kaspersky BRING ON THE FUTURE

Kaspersky Optimum Security

Consiga un nivel óptimo de ciberseguridad con protección administrada y detección y respuesta de endpoints en la nube

El desafío

Debe poder defender su empresa de forma eficaz contra amenazas nuevas, desconocidas y evasivas, sin agotar su escaso tiempo y recursos.

Aumento de los ataques avanzados

Las amenazas evasivas de hoy en día (diseñadas para eludir la protección tradicional de los endpoints) conllevan riesgos mucho más importantes para las empresas que antes, ahora que los ataques son cada vez más difíciles de detectar, analizar y responder. Si una amenaza no detectada arraiga en su infraestructura, podría enfrentarse a importantes pérdidas, lo que repercutiría en los resultados de la empresa:

- Interrupción de los procesos fundamentales de la empresa.
- Daños considerables a la reputación y pérdida de clientes.
- Multas, sanciones y pérdida de utilidades.

Hay que fortalecer la protección de los endpoints

Los ataques evasivos de hoy en día 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 por la disolución del perímetro y el crecimiento del trabajo remoto, lo que pone a los endpoints (tradicionalmente la entrada más atractiva a su infraestructura) aún más en el punto de mira.

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

Escasez de recursos

Para proporcionar la ventaja adicional que la seguridad de los endpoints requiere ahora, es necesario desarrollar dentro de su organización las capacidades adecuadas de respuesta ante incidentes.

Sin embargo, los costos asociados a un proyecto de este tipo pueden desbordarse rápidamente:

- Los costos de 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 acabar perdiendo mucho tiempo en tareas rutinarias.

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

La solución

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

Protección avanzada contra amenazas

Alcance el equilibrio óptimo entre simplificación y eficacia, inteligencia humana y automatización, eficiencia y funcionalidad, ¡sin arriesgar su protección!

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

Solución rápida, escalable y lista para usarse

Los métodos de prevención automática son la base de cualquier protección de endpoints, pero deben complementarse con herramientas avanzadas si se quiere 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. Sus técnicos de ciberseguridad ahora pueden, con rapidez y precisión, hacer frente incluso a las amenazas que antes les quitaban el sueño.

Niveles óptimos de inversión

No es necesario que contrate a más personas, ni que vuelva a capacitar al personal, ni que se atasque con una implementación complicada: Kaspersky Optimum Security simplifica y ayuda a automatizar los procesos fundamentales de respuesta ante incidentes, según sus requisitos específicos.

Se adapta a sus necesidades con opciones en las instalaciones y en la nube, y con un conjunto de herramientas de seguridad escalables y listas para usar que le ayudan a mantener la complejidad del sistema de TI baja, la productividad del usuario alta y los costos de implementación transparentes.

Ventajas clave

- Anticípese y defienda su empresa contra 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 endpoints (EDR) de fácil uso.
- Ahorre valiosos recursos mediante la automatización de las operaciones y la administración de las funciones.
- Ahorre tiempo y trabajo gracias a una solución cuyas diversas funciones se administran en una única consola en la nube o en las instalaciones.

Capacidades principales

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

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

Detección avanzada

- Algoritmos de análisis del comportamiento basados en el aprendizaje automático para exponer con rapidez y precisión los comportamientos sospechosos
- Búsqueda automatizada de amenazas basada en indicadores de ataque patentados para encontrar amenazas complejas que están ocultas, con el respaldo de los especialistas de Kaspersky
- Control adaptativo de anomalías para ajustar automáticamente 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 incidente.
- La visualización y el simple 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 brindarle recomendaciones personalizadas

Respuesta automatizada

- La respuesta con un solo clic permite contener rápidamente un incidente individual.
- La respuesta asistida a partir de la experiencia de los especialistas de Kaspersky le permite enfrentarse incluso a las amenazas más complejas y peligrosas
- La respuesta automatizada entre endpoints le permite encontrar las amenazas analizadas o importadas en toda la red y responder a ellas.

Cómo se aplica

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 estas, 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 C&C[1] y explora su entorno

Rooting

Se utiliza una gama de herramientas (como las legítimas y las nativas del sistema) para ganar persistencia e iniciar el movimiento horizontal si es necesario

Concienciación de los empleados en materia de seguridad

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

Reducción de la superficie de ataque

Búsqueda automatizada de amenazas con IoA[2]

Análisis de causa raíz y exploración del IoC[3]

Prevención automática de amenazas

Casos de respuesta guiada y remota

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

Conociendo el MDR

Kaspersky Managed Detection and Response (MDR) ofrece protección avanzada y continua contra el creciente volumen de amenazas diseñadas para eludir las barreras de seguridad automatizadas, y brinda alivio a las organizaciones que tienen problemas para encontrar personal especializado o recursos internos limitados.

Sus capacidades superiores de detección y respuesta están respaldadas por uno de los equipos de búsqueda de amenazas más exitosos y experimentados del sector. A diferencia de ofertas similares en el mercado, Kaspersky MDR aprovecha los modelos de aprendizaje automático patentados, la exclusiva inteligencia de amenazas y un historial probado de investigación de ataques selectivos. Fortalece automáticamente su resiliencia corporativa frente a las ciberamenazas, al mismo tiempo que optimiza sus recursos existentes y futuras inversiones en seguridad de TI.

Conociendo la solucion

El nuevo Kasperky Optimum Security une varios productos en una única solución: Kaspersky Endpoint Security for Business Advanced + Kaspersky Endpoint Detection and Response Optimum + Kaspersky Managed Detection and Response.

Prevención automática avanzada
Gestión de parches
Componentes de Control (Web/Dipositivos/Aplicaciones)

Visibilidad de amenazas mejorada
Análisis de raíz de la causa
respuesta automatizada

Monitoreo de seguridad 24/7
Búsqueda de amenazas automatizada
Escenarios de repuesta guiada y remota

Mayor protección

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

El 31 % de los ciberataques que tuvieron éxito 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]

Una capa más de detección

Exponga las amenazas nuevas y desconocidas de forma aún más rápida y fiable con **Kaspersky Sandbox**, que analiza las amenazas automáticamente en un entorno aislado, utilizando 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 administración más allá de la implementación inicial.

Una ventaja más 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 costo adicional desde **Kaspersky Threat Intelligence Portal**, de fácil uso.

El personal es la clave de su seguridad

La clave para reducir su superficie de ataque y la cantidad de incidentes es capacitar 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 ayudar a proteger su infraestructura, de modo que trabajen activamente con usted para mantener un entorno seguro a nivel cibernético.

En funcionamiento

Descubrirá que Kaspersky Optimum Security es 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]

Paquete completo

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

Facilidad de administración

- La consola de gestión en la nube permite un control rápido y eficaz desde cualquier parte del mundo.
- Las opciones basadas en las nubes y en las instalaciones de la empresa ofrecen la misma experiencia de administración.
- La implementación es rápida y sin complicaciones, tanto si ya utiliza las soluciones de Kaspersky como si no lo hace.
- Todas las herramientas pueden controlarse y administrarse de forma fácil e intuitiva, sin que sea necesario un largo proceso de familiarización o capacitación.

Ahorro de tiempo y recursos

- La protección administrada ayuda a las organizaciones que carecen de personal de seguridad de TI o de conocimientos técnicos a crear capacidades de detección y respuesta sin las 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 hará que menos amenazas penetren en sus defensas, lo que generará menos incidentes que tenga que procesar.

Enfoque por etapas de Kaspersky

Juntos podemos desarrollar sus defensas a partir de una protección fiable con Kaspersky Security Foundations, pasar a una respuesta esencial ante incidentes con Kaspersky Optimum Security y, finalmente, llegar a la aplicación de potentes herramientas destinadas a la protección contra las amenazas más avanzadas con Kaspersky Expert Security.

Escoja la etapa que más le convenga:

Kaspersky Security Foundations

Bloquee automáticamente la gran mayoría de las amenazas

- Prevención automatizada multivectorial de los incidentes que provocan las amenazas básicas, que son la gran mayoría de los ciberataques.
- La etapa inicial para organizaciones de cualquier tamaño y complejidad en el desarrollo de una estrategia de defensa integrada
- Protección fiable de los endpoints para quienes tienen equipos de TI pequeños y conocimientos de seguridad limitados

Kaspersky Optimum Security

Aumente sus defensas contra las amenazas evasivas para los siguientes grupos:

- Los grupos que tienen un pequeño equipo de seguridad de TI con conocimientos técnicos básicos de ciberseguridad.
- Los grupos que tienen un entorno de TI que crece en tamaño y complejidad, lo que aumenta la superficie de ataque.
- Los grupos 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:

- Los entornos de TI son complejos y están distribuidos.
- El equipo de seguridad de TI está desarrollado o se ha establecido un Centro de operaciones de seguridad (SOC).
- El apetito de riesgo es bajo debido a los altos costos de los incidentes de seguridad y las filtraciones de datos.
- El cumplimiento de la normativa es una preocupación.

1 Informe de los analistas de Kaspersky Incident Response 2019, Kaspersky, 2020
2 (ISC)2 Estudio de la fuerza de trabajo de la ciberseguridad, (ISC)2, 2020

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

latam.kaspersky.com

2021 AO Kaspersky Lab.
Las marcas comerciales y de servicios registradas pertenecen a sus respectivos propietarios.