kaspersky

Kaspersky Security for Enterprise

Acerca del portfolio de Kaspersky Enterprise

El primer paso es crear una base de seguridad para su organización eligiendo el producto o servicio adecuado. Sin embargo, desarrollar una estrategia de ciberseguridad corporativa con visión de futuro es la clave para el éxito a largo plazo.

El portfolio empresarial de Kaspersky refleja las exigencias de seguridad de las empresas actuales y responde a las necesidades de organizaciones con diferentes niveles de madurez con un enfoque paso a paso. Este enfoque combina diferentes niveles de protección contra todo tipo de ciberamenazas para detectar los ataques más complejos, responder de forma rápida y adecuada a cualquier incidente y evitar amenazas futuras.

La función de la seguridad de endpoints en la planificación a largo plazo

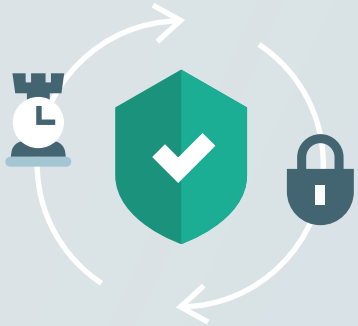
Proceso tradicional de evolución de la seguridad

Toma de decisiones:

- Tendencias del mercado
- Solución de seguridad compartimentada
- Enfoque basado en "apagar fuegos"
- Impulsado por el cumplimiento de normativas

Aprovechamiento de productos tradicionales:

- EPP
- Firewalls/NGFW
- Firewall para aplicaciones web
- Prevención de pérdidas de datos
- SIEM

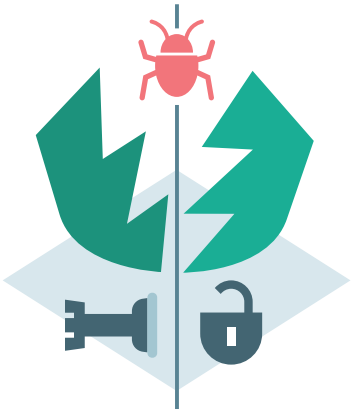


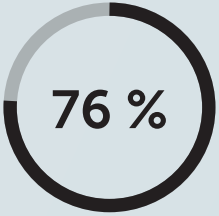
Atributos

- Planificación de seguridad a corto plazo
- Dependencia de tecnologías y funciones
- Defensa de la red basada en el perímetro

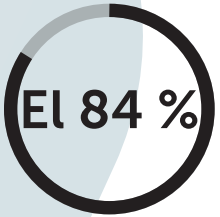
Por qué fallan los enfoques tradicionales

- Creciente complejidad de las amenazas y del panorama de amenazas
- Complejidad de las tecnologías de ciberseguridad
- Requisitos empresariales para una estrategia de ciberseguridad a largo plazo





de todas las alertas son generadas por endpoints



de todas las brechas de seguridad de endpoints implican más de un endpoint

Los endpoints son los puntos de entrada más comunes a la infraestructura de una organización, el objetivo principal de los cibercriminales y las fuentes clave de los datos necesarios para una investigación eficaz sobre incidentes complejos.

3 pasos hacia la planificación de ciberseguridad avanzada para empresas

2

Amenazas avanzadas y ataques dirigidos

Defensa avanzada

Céntrese en la detección avanzada y en una respuesta rápida a las amenazas complejas que no detecta la protección preventiva.

Endpoints

Kaspersky Endpoint Detection and Response

Servicios

Servicio de Kaspersky Targeted Attack Discovery

1

Panorama de amenazas más amplio

Fundamentos de seguridad

Refuerce los sistemas y bloquee automáticamente el número máximo de amenazas posible.

Endpoints

Kaspersky Endpoint Security for Business

Kaspersky Embedded Systems Security

Red

Kaspersky Secure for Mail Server

Kaspersky Security for Internet Gateway

3

Campañas dirigidas y Ciberarmas

Enfoque de ciberseguridad integrada

Preparación para ataques de nivel de APT. Alto nivel de experiencia, capacidades avanzadas de inteligencia frente a amenazas y búsqueda continua de amenazas.

Kaspersky Threat Management & Defense

Red

Kaspersky Anti Targeted Attack

Inteligencia

Kaspersky Threat Intelligence

Personas

Formación Kaspersky Cybersecurity

Privacidad

Kaspersky Private Security Network

Nube

Kaspersky Hybrid Cloud Security

Asistencia

Asistencia premium y servicios profesionales Kaspersky

Datos

Kaspersky Security for Storage

Personas

Kaspersky Security Awareness

4 beneficios para su empresa de este enfoque

Forma la base para el desarrollo de una estrategia de ciberseguridad a largo plazo, teniendo en cuenta los aspectos específicos de la empresa y las tendencias en el panorama de amenazas.

Optimización de la inversión en tecnología de seguridad y reducción del coste total de propiedad.

Reducción de los daños operativos y económicos causados por el cibercrimen.

Aumento del retorno de la inversión gracias a la perfecta automatización del flujo de trabajo sin interrumpir los procesos empresariales.

1 Fundamentos de seguridad

Tecnologías preventivas automatizadas y concienciación sobre seguridad

Bloqueo del máximo número posible de amenazas

Perfecto para pequeñas empresas que no disponen de un equipo de seguridad específico o tienen una experiencia en ciberseguridad muy limitada

- Prevención automatizada de varios vectores de un gran número de posibles incidentes causados por amenazas genéricas
- El paso fundamental para grandes o medianas empresas a la hora de desarrollar una estrategia de defensa integrada contra amenazas complejas

Endpoints

- **Kaspersky Endpoint Security for Business**
- **Kaspersky Embedded Systems Security**

Nube

- **Kaspersky Hybrid Cloud Security**

Red

- **Kaspersky Secure Mail Gateway**
- **Kaspersky Security for Internet Gateway**

Personas

- **Kaspersky Security Awareness**

Datos

- **Kaspersky Security for Storage**

Asistencia

- **Asistencia premium Kaspersky**
- **Kaspersky Professional Services**

Kaspersky Endpoint Security for Business

La mayoría de los ciberataques contra las empresas comienzan en un endpoint. Unas capacidades limitadas de prevención y automatización provocan que los especialistas se sobrecarguen con incidentes de seguridad. Todos los endpoints pueden convertirse en la causa de las interrupciones en la actividad. Kaspersky Endpoint Security for Business evita las amenazas y refuerza los endpoints al combinar la seguridad adaptativa con herramientas de control adicionales. Las amenazas se bloquean antes de que puedan dañar los datos o perjudicar a la productividad de los usuarios, incluso cuando el endpoint no se encuentra dentro del perímetro corporativo.

Perfecto para

Organizaciones cuyas expectativas de IT están creciendo y diversificándose

Organizaciones que desean reducir las oportunidades y la frecuencia de los errores de usuario que provocan brechas de seguridad

Beneficios para su empresa

Evita interrupciones en las actividades de la empresa y errores humanos

Facilita la transformación digital y protege la fuerza de trabajo móvil

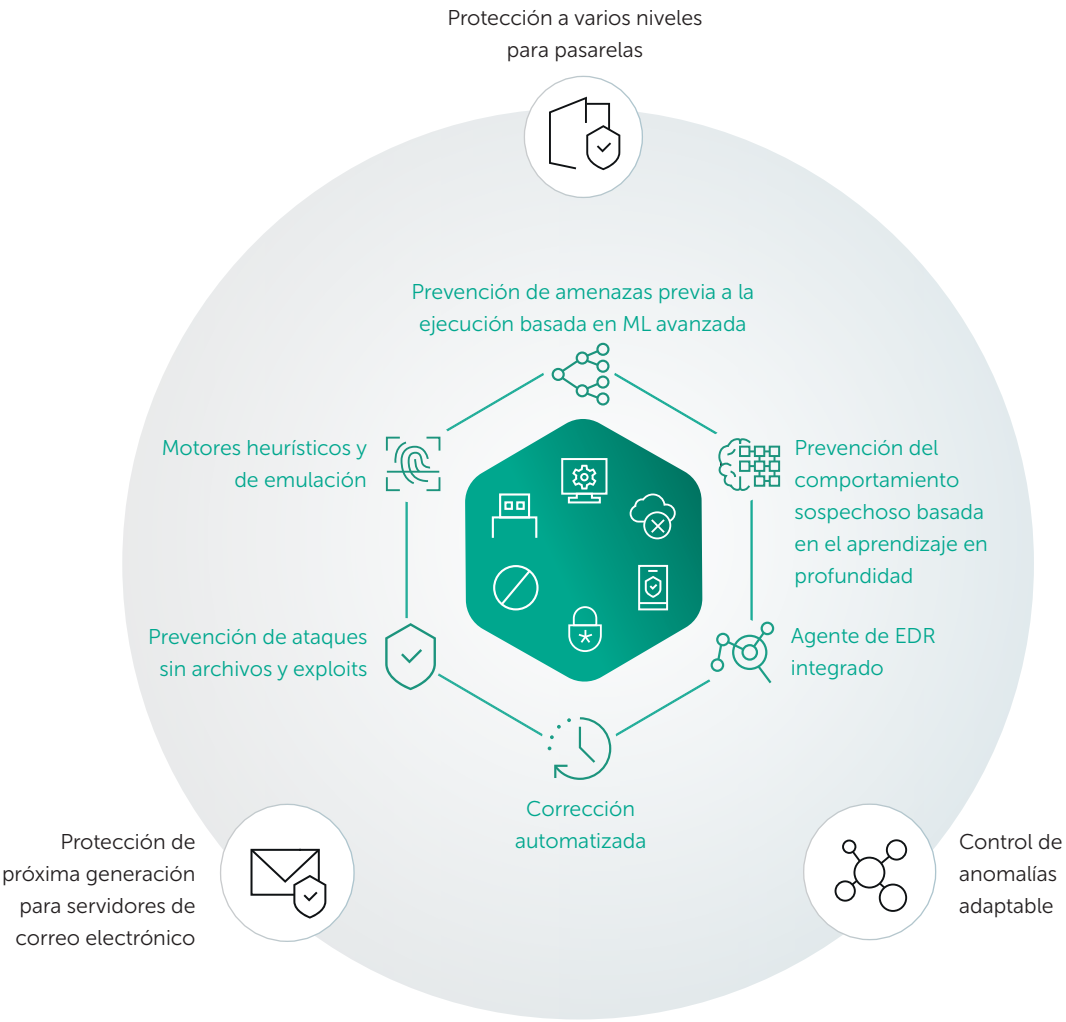
Mejora la preparación para las auditorías: busca y corrige vulnerabilidades, "alteraciones en la configuración" y dispositivos sin cifrar

Maximiza el retorno de la inversión reduciendo la superficie de ataque y el número de incidentes que gestionar

Permite el control de todos los endpoints gracias a una consola integrada y un agente unificado

Casos de uso

- Reduce la exposición a los ataques mediante la aplicación de un refuerzo adaptativo, protegiendo endpoints, servidores de correo electrónico y archivos, y pasarelas de Internet
- Garantiza el cumplimiento de los requisitos normativos en los endpoints
- Automatiza las tareas de detección, respuesta e implementación de software, lo que da más tiempo para otros asuntos a los especialistas en seguridad
- Optimiza la integración y la adopción de otras tecnologías de seguridad


Protección a varios niveles para pasarelas
Prevención de amenazas previa a la ejecución basada en ML avanzada
Motores heurísticos y de emulación
Prevención del comportamiento sospechoso basada en el aprendizaje en profundidad
Prevención de ataques sin archivos y exploits
Agente de EDR integrado
Corrección automatizada
Protección de próxima generación para servidores de correo electrónico
Control de anomalías adaptable

Kaspersky Hybrid Cloud Security

Hybrid Cloud Security es una solución que simplifica y protege la transformación digital cuando las organizaciones virtualizan o trasladan cargas de trabajo a la nube.
La tecnología de agente ligero patentada permite la centralización y la optimización inteligente de la función de seguridad, lo que reduce significativamente el uso de los recursos del hipervisor. La integración nativa con una amplia gama de plataformas de virtualización, contenedores y nubes públicas proporciona visibilidad y control uniformes en toda la infraestructura. Una completa gama de tecnologías de seguridad gestionadas desde la misma consola garantiza una gestión de riesgos optimizada en entornos diversos a diario.

Perfecto para

Empresas que virtualizan cargas de trabajo de servidores y equipos de escritorio

Organizaciones que están trasladando o mantienen infraestructuras en nubes públicas

Empresas que aprovechan las nubes públicas y los contenedores para DevOps

Beneficios para su empresa

Garantiza una visibilidad y un control uniformes en las implementaciones de centros de datos y cloud

Reduce la superficie de ataque y el tiempo de espera y complica el movimiento lateral

Libera hasta un 30 % de los recursos del hipervisor y reduce el tiempo de inicio de sesión de minutos a segundos

Compatibilidad con el cumplimiento

Garantiza una colaboración eficaz entre los equipos de IT, seguridad de la información y desarrollo, reduciendo los riesgos y las brechas de seguridad

Casos de uso

- Protección con precaución en cuanto a los recursos para infraestructuras de servidores virtualizados
- Seguridad para VDI VMWare y Citrix
- Permite el cumplimiento de los requisitos de seguridad fundamentales
- Protección de cargas de trabajo en la nube para instancias de AWS y Azure con implementación automatizada y visibilidad sistemática mediante integración de API nativa
- Seguridad para DevOps con protección de contenedores y API de gestión

Kaspersky Security for Mail Server

Kaspersky Security for Mail Server protege contra las amenazas de correo, lo que evita que lleguen al endpoint, donde trabaja la mayor parte de la ingeniería social y el malware. Se bloquea todo tipo de malware, incluido el ransomware y la minería, así como los intentos de phishing, con especial atención a los ataques al correo electrónico corporativo. La solución también bloquea el correo masivo no deseado y evita las transmisiones de datos no deseadas.

Perfecto para

Cualquier empresa con una IT bien desarrollada que se preocupe sobre la privacidad y la seguridad de los datos

Cualquier empresa que dependa en gran medida de las comunicaciones por correo electrónico y que requiera una gestión detallada

Empresas que deseen enriquecer sus datos de detección de amenazas persistentes avanzadas (APT) con contexto de correo electrónico y bloquear los componentes de APT transmitidos por correo electrónico

Beneficios para su empresa

Aumenta la productividad al bloquear los correos electrónicos masivos no deseados, incluido el spam, y ofrecer categorías de correo para una gestión de las comunicaciones más cómoda

Ayuda a evitar interrupciones en la actividad empresarial mediante el bloqueo de amenazas de correo electrónico

Aumenta la seguridad de los datos al evitar la transferencia de tipos de datos poco deseables

Ayuda a reducir los gastos generales del servicio al reducir los incidentes a nivel de usuario

Aumenta la eficacia de la seguridad para pasarelas de correo existentes al añadir capacidades de detección superiores, sin aumentar los falsos positivos

Casos de uso

- Funciona con una amplia gama de agentes de transferencia de correo externos o como dispositivo virtual todo en uno.
- Proporciona seguridad de correo integrada por API para servidores Microsoft Exchange, que funcionan tanto en el nivel de la pasarela como del buzón de correo
- Bloquea las transferencias de tipos de archivo poco deseables
- Se integra con Kaspersky Anti Targeted Attack para bloquear los componentes de APT transmitidos por correo electrónico

Kaspersky Security for Internet Gateway

Kaspersky Security for Internet Gateway ofrece protección contra amenazas basadas en web a nivel del perímetro de defensa corporativo, impidiendo que alcancen el objetivo número uno para todas las formas de ataque, el endpoint. La solución ayuda a evitar los ataques basados en la ingeniería social y bloquea todo tipo de malware, incluidos el ransomware y la minería, así como los intentos de phishing. Combínelo con su proxy corporativo existente para mejorar el rendimiento o impleméntelo como dispositivo virtual todo en uno listo para usar.

Perfecto para

Cualquier empresa con una IT bien desarrollada que se preocupe sobre la privacidad y la seguridad de los datos

MSP y XSP (incluidos proveedores de telecomunicaciones)

Beneficios para su empresa

Evita las interrupciones en la actividad bloqueando las amenazas basadas en web antes de que alguien haga clic y les permita acceder

Aumenta la eficacia de la seguridad para pasarelas de correo existentes al añadir capacidades de detección superiores, sin aumentar los falsos positivos

Ayuda a reducir los gastos generales del servicio al reducir el número de incidentes a nivel de usuario

Aumenta la productividad y reduce los riesgos regulando el uso de Internet y la transmisión de tipos de archivo específicos

Ofrece capacidades multiusuario para la comodidad de los proveedores de servicios gestionados

Casos de uso

- Bloquea los recursos web maliciosos y de phishing, así como el malware descargado
- Evita el uso de recursos web poco deseables
- Permite la gestión de espacios de trabajo independientes con sus propios conjuntos de reglas
- Filtra los tipos de archivo no deseados que se transmiten en ambas direcciones, en función de varios criterios
- Se integra con Kaspersky Anti Targeted Attack como sensor de web y bloquea los componentes de los ataques dirigidos según los resultados de la detección avanzada

Kaspersky Security for Storage

El almacenamiento conectado de fácil acceso puede convertirse fácilmente en una fuente de infección en toda la infraestructura y en un objetivo de amenazas como el ransomware. Kaspersky Security for Storage protege los datos de la empresa y evita el contagio de la red con una sólida gama de tecnologías de protección basadas en la inteligencia global frente amenazas. Incluye funciones exclusivas como el mecanismo anticifrado remoto, facilitado por la integración con las API del sistema de almacenamiento.

Perfecto para

Cualquier empresa con una IT bien desarrollada que se preocupe sobre la privacidad y la seguridad de los datos

Empresas, por ejemplo, del sector de la banca, el comercio electrónico y los seguros, que trabajan con grandes volúmenes de datos confidenciales o privados

Beneficios para su empresa

Protege los datos en los sistemas de almacenamiento que se conectan sin acceder al software del almacenamiento

Reduce las complicaciones administrativas y aumenta la seguridad gracias a una consola de gestión única

Preserva la continuidad del negocio al mantener los datos almacenados a salvo de ransomware y crypto-wipers que se ejecutan de forma remota

Facilita el cumplimiento de normativas al ofrecer seguridad para una amplia gama de modelos que se pueden utilizar como almacenamiento regulado

Casos de uso

- Protege tanto los almacenamientos conectados a la red como el servidor en el que se ejecuta
- Siempre que aparezca un archivo nuevo en el almacenamiento protegido o se cambie un archivo existente, se comprobará si existe algún elemento malicioso. También es posible realizar análisis a petición
- Cuando los archivos empiezan a cifrarse desde lejos, la solución detecta y bloquea el origen en la red, evitando daños adicionales*

*Solo con integración de API disponible para algunos almacenamientos

Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security se caracteriza por una potente inteligencia sobre amenazas, detección de malware en tiempo real, controles exhaustivos para los dispositivos y aplicaciones, y una gestión flexible. Proporciona un sistema de seguridad todo en uno diseñado específicamente para los sistemas integrados.

Perfecto para

Servicios financieros

Minoristas y transporte

Proveedores de servicios de cajeros y puntos de venta

Beneficios para su empresa

Mitiga los riesgos asociados a las amenazas dirigidas a infraestructuras financieras específicas

Satisface los requisitos de cumplimiento de normativas como PCI/DSS, SWIFT, etc.

Optimiza los costes administrativos a través de una única consola de gestión

Casos de uso

- Protege sistemas integrados dispersos geográficamente y que pocas veces se actualizan que presentan problemas de seguridad específicos y únicos.
- Protección para Windows XP sin soporte que todavía se utiliza de forma generalizada en hardware de gama baja.
- Su diseño eficaz ofrece una seguridad potente y elimina el riesgo de sobrecarga de los sistemas.

Asistencia premium Kaspersky (MSA) servicio

Cuando se produce un incidente de seguridad, el tiempo necesario para identificar la causa y eliminarla es fundamental. Detectar y solucionar rápidamente un problema puede permitir a las empresas ahorrar costes importantes. Nuestros planes de acuerdo de servicio de mantenimiento (MSA) están diseñados específicamente para lograr este objetivo. Con acceso continuo a nuestros expertos, priorización adecuada y fundamentada de los problemas con tiempos de respuesta garantizados y parches privados: todo lo necesario para garantizar que el problema se resuelva lo antes posible.

Perfecto para cualquier organización que utilice productos de Kaspersky

Beneficios para su empresa

Garantiza la continuidad del negocio con expertos asignados en espera, con la tarea de encargarse de su problema y lograr la solución más rápida posible

Reducción del coste de un incidente de seguridad a través del acceso a una línea de asistencia prioritaria, tiempos de respuesta garantizados y parches privados

Un gestor de cuentas técnico exclusivo actúa como representante en Kaspersky Lab con autoridad necesaria para utilizar la experiencia y resolver el problema rápidamente

Casos de uso

- Transferencia directa de los problemas importantes a los especialistas auxiliares de la sede de Kaspersky Lab, que son los más adecuados para darle la solución apropiada en el menor tiempo.
- Las medidas proactivas totalmente adaptadas a su sistema, incluidas las revisiones prioritarias y los parches personalizados, le mantienen totalmente protegido.
- Reduzca el tiempo dedicado al mantenimiento y la solución de problemas de sus valiosos recursos internos.

Kaspersky Professional Services servicio

La ciberseguridad supone una gran inversión. Obtenga el mayor provecho posible mediante la colaboración con expertos que saben exactamente cómo puede optimizar su seguridad a fin de satisfacer los requisitos únicos de su organización. Siguiendo siempre las prácticas recomendadas y las metodologías establecidas, los expertos en seguridad estarán disponibles para ayudarle con cada aspecto relativo a la implementación, configuración y actualización de los productos de Kaspersky en su infraestructura de IT empresarial.

Kaspersky Professional Services comprende:

- Implementación y actualización
- La configuración
- Formación sobre productos

Perfecto para cualquier organización que utilice productos de Kaspersky

Beneficios para su empresa

Maximiza el retorno de la inversión en sus soluciones de seguridad al garantizar que funcionan al 100 % de su capacidad

Reduce los costes en personal de IT interno

Minimiza los riesgos de tiempo de inactividad mediante auditorías periódicas de las configuraciones de los productos, lo que garantiza que están en marcha los mecanismos defensivos más actualizados

Reduce el periodo de adopción del producto, lo que permite disfrutar más rápidamente todas las ventajas del producto implementado

Casos de uso

- Disminuye los riesgos de implementación que pueden reducir la protección, afectar negativamente a la productividad e incluso provocar tiempos de inactividad
- Minimiza el impacto que supone implementar una nueva solución de seguridad en las operaciones empresariales diarias y reduce los costes generales de implementación
- Prepara a su personal para realizar el mantenimiento continuo del producto con nuestros programas de formación que ayudan a evitar errores, demuestran las compatibilidades del producto y explican sus principios operativos

Kaspersky Security Awareness

Nuestros programas de formación por ordenador cambian los hábitos y forman nuevos patrones de comportamiento que son el auténtico objetivo de la formación en concienciación. El portfolio de formación de Kaspersky Security Awareness incluye: Automated Security Awareness Platform (ASAP): formación de concienciación para todos los empleados que desarrolla habilidades específicas de higiene cibernética día a día; Cybersecurity for IT Online (CITO): formación para especialistas de IT generalistas que desarrolla habilidades prácticas para reconocer un posible escenario de ataque y recopilar datos de incidentes; y Kaspersky Interactive Protection Simulation (KIPS): juego sobre ciberseguridad para los responsables de la toma de decisiones.

Perfecto para

Organizaciones cuyas expectativas de IT están creciendo y diversificándose

Organizaciones que desean reducir las oportunidades y la frecuencia de los errores de usuario que provocan brechas de seguridad

Beneficios para su empresa

Protege a las empresas desde dentro

Mantiene una "mentalidad de ciberseguridad" en toda la cultura corporativa

Reduce los errores humanos hasta en un 80 %

Casos de uso

- Desarrolla un comportamiento ciberseguro a través de escenarios y situaciones habituales, simulaciones de ciberataques y diferentes tareas y explicaciones.
- Fomenta la comprensión de las amenazas potenciales y proporciona las habilidades necesarias para tratarlas.
- Desarrolla las habilidades prácticas esenciales para reconocer un posible ataque en un incidente de PC aparentemente benigno, y la recopilación de datos del incidente para su traspaso al equipo de seguridad de IT.
- Establece una mejor concepción de la seguridad entre los altos directivos y los responsables de la toma de decisiones.

2 Defensa avanzada

Tecnología de detección avanzada y respuesta centralizada

Máxima automatización en la fase de detección y respuesta a amenazas complejas que no han detectado las tecnologías preventivas

- Entornos de IT cada vez más complejos y en crecimiento con una mayor superficie de ataque
- Pequeño equipo de seguridad con experiencia limitada
- Con capacidades básicas de respuesta ante incidentes

Perfecto para empresas medianas:

Endpoint

Kaspersky Endpoint Detection and Response

Personas

Formación Kaspersky Cybersecurity

Servicios

Kaspersky Targeted Attack Discovery

Red

Kaspersky Anti-Targeted Attack

Privacidad

Kaspersky Private Security Network

Inteligencia

Kaspersky Threat Intelligence

Kaspersky Endpoint Detection and Response

Para defenderse con éxito de amenazas avanzadas en la fase más temprana posible, es esencial complementar las tecnologías preventivas con capacidades avanzadas de detección de endpoints y de respuesta. Kaspersky EDR es una solución especializada que aborda las amenazas avanzadas para a los endpoints y comparte un único agente con nuestra solución de protección líder en el mundo, Kaspersky Endpoint Security. Kaspersky EDR proporciona una visibilidad integral de todos los endpoints de la red corporativa, lo que permite la automatización de tareas rutinarias para detectar, priorizar, investigar y neutralizar las amenazas complejas con rapidez.

Perfecto para

Empresas

Organizaciones que ya utilizan Kaspersky Endpoint Security

Equipos de SOC y respuesta ante incidentes

Beneficios para su empresa

Mitiga los riesgos asociados a amenazas avanzadas y ataques dirigidos

Optimiza los costes administrativos mediante la automatización de tareas y una única interfaz simplificada orientada a la empresa

Aumenta la velocidad y la efectividad del procesamiento de incidentes, sin costes adicionales

Aumenta la productividad y deja tiempo a los equipos de IT y seguridad para otras tareas

Facilita el cumplimiento de las políticas de seguridad internas y los requisitos normativos

Casos de uso

- Aborda el ciclo completo de protección de endpoints, desde el bloqueo automático de amenazas hasta la respuesta ante incidentes complejos frente a amenazas avanzadas, utilizando un solo agente
- Proporciona un acceso rápido a los datos de los endpoints, incluso cuando las estaciones de trabajo en peligro no están disponibles o los datos están cifrados
- Complementa las investigaciones de incidentes con la búsqueda de amenazas, el análisis de IOA y la asignación a MITRE ATT&CK
- Permite una respuesta eficaz en infraestructuras distribuidas a través de acciones automatizadas de amplio alcance

Kaspersky Anti Targeted Attack

El número y la calidad de los ataques dirigidos crecen continuamente. Para contrarrestar estas amenazas emergentes, es necesario adaptar constantemente los sistemas de seguridad. Kaspersky Anti Targeted Attack se centra en la detección avanzada de amenazas en el nivel de la red, con la recopilación, el análisis y la correlación de datos completamente automatizados y proporciona una comprensión detallada del alcance de la amenaza. El resultado es una protección eficaz de la infraestructura de su empresa frente a amenazas complejas y ataques dirigidos, sin necesidad de recursos adicionales.

Perfecto para

Empresas

Equipos de SOC

MSSP

Cualquier organización que deba cumplir requisitos normativos

Beneficios para su empresa

Mitiga los riesgos asociados a amenazas avanzadas y ataques dirigidos

Reduce los daños financieros y operativos mediante la introducción de un único sistema fiable para proteger contra ataques complejos

Optimiza los costes administrativos mediante la automatización de tareas y una única interfaz simplificada orientada a la empresa

Optimiza las tareas a través de la perfecta automatización del flujo de trabajo sin interrumpir los procesos empresariales

Ayuda a garantizar el cumplimiento de los requisitos normativos

Casos de uso

- Detección rápida de las acciones de los cibercriminales que burlan las tecnologías preventivas a través de la supervisión centralizada y el control de los posibles puntos de entrada a la infraestructura
- Detección de señales de amenaza y correlación de eventos de varios vectores dentro de un ataque en una única imagen, para permitir una investigación más eficaz
- Provisión oportuna al equipo de respuesta ante incidentes de toda la información necesaria sobre las amenazas detectadas

Kaspersky Private Security Network

Kaspersky Private Security Network permite a las empresas sacar el máximo partido de la mayoría de las ventajas que ofrece la inteligencia de amenazas global basada en la nube sin que sus datos abandonen el perímetro de control. Se trata de una versión personal, local y totalmente privada para la organización de Kaspersky Security Network.

Perfecto para

Empresas con estrictos requisitos de control de acceso a los datos

Infraestructuras críticas con redes físicamente aisladas

Proveedores de comunicaciones, seguridad gestionada y otros servicios

Beneficios para su empresa

Permite una detección superior de las amenazas dirigidas a su empresa

Garantiza tiempos de respuesta más rápidos mediante el acceso en tiempo real a las estadísticas de amenazas y reputación

Aumenta la eficacia operativa al minimizar los falsos positivos

Facilita el pleno cumplimiento de los requisitos normativos de la seguridad de redes y entornos aislados

Casos de uso

- Todas las ventajas de la seguridad con asistencia en la nube, sin necesidad de compartir información fuera de su infraestructura controlada
- Permite crear una protección personalizada añadiendo sus propios "veredictos"
- Adaptado para redes críticas aisladas

Kaspersky Targeted Attack Discovery servicio

Kaspersky Targeted Attack Discovery es un completo servicio de evaluación de riesgos que determina si está siendo atacado actualmente, qué está sucediendo y quién es el autor de la amenaza. Nuestros expertos detectan, identifican y analizan los incidentes en curso, así como los que se produjeron anteriormente, y elaboran una lista de los sistemas afectados por dichos ataques. Le ayudaremos a descubrir actividades maliciosas, comprender las posibles fuentes de un incidente y a planificar las acciones correctivas más eficaces.

Perfecto para

Empresas con equipos de seguridad inmaduros o inexistentes

Instituciones gubernamentales

Infraestructuras críticas

1 Conocimientos necesarios

5 Personalización y escalabilidad

3 Coste

Beneficios para su empresa

Previene y minimiza los daños derivados de los ataques a los sistemas, lo que reduce significativamente el coste

Ayuda a mantener la relación de confianza con sus clientes, socios e inversores para fomentar aún más las oportunidades de negocio

Garantiza que evite sanciones y multas por incumplimiento de normativas

Refuerza sus defensas contra futuros incidentes mediante recomendaciones correctivas

Casos de uso

- Permite entender la presencia digital de su organización y los riesgos asociados
- Ayuda a evaluar el riesgo mediante la realización de inspecciones en profundidad de la infraestructura y los datos de IT (como los archivos de registro) y el análisis de las conexiones de red salientes
- Identifica signos de intrusiones en curso o pasadas en sus redes
- Reconoce cómo está afectando este ataque a sus sistemas y qué puede hacer al respecto

Kaspersky Threat Intelligence

Contrarrestar las ciberamenazas de hoy requiere una visión global de las tácticas y herramientas que utilizan los actores de amenazas. La generación de esta inteligencia y la identificación de las tácticas defensivas más eficaces requieren una vigilancia constante y altos niveles de experiencia. Con los petabytes de datos de amenazas que se pueden extraer, las avanzadas tecnologías de aprendizaje automático y un conjunto exclusivo de expertos de todo el mundo, Kaspersky Lab trabaja para respaldarle con la inteligencia sobre amenazas más recientes de todo el mundo y ayudarle a mantener la inmunidad incluso ante ciberataques desconocidos.

Perfecto para

Empresas

Instituciones gubernamentales

Equipos de SOC y respuesta ante incidentes

MSSP

Beneficios para su empresa

Detección instantánea de amenazas para evitar la interrupción de las operaciones empresariales

Minimiza las posibles pérdidas financieras derivadas de los incidentes

Garantiza la rentabilidad de las inversiones en determinadas tecnologías y personal, en función de la información oportuna sobre las amenazas dirigidas a su empresa

Evita que los competidores obtengan una ventaja competitiva injusta a través de la filtración de la propiedad intelectual

Ayuda a crear **una defensa proactiva y adaptable**

Casos de uso

- Refuerce las soluciones de seguridad de red con **fuentes de datos de amenazas continuamente actualizadas.**
- Priorice de forma eficaz las cantidades abrumadoras de alertas de seguridad e identifique inmediatamente aquellas que se deben escalar a los equipos de respuesta ante incidentes con **fuentes de datos de amenazas** y **CyberTrace**.
- Obtenga una visión de la situación en tiempo real y aproveche las fuentes de inteligencia frente a amenazas de forma más eficaz con **CyberTrace**.
- Identifique la presencia digital de su organización y mitigue los riesgos asociados con **informes de inteligencia sobre amenazas personalizados**.

Formación Kaspersky Cybersecurity: Respuesta ante incidentes

servicio

La formación sobre la ciberseguridad es ahora una herramienta fundamental para las empresas, que deben enfrentarse a un número cada vez mayor de amenazas que no dejan de evolucionar. El personal de seguridad de IT debe formarse en el uso de técnicas avanzadas imprescindibles para las estrategias de gestión y mitigación eficaces de las amenazas a la empresa. La formación Kaspersky Cybersecurity ayuda a dotar a su equipo de seguridad interno de todos los conocimientos necesarios para hacer frente a un entorno de amenazas en constante evolución.

Perfecto para

Empresas

Instituciones gubernamentales

Equipos de SOC y respuesta ante incidentes

MSSP

3 Conocimientos necesarios

3 Personalización y escalabilidad

2 Coste

Beneficios para su empresa

Mitiga los posibles daños derivados de los incidentes de seguridad de forma rápida y eficaz, para reducir de forma significativa el coste del incidente

Garantiza que evite sanciones y multas por incumplimiento de normativas

Ayuda a mantener la relación de confianza con sus clientes, socios e inversores para fomentar aún más las oportunidades de negocio

Fortalece sus defensas frente a incidentes futuros a través de las lecciones aprendidas

Casos de uso

- Diferenciación de las APT del resto de amenazas
- Comprensión de las distintas técnicas de los atacantes y la anatomía de los ataques dirigidos
- Aplicación de métodos específicos de supervisión y detección
- Creación de reglas de detección eficaces
- Reconstrucción de la cronología y lógica del incidente y seguimiento del flujo de trabajo de respuesta ante incidentes

3 Enfoque de ciberseguridad integrada

Threat Management and Defense

Preparación para ataques de nivel de APT

Perfecto para empresas con un alto nivel de experiencia, acostumbradas a trabajar con inteligencia frente a amenazas y realizar tareas de búsqueda de amenazas

- Entornos complejos y distribuidos
- Equipo de seguridad interno o SOC
- Mayores costes de incidentes y robo de datos
- Cumplimiento de normativas

Servicios

- **Protección gestionada de Kaspersky**
- **Kaspersky Incident Response**

Personas

- **Formación Kaspersky Cybersecurity**

Inteligencia

- **Kaspersky Threat Intelligence**

Kaspersky Threat Management and Defense

Kaspersky Threat Management and Defense es una solución especializada que proporciona un marco completo para la detección rápida de amenazas, la investigación de incidentes, la respuesta y la corrección. Consta de inteligencia global frente a amenazas, tecnologías de respuesta y detección avanzada de amenazas, una amplia gama de formación sobre ciberseguridad, búsqueda continua de amenazas y respuesta a las amenazas que burlan las barreras de seguridad existentes. La solución se puede integrar en su estrategia organizativa actual para contrarrestar las amenazas complejas, complementar las tecnologías de protección existentes y ofrecerle una especialización líder cuando sea necesario.

Perfecto para

Empresas

Instituciones gubernamentales

Equipos de SOC y respuesta ante incidentes

MSSP

5 Conocimientos necesarios

5 Personalización y escalabilidad

5 Coste

Beneficios para su empresa

Minimiza los daños financieros y operativos causados por el cibercrimen y ayuda a mantener la estabilidad de la empresa

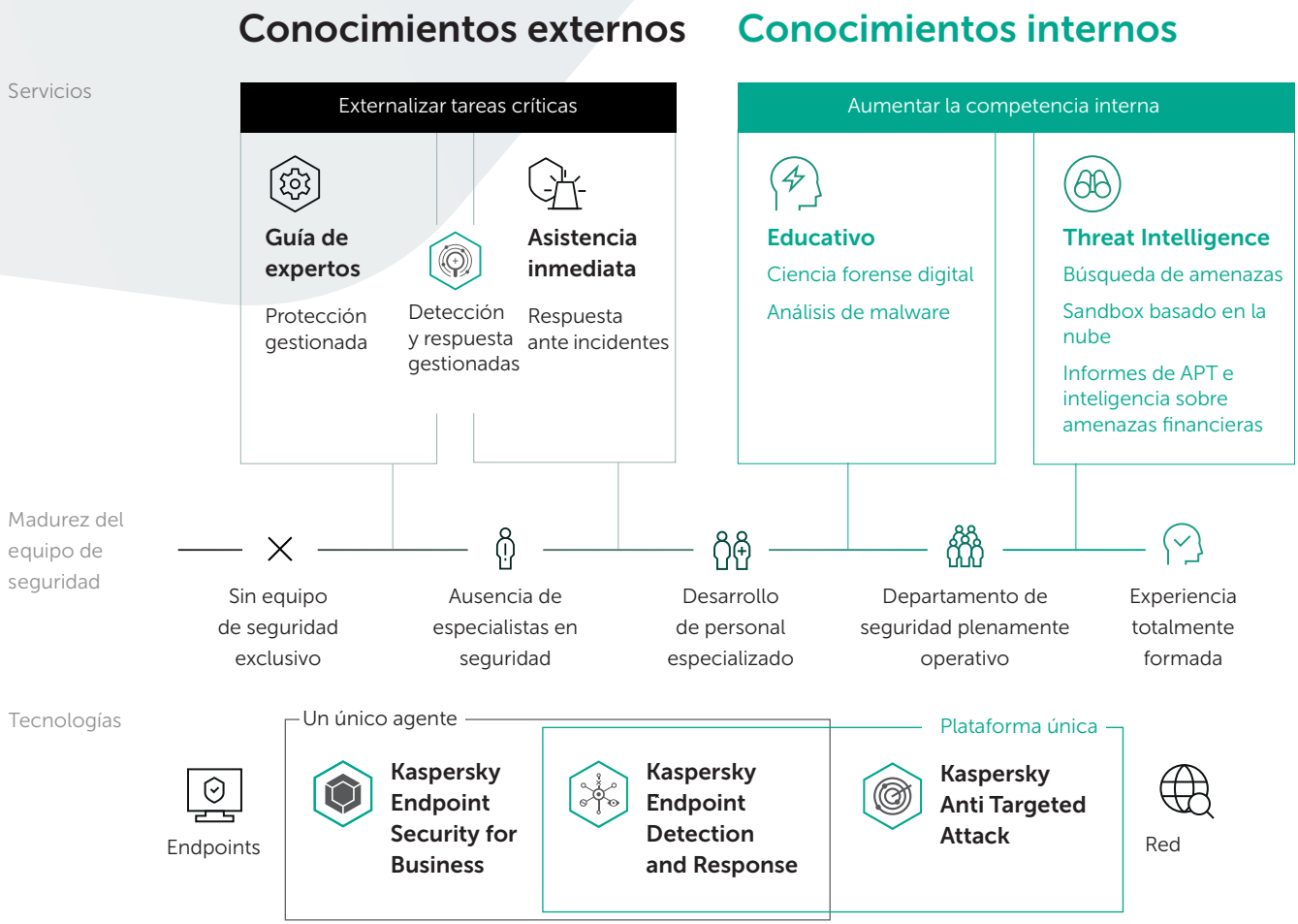
Aumenta el retorno de la inversión mediante la automatización y evita interrupciones en los procesos empresariales

Reduce los índices de rotación de personal y aumenta la eficacia operativa mediante el aumento de la especialización interna

Implementa estrategias de seguridad de la información rentables y completamente informadas basadas en modelos de amenazas personalizados

Casos de uso

- La plataforma tecnológica todo en uno automatiza la laboriosa recopilación de pruebas y las tareas manuales rutinarias
- La inteligencia de amenazas proactiva proporciona el contexto necesario para detectar, priorizar, investigar y responder con prontitud a las amenazas
- Estrategia de gestión de amenazas empresariales mediante la provisión de habilidades avanzadas
- La búsqueda de amenazas permite la detección de amenazas desconocidas y avanzadas diseñadas para eludir las tecnologías preventivas
- El acceso a la experiencia de terceros permite una investigación eficaz y una respuesta a incidentes complejos


Conocimientos externos
Conocimientos internos
Servicios
Externalizar tareas críticas
Aumentar la competencia interna
Guía de expertos
Protección gestionada
Detección y respuesta gestionadas
Asistencia inmediata
Respuesta ante incidentes
Educativo
Ciencia forense digital
Análisis de malware
Threat Intelligence
Búsqueda de amenazas
Sandbox basado en la nube
Informes de APT e inteligencia sobre amenazas financieras
Madurez del equipo de seguridad
Sin equipo de seguridad exclusivo
Ausencia de especialistas en seguridad
Desarrollo de personal especializado
Departamento de seguridad plenamente operativo
Experiencia totalmente formada
Tecnologías
Un único agente
Plataforma única
Endpoints
Kaspersky Endpoint Security for Business
Kaspersky Endpoint Detection and Response
Kaspersky Anti Targeted Attack
Red

Aspectos que hay que recordar al crear una estrategia de ciberseguridad a largo plazo

Un enfoque aislado de la ciberseguridad pone en peligro a las empresas

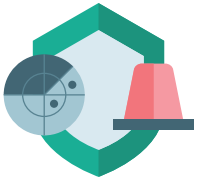
Los crecientes costes de las vulneraciones de redes y robo de datos ejercen serias presiones financieras en las empresas que desean transformarse, motivo por el que la ciberseguridad es un asunto tan importante. Para tener éxito en este entorno, las empresas deben convertir la ciberseguridad en una parte integral de su estrategia empresarial general, lo que desempeña un papel clave en la gestión de riesgos y la planificación a largo plazo.

La ciberseguridad no es solo un destino, es un viaje continuo

El plan de seguridad de una empresa se debe revisar y ajustar con regularidad a medida que estén disponibles nuevos conocimientos y herramientas. Todos los incidentes de seguridad deben someterse a un análisis detallado que tenga como consecuencia la creación de nuevos procedimientos y medidas de gestión de los ataques para evitar que ocurran incidentes similares en el futuro. Los mecanismos de defensa existentes deben mejorar de forma continua.

La concienciación, la comunicación y la cooperación son la clave del éxito en un mundo de ciberamenazas en constante cambio

Más del 80 % de los ciberincidentes se debe a errores humanos. La formación del personal en todos los niveles es esencial para aumentar la concienciación sobre la seguridad en toda la organización y motivar al conjunto de los empleados a prestar atención a las ciberamenazas y a las tácticas defensivas, incluso si no creen que forme parte de sus responsabilidades laborales.



Una mentalidad "detección y respuesta" practivas es la mejor forma de contrarrestar las amenazas en constante evolución actuales

Los sistemas de prevención tradicionales deberían funcionar en armonía con tecnologías de detección avanzadas, análisis de amenazas, capacidades de respuesta y técnicas de seguridad predictivas. Esto ayuda a crear un sistema de ciberseguridad que se adapta y responde continuamente a los desafíos empresariales emergentes.

¿Por qué elegir Kaspersky?

La marca más probada. Más premiada.

Kaspersky ha conseguido situarse más veces que ningún otro proveedor de seguridad en los primeros puestos de evaluaciones independientes. Y sigue haciéndolo año tras año.

www.kaspersky.es/top3

Una de las marcas más recomendadas

Kaspersky ha sido de nuevo la marca recomendada en la categoría de plataformas de protección de endpoints de Gartner Peer Insights Customer Choice, con unos índices de satisfacción de los clientes de 4,6 sobre 5 a 28 de mayo de 2019*.

La marca más transparente

Con la activación de nuestro primer centro de transparencia, y la base de procesamiento estadístico en Suiza, ofrecemos un control de los datos que ningún otro proveedor puede igualar.

*Gartner Peer Insights Customers Choice representa las opiniones subjetivas de revisiones, valoraciones y datos de usuarios finales individuales aplicados respecto a una metodología documentada, y de ninguna forma representan la opinión ni el aval de Gartner o de sus filiales.
Leer en el sitio web

Póngase en contacto con nosotros

Encuentre un partner próximo: www.kaspersky.com/buyoffline
Kaspersky for Business: www.kaspersky.es/business
Ciberseguridad de empresa: www.kaspersky.com/enterprise
Noticias de seguridad de IT: business.kaspersky.com/
Descubra nuestro exclusivo enfoque en: www.kaspersky.com/true-cybersecurity

#bringonthefuture

www.kaspersky.es

kaspersky

Bring on the future

www.kaspersky.es