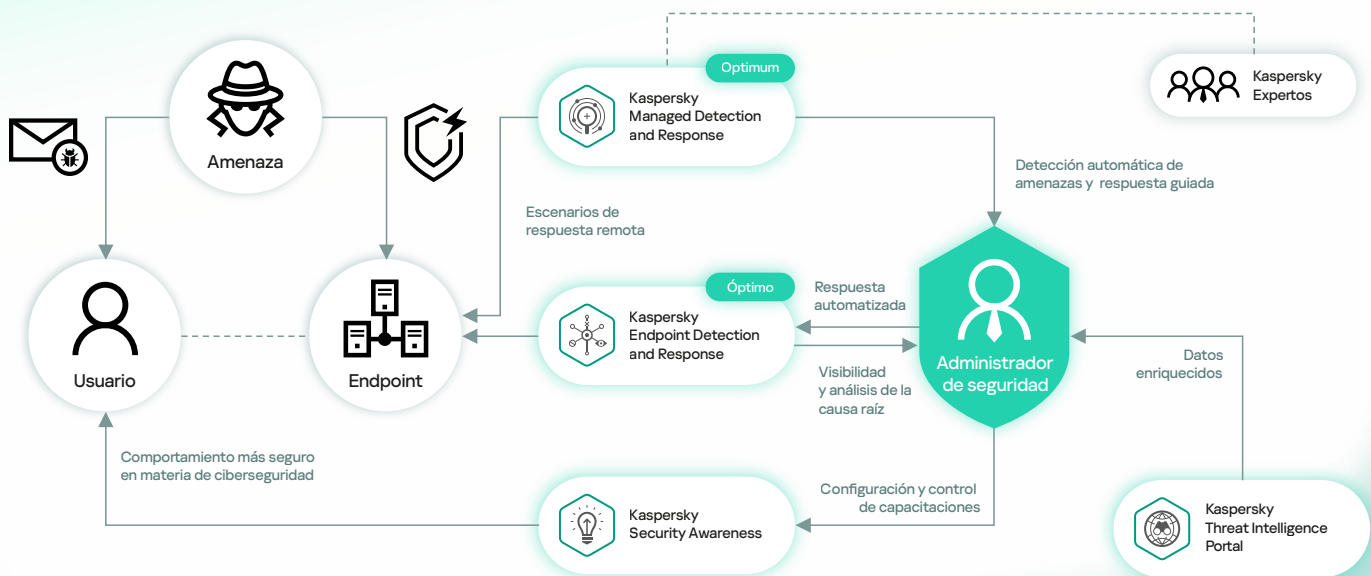
Permítanos brindarle ayuda

Para garantizar una protección eficaz de su infraestructura de IT, diseñe, implemente y configure sus productos según prácticas recomendadas y requisitos de seguridad específicos.

Aumente el retorno de la inversión a partir de la solución de seguridad y garantice un rendimiento al 100 % de las funcionalidades al permitirles a especialistas en **Kaspersky Professional Services** revisar el estado de la solución, implementarla, realizar su mantenimiento y optimizarla.

Cómo funciona todo junto

En Kaspersky Optimum Security, se unen la prevención, la detección, el análisis, la respuesta y la capacitación de empleados. Cada componente aporta su valor y puede usarse de forma independiente, pero todos funcionan en conjunto para cubrir las necesidades de protección de todos los endpoints evasivos mediante una única solución integrada.



El 44 % de las organizaciones percibe que proteger entornos cada vez más complejos es uno de sus principales problemas

IT Security Economics 2021 de Kaspersky



Solución completa

- Parte del ecosistema de seguridad de Kaspersky es reforzar sus defensas desde Security Foundations hasta las funciones avanzadas optimizadas.
- Las diversas funciones de Kaspersky Optimum Security se pueden gestionar a través de una única consola en la nube.
- Múltiples capas de protección le hacen frente tanto a amenazas evasivas y de bienes como al riesgo por errores humanos.



Facilidad de gestión

- Nuestra consola de gestión en la nube le permite controlar de forma rápida y eficaz desde cualquier parte del mundo.
- Las opciones SaaS y en las instalaciones de la empresa ofrecen la misma experiencia de gestión.
- La implantación es rápida y sin complicaciones, tanto si ya utiliza las soluciones de Kaspersky como si no lo hace.
- Su equipo puede controlar y administrar todas las herramientas de forma fácil e intuitiva, sin que sea necesario un largo proceso de familiarización o capacitación.



Ahorre tiempo y recursos

- La protección administrada le permite desarrollar funcionalidades de detección y respuesta sin tener que invertir en seguridad, incluso si no cuenta con personal dedicado a la ciberseguridad o los conocimientos.
- Los procesos fundamentales están automatizados, lo que hace que la respuesta ante incidentes sea rápida, precisa y eficiente.
- Una mayor concienciación de los empleados en materia de seguridad supone que menos amenazas vulneren sus defensas, lo que tendrá como resultado un menor número de incidentes que resolver.

En la práctica

Cómo funciona todo

Prueba de

El usuario recibe un correo electrónico de phishing o accede a un recurso web malicioso, que infecta su host.

Concienciación en materia de seguridad para empleados

Reducción de la superficie de ataque

Prevención automática de amenazas

Instalación

La infección inicial despliega los componentes necesarios, se comunica con el servidor de mando y control¹ y explora su entorno.

Mecanismos de detección avanzados, como el análisis de comportamiento basado en el aprendizaje automático y sandbox

Detección automatizada de amenazas con IoA²

Escenarios de respuesta guiada y remota

Liberación de dispositivos

Se utiliza una gama de herramientas para ganar persistencia e iniciar el movimiento horizontal si es necesario

Análisis de causa raíz y exploración del IoC³

¹ Comando y control

² Indicadores de ataque

³ Indicador de compromiso

Enfoque de ciberseguridad por etapas de Kaspersky

Juntos podemos desarrollar sus defensas a partir de una protección fiable con Kaspersky Security Foundations, alcanzando progresivamente una respuesta esencial ante incidentes con Kaspersky Optimum Security y, finalmente, llegando a la aplicación de potentes herramientas destinadas a la protección frente a las amenazas más avanzadas con Kaspersky Expert Security. Seleccione la etapa más adecuada para sus necesidades:



Kaspersky Security Foundations

Bloquee automáticamente gran parte de las amenazas

» [Más información](#)



Kaspersky Optimum Security

Mejora de las defensas frente las amenazas evasivas,

» [Más información](#)



Kaspersky Expert Security

Preparación frente a ataques complejos y similares a APT.

» [Más información](#)

Quiénes somos

Somos una empresa de ciberseguridad privada internacional con miles de clientes y socios en todo el mundo y nos comprometemos a ser transparentes e independientes. Desarrollamos herramientas y brindamos servicios desde hace 25 años para mantener su seguridad con nuestras **tecnologías más probadas y más premiadas**.

IDC

Evaluación de proveedores de IDC MarketScape sobre seguridad de endpoints moderna y global para empresas y pymes en 2021

Competidor principal



AV-Test

Protección avanzada de endpoints: Prueba de protección de ransomware

Protección 100%



Radicati Group

Cuadrante de mercado sobre amenazas persistentes avanzadas (APT)

Mejor competidor



Eche un vistazo más de cerca

Para obtener más información sobre cómo Kaspersky EDR Optimum aborda las ciberamenazas al mismo tiempo que facilita el uso de su equipo de seguridad y sus recursos, visite www.kaspersky.com/enterprise-security/edr-security-software-solution

¹ Endpoint Detection and Response
² Managed Detection and Response

Noticias sobre amenazas cibernéticas: securelist.com
Noticias de seguridad de TI: business.kaspersky.com
Seguridad de TI para PYMES: kaspersky.com/business
Seguridad de TI para grandes empresas: kaspersky.com/enterprise

kaspersky.es