kaspersky PREPARADOS PARA EL FUTURO

Kaspersky Optimum Security

Consiga un nivel óptimo de ciberseguridad con protección gestionada y detección y respuesta de terminales en la nube

El desafío

Debe poder defender su empresa de forma eficaz frente a amenazas nuevas, desconocidas y evasivas, sin agotar su tiempo y recursos limitados.

El 30 % de los ciberataques con éxito utilizan herramientas legítimas del sistema[1]

El número de ciberataques no deja de aumentar

Las actuales amenazas evasivas (diseñadas para eludir la protección tradicional de los terminales) conllevan riesgos mucho más importantes para las empresas, debido a que cada vez es más difícil detectar, analizar y responder a los ataques. 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 empresariales críticos
- Importantes daños a la reputación y pérdida de clientes
- Multas, sanciones y pérdida de ingresos.

Es necesario fortalecer la protección de los terminales

Los actuales ataques evasivos se han vuelto mucho más eficaces, debido a que los delincuentes utilizan herramientas legítimas del sistema y otros métodos y tecnologías ya preparados. Esto les permite obtener acceso, persistir y realizar acciones maliciosas dentro de su infraestructura con mayor rapidez y sin ser detectados.

Esta situación se agrava debido a la disolución del perímetro y el crecimiento del teletrabajo, lo que sitúa a los terminales (tradicionalmente la entrada más atractiva a su infraestructura) aún más en el punto de mira.

Los recursos disponibles son escasos

Para lograr la seguridad adicional que requieren los terminales en la actualidad, es necesario desarrollar dentro de su organización las capacidades adecuadas de respuesta ante incidentes.

No obstante, los costes asociados a un proyecto de este tipo pueden descontrolarse rápidamente:

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

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.

El 45 % de los ataques se detectaron debido a archivos o actividad sospechosos en los terminales[1]

Protección avanzada frente a amenazas

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.

Solución llave en mano, rápida y escalable

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 y de respuesta rápida; todo ello desde la nube. Permite a sus ingenieros de ciberseguridad hacer frente, con rapidez y precisión, incluso a las amenazas que antes les quitaban el sueño.

Niveles óptimos de inversión

No necesita contratar a más personal, ni volver a formarles, ni se volverá a atascar con una implementación complicada: Kaspersky Optimum Security simplifica y ayuda a automatizar los procesos fundamentales de respuesta ante incidentes, en base a sus requisitos específicos.

Se adapta a sus necesidades con opciones locales en las instalaciones y en la nube, y con un conjunto de herramientas de seguridad escalables y listas para utilizar que le ayudan a reducir la complejidad de su sistema de TI, a aumentar productividad del usuario y a controlar los costes de implementación.

Principales ventajas

- Anticípese y 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.
- 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 funcionalidad 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.

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.

El 55 % de los ataques tardaron varias semanas o más tiempo en detectarse[1]

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 patentados para detectar amenazas complejas ocultas, con la asistencia 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

Investigación simplificada

- Toda la información relacionada con un incidente se recopila automáticamente en una única tarjeta de incidentes.
- La visualización, junto con un sencillo proceso de investigación, le permiten analizar de forma rápida y eficaz el incidente en un único entorno y 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 los especialistas de Kaspersky 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.

Cómo se utiliza

Kaspersky Optimum Security incluye una serie de herramientas y capacidades principales que, en conjunto, pueden utilizarse eficazmente para evitar y detectar las amenazas, y responder a las mismas, en las distintas fases de un ataque:

Penetración

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

Instalación

La infección inicial despliega los componentes necesarios, se comunica con el servidor de mando y control[1] y explora su entorno.

Liberación de dispositivos

Si es necesario, utiliza una amplia gama de herramientas (incluidas las legítimas y las nativas del sistema) para ganar persistencia e iniciar el movimiento horizontal.

Concienciación en materia de seguridad para empleados

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

Reducción de la superficie de ataque

Detección automatizada de amenazas con IoA[2]

Análisis de causa raíz y exploración del IoC[3]

Prevención automática de amenazas

Escenarios de respuesta guiada y remota

[1] Comando y control
[2] Indicadores de ataque
[3] Indicador de compromiso

Protección adicional

Puede mejorar aún todavía sus defensas con una variedad de herramientas destinadas a diferentes aspectos de su seguridad: detección, investigación y concienciación.

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.[1]

Capa de detección adicional

Descubra las amenazas nuevas y desconocidas de forma más rápida y fiable con **Kaspersky Sandbox**, que las analiza automáticamente en un entorno aislado, mediante algoritmos de detección y técnicas antievasión patentados. Las respuestas configuradas se aplican automáticamente a las amenazas descubiertas, lo que aumenta bastante sus capacidades de detección sin requerir ninguna gestión adicional a la implementación inicial.

Una ventaja adicional para las investigaciones

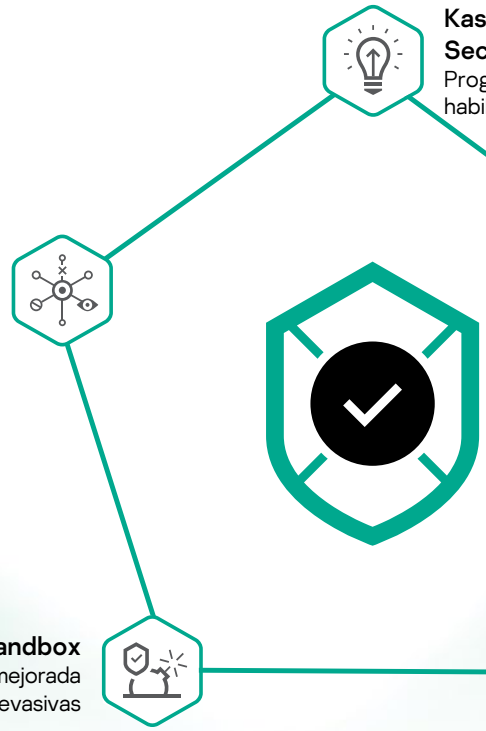
Ayude a sus especialistas en ciberseguridad a analizar y comprender las amenazas de forma más exhaustiva y rápida con la información más reciente sobre archivos, hashes, IP y URL asociadas a las amenazas. Obtenga esta información complementaria sin coste adicional en el portal **Kaspersky Threat Intelligence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

El personal es la clave de su seguridad

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 seguro a nivel cibernético.

Funcionamiento

Puede elegir 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. Kasperky Optimum Security reúne varios productos en una única solución:



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

Kaspersky Endpoint Detection and Response Optimum
Mejor visibilidad de las amenazas
Análisis de causa raíz
Respuesta automatizada

Kaspersky Managed Detection and Response Optimum
Control ininterrumpido de la seguridad
Detección automática de amenazas
Escenarios de respuesta guiada y remota

Kaspersky Sandbox
Detección automática mejorada de amenazas evasivas

Kaspersky Threat Intelligence Portal
Datos enriquecidos para la investigación

En la práctica

Descubrirá que Kaspersky Optimum Security es muy fácil de administrar desde una única consola, lo que le permite aprovechar al máximo su escaso tiempo y recursos.

El 56 % de los encuestados afirma que sus organizaciones están en riesgo debido a la escasez de personal de ciberseguridad[2]

Solución completa

- Parte del ecosistema de seguridad de Kaspersky consiste en reforzar sus defensas, desde los cimientos de la seguridad hasta las funciones avanzadas optimizadas.
- Las diversas funciones de Kaspersky Optimum Security se pueden gestionar a través de una única consola en la nube.
- Una solución con varias capas de protección, que trata las amenazas de productos básicos y las evasivas, así como las posibilidades de errores humanos.

Facilidad de gestión

- La consola de gestión en la nube permite un control rápido y eficaz desde cualquier parte del mundo.
- Las opciones basadas en la nube 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.
- Todas las herramientas se pueden gestionar y controlar de forma fácil e intuitiva, sin que sea necesario un largo proceso de familiarización o formación.

Ahorre tiempo y recursos

- La protección gestionada ayuda a las organizaciones que carecen de personal de seguridad de TI o de conocimientos técnicos a crear capacidades de detección y respuesta sin necesidad de realizar inversiones en seguridad asociadas.
- Los procesos fundamentales de ciberseguridad están automatizados, lo que hace que la respuesta ante incidentes sea más 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.

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

- Prevención automatizada multivectorial de los incidentes que provocan las amenazas de productos básicos, que suponen la gran mayoría de los ciberataques.
- Esta es la etapa básica para empresas de cualquier tamaño y complejidad en el desarrollo de una estrategia de defensa integrada
- Protección fiable de los terminales para quienes tienen equipos de TI pequeños y conocimientos de seguridad incipientes

Kaspersky Optimum Security

Mejora de las defensas frente las amenazas evasivas para los siguientes grupos:

- Empresas que tienen un pequeño equipo de seguridad de TI con conocimientos técnicos básicos de ciberseguridad.
- Empresas que tienen un entorno de TI que crece en tamaño y complejidad, lo que aumenta la superficie de ataque.
- Empresas que no tienen recursos de ciberseguridad y necesitan una mayor protección.
- El desarrollo de la capacidad de respuesta ante incidentes es cada vez más importante.

Kaspersky Expert Security

Preparación para ataques complejos y de tipo APT en los siguientes casos:

- Entornos de TI complejos y distribuidos.
- Equipo de seguridad de TI desarrollado o con un Centro de operaciones de seguridad (SOC).
- Baja tolerancia al riesgo debido a los elevados costes de los incidentes de seguridad y las filtraciones de datos.
- Gran importancia del cumplimiento de la normativa.

Para obtener más información sobre cómo Kaspersky Optimum Security aborda las ciberamenazas al tiempo que facilita el trabajo de su equipo de seguridad y sus recursos, visite: http://go.kaspersky.es/optimum.

1 Kaspersky Incident Response Analyst Report 2019, Kaspersky, 2020
2 (ISC)2 Cybersecurity workforce study, (ISC)2, 2020

Noticias sobre ciberamenazas: www.securelist.es
Noticias sobre seguridad de TI: business.kaspersky.es

www.kaspersky.es