KASPERSKY lab

Kaspersky Security Solutions for Enterprise

#TrueCybersecurity

Kaspersky
Security Solutions for Enterprise

Seguridad empresarial en una época de transformación digital

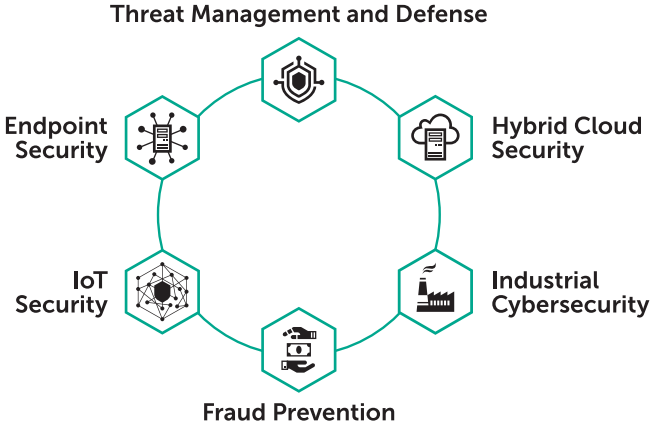
El número de ciberataques sigue aumentando considerablemente, y los ataques a la infraestructura corporativa son cada vez más profesionales y altamente adaptados. Ya no se trata de si sufrirá un ataque, sino de cuándo lo sufrirá y la rapidez y eficacia con la que se podrá recuperar.

Mientras tanto, la infraestructura de IT corporativa se ha vuelto cada vez más compleja, ya que se extiende más allá del perímetro organizativo, hasta los dispositivos móviles, las nubes públicas y proveedores externos. Aunque la transformación digital ofrece grandes beneficios en el ámbito de la eficacia y agilidad empresariales, también trae consigo nuevos desafíos de seguridad. Garantizar la continuidad empresarial y proteger tanto los resultados financieros como los datos corporativos y de los clientes impone considerables exigencias a su equipo de seguridad de IT y a su presupuesto.

La nueva cartera de soluciones empresariales de Kaspersky Lab refleja las demandas de seguridad de las empresas de hoy en día y crea una completa plataforma de ciberseguridad que combina funciones de protección totalmente escalables para sistemas físicos, virtuales y basados en la nube, incluidos los endpoints estáticos y móviles, los servidores, las redes, y el hardware y software especializados.

Esta combinación exclusiva de los principales servicios y tecnologías permite a su equipo de seguridad evitar la mayoría de los ataques, detectar nuevas amenazas concretas y predecir amenazas futuras, así como responder a incidentes emergentes. Ayudará a garantizar la continuidad operativa y el cumplimiento de las normativas.

Nuestra cartera se compone de las soluciones siguientes, todas ellas complementadas con una amplia gama de servicios expertos, formación en seguridad y asistencia profesional:



Estas soluciones y sus tecnologías de componentes se entremezclan para crear un marco de seguridad adaptable. Esto permite predecir, prevenir, detectar y corregir las amenazas a la ciberseguridad y los ataques dirigidos más sofisticados, y promover la continuidad empresarial y la resiliencia con un impacto mínimo en el rendimiento.

La auténtica ciberseguridad, asistida por una combinación de aprendizaje automático y experiencia humana, y respaldada por inteligencia sobre amenazas líder del sector, ofrece una protección superior del rendimiento junto con una mayor visibilidad y capacidad de gestión, además de una asistencia completa para su transformación digital.

La lucha por la libertad digital

Sus datos y privacidad son el objetivo de ataque de los cibercriminales y agentes de espionaje. Por tanto, necesita un partner que esté dispuesto a velar por sus intereses en la lucha por proteger sus activos corporativos. Kaspersky Lab tiene 20 años de experiencia en la detección de todo tipo de ciberamenazas, independientemente de si provienen de "script kiddies", cibercriminales o gobiernos, o bien del norte, el sur, el este o el oeste. Creemos que el mundo digital debe estar libre de ataques y espionajes financiados por el Estado y seguiremos luchando para fomentar la creación de un mundo digital verdaderamente gratuito y seguro.

Probado

Kaspersky Lab suele ocupar los primeros puestos en un gran número de encuestas y puntuaciones independientes.

- Comparado con **80 proveedores reconocidos** en el sector
- **72 primeros puestos** en 86 pruebas y revisiones en 2017
- **Entre los 3 primeros*** en más del 90 % de todas las pruebas de productos
- En 2017, Kaspersky Lab recibió el **estatus Platinum** por los premios Gartner Peer Insights** Customer Choice Awards en el mercado de plataformas de protección de endpoints

Nuestro equipo de análisis e investigación global ha participado activamente en el descubrimiento y la revelación de los ataques de malware más importantes vinculados con diversos gobiernos y organizaciones estatales.

Transparente

Actuamos con absoluta transparencia y presentamos de forma clara lo que hacemos:

- Revisión independiente del código fuente, las actualizaciones de software y las reglas de detección de amenazas de la empresa
- Revisión independiente de los procesos internos
- Tres centros de transparencia para el año 2020
- Mayores recompensas por detección de amenazas: un máximo de 100 000 USD por cada vulnerabilidad descubierta

Independiente

Como empresa privada, somos independientes de consideraciones comerciales a corto plazo y de influencias institucionales.

Compartimos nuestra experiencia, conocimientos y resultados técnicos con la comunidad de seguridad mundial, los proveedores de seguridad de IT, las organizaciones internacionales y los cuerpos de seguridad.

Nuestro equipo de investigación está repartido a nivel global e integrado por algunos de los más renombrados expertos en seguridad del mundo. Detectamos y neutralizamos todo tipo de APT, independientemente de su origen o finalidad.

* www.kaspersky.es/top3
** https://www.gartner.com/reviews/customerchoice- awards/endpoint-protection-platforms

Endpoint Security

La plataforma líder de protección de endpoints de varios niveles, basada en tecnologías de ciberseguridad de próxima generación

El entorno de las amenazas avanza de manera exponencial, lo que supone un riesgo cada vez mayor ante ataques de día cero para los procesos empresariales de especial importancia, datos confidenciales y recursos económicos. Con el fin de mitigar los riesgos a los que se enfrenta su empresa, debe ser más inteligente, estar mejor equipado y contar con más información que los ciberprofesionales que le atacan. Sin embargo, nos encontramos ante un hecho indiscutible: la mayoría de los ciberataques contra empresas se inician a través del endpoint. Si puede proteger de manera eficaz todos los endpoints corporativos, tanto fijos como móviles, dispondrá de una sólida base para su estrategia de seguridad global.

En los premios Gartner Peer Insights Customer Choice Awards for Endpoint Protection Platforms de 2017 **fuimos el único proveedor que recibió un premio Platinum***.

* El logotipo de Gartner Peer Insights Customer Choice es una marca registrada y una marca de servicio de Gartner, Inc., o de sus filiales, y se utiliza aquí con permiso. Todos los derechos reservados. Los premios Gartner Peer Insights Customer Choice Awards (https://www.gartner.com/reviews/customer-choice-awards/endpointprotection-platforms) están determinados por las opiniones subjetivas de los usuarios finales individuales, que se basan en sus propias experiencias, el número de revisiones publicadas en Gartner Peer Insights y las valoraciones generales que recibe un proveedor determinado en el mercado, tal como se describe detalladamente aquí: http://www.gartner.com/reviews-pages/peer-insights-customer-choice-awards/; de ninguna forma pretenden representar la opinión de Gartner o de sus filiales.

La transformación digital trae consigo riesgos adicionales

La creciente complejidad de la mayoría de las redes de IT corporativas puede crear "brechas de visibilidad" donde las amenazas se pueden ocultar.

De media, un ataque dirigido puede continuar acechando en los sistemas objetivo y pasar totalmente inadvertido durante 214 días.

Durante este periodo, la amenaza podría continuar llevando a cabo un amplio abanico de actividades maliciosas. Por eso es de vital importancia el uso de herramientas eficaces que puedan detectar, eliminar y corregir las amenazas rápidamente.

Lamentablemente, a pesar de las grandiosas declaraciones de algunos proveedores, no hay ni un producto de seguridad milagroso que pueda garantizar una protección del 100 % frente a todos los tipos de riesgos. Del mismo modo, tampoco hay una corrección que sea definitiva. La seguridad de IT es un proceso constante de evaluación del desarrollo de los peligros; a continuación, habrá que:

- adaptar y actualizar de las políticas de seguridad, e
- implementar nuevas tecnologías de seguridad

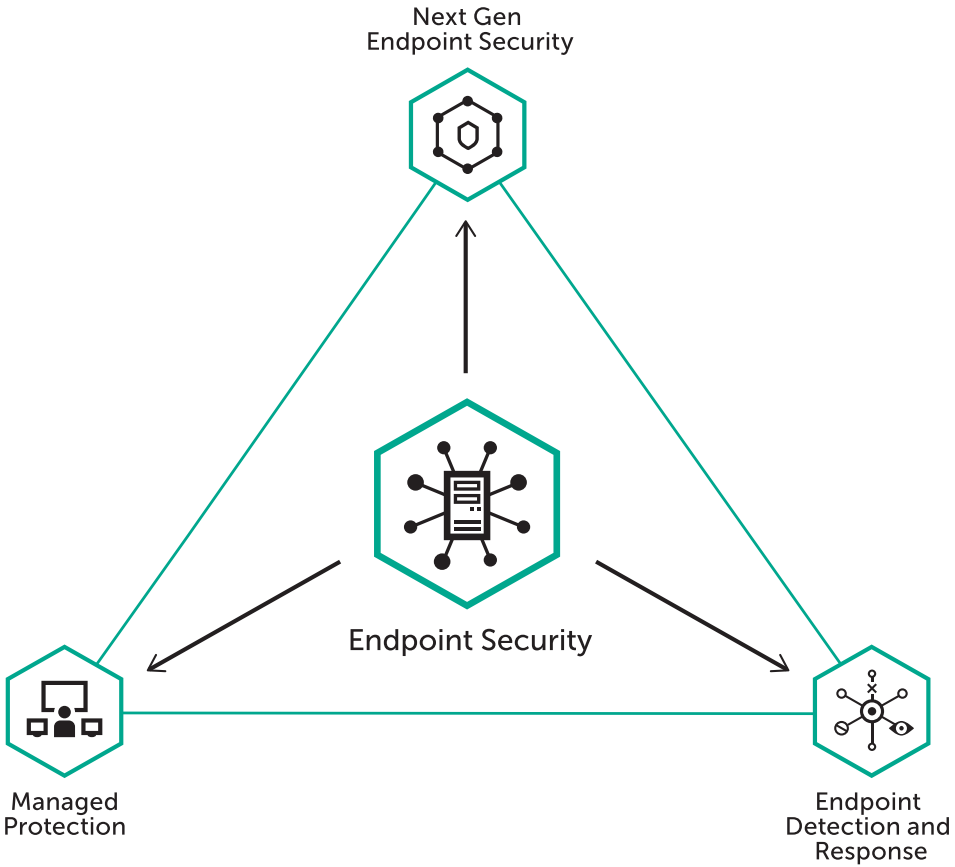
Todo ello para enfrentarse a nuevos riesgos.

Kaspersky Endpoint Security responde a estas necesidades a través de una plataforma de seguridad con protección a varios niveles, fiable y de eficacia probada que protege también sus resultados financieros. Se trata de una solución perfectamente integrada que combina funciones extraordinarias de protección, detección y respuesta ante incidentes. Está basada en inteligencia de seguridad global y aprendizaje automático de próxima generación inigualables para enriquecer automáticamente su SOC y mejorar sus funciones de mitigación de riesgos. La protección para todos los endpoints físicos, virtuales y basados en la nube se gestiona a la vez a través de una sola consola, lo que mejora la eficiencia y reduce el coste total de propiedad.

Esta plataforma incluye:

- **Next Gen Endpoint Security**
  Protección totalmente escalable basada en nuestro premiado motor de inteligencia sobre amenazas, e incorporación de controles con gran nivel de detalle y tecnologías antiransomware y de prevención de exploits.
- **Endpoint Detection and Response**
  Búsqueda de adversarios y detención de las amenazas antes de que puedan causar costosos daños, además de responder de manera rápida y eficaz a los incidentes y el robo de datos.
- **Managed Protection**
  Un servicio de respuesta ante incidentes y de supervisión continua del reconocido líder mundial en la investigación de APT, dedicado a la caza de ciberamenazas para su organización.

Solución de seguridad para endpoints



Modus operandi de los ataques

La mayoría de los ataques tienen cuatro fases distintas:

- **Detección**, es decir, la identificación de puntos de entrada apropiados para el ataque
- **Intrusión** en un endpoint de la red corporativa
- **Infección**, a menudo propagándose a muchas ubicaciones de la red corporativa
- **Implementación** de las acciones maliciosas del cibercriminal

Defensa para cada una de las fases

Una de las claves para lidiar con un ataque es tener defensas que puedan ofrecer protección en cada una de las cuatro fases del ataque.

Prevención de la exposición a la detección
Para bloquear el acceso a los puntos de entrada potenciales

Protección previa a la ejecución de la intrusión
Para detectar las amenazas antes de que puedan causar infecciones

Procesos posteriores a la ejecución de la infección
Para detectar comportamientos sospechosos y ayudar a prevenir que la infección lleve a cabo acciones maliciosas

Respuesta automática a la implementación
Para ayudar a la víctima a recuperar los sistemas y datos empresariales, además de identificar cómo evitar ataques similares en el futuro

Protección a varios niveles con un solo proveedor

Ofrecemos defensas para cada fase de un ataque, y en cada fase, no solo ofrecemos un nivel de defensa, sino que ofrecemos varias técnicas de defensa. De esta forma, nuestros clientes se benefician de una protección a varios niveles en cada fase de un ataque.

Fase de defensa 1: prevención de la exposición
Ayudamos a bloquear los ataques en los puntos de entrada potenciales.

Nuestros niveles de protección incluyen:

- Filtrado de red
- Filtrado de contenido en la nube
- Controles de puertos

Fase de defensa 2: seguridad previa a la ejecución
Ayudamos a poner fin al inicio del "intruso".

Nuestros niveles de protección y servicios incluyen:

- Refuerzo de endpoints
- Servicios de reputación
- Detección previa a la ejecución basada en el aprendizaje automático

Fase de defensa 3: control de tiempo de ejecución
Buscamos comportamientos sospechosos de forma proactiva en todos los dispositivos conectados a la red corporativa, incluidos en los propios dispositivos móviles de los empleados.

Nuestros niveles de protección incluyen:

- Análisis de comportamiento basado en el aprendizaje automático, incluidas:
  - Prevención de exploits
  - Protección contra ransomware
- Control de privilegios de ejecución

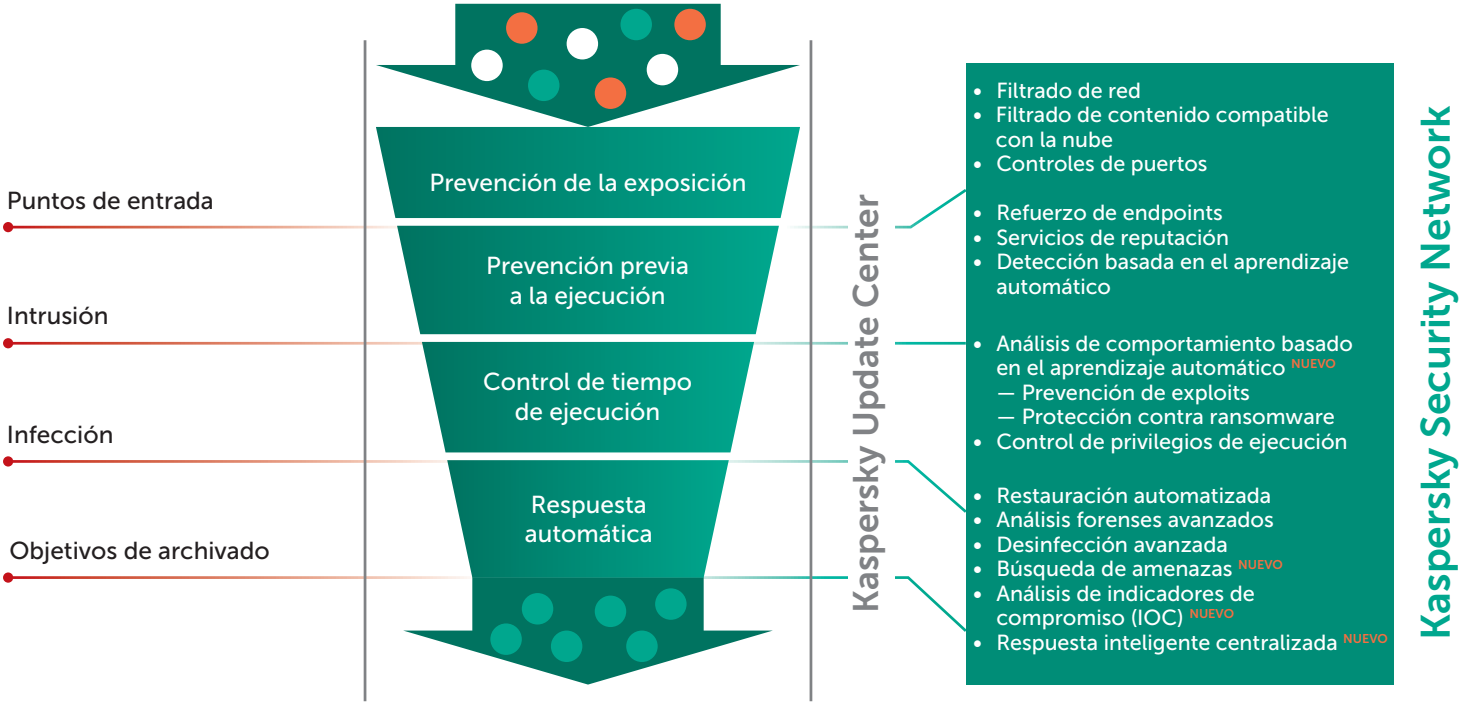
Fase de defensa 4: respuesta automática
Si su empresa ha sufrido un ataque, nosotros le ayudamos a lidiar con las secuelas de forma más rápida.

Entre nuestros servicios y tecnologías se incluyen:

- Restauración automática: para ayudar a restaurar el sistema al estado previo al ataque
- Análisis forenses avanzados
- Desinfección avanzada
- Búsqueda de amenazas
- Análisis de indicadores de compromiso (IOC)
- Respuesta inteligente centralizada

Nuestro nivel meta ayuda a las empresas a hacer más para protegerse contra los ataques dirigidos y APT peligrosos mediante la correlación de los hallazgos de los niveles de defensa individual y la identificación de las amenazas que pueden colarse a través de las defensas individuales.

Cadena de ataques



Seguridad móvil

Herramientas de gestión y seguridad de apoyo a su estrategia de seguridad móvil

Según nuestra encuesta de 2017, el 38 % de las empresas experimentó exploits o pérdidas a través de los dispositivos móviles como el principal vector de ataque.

1 700 000 USD

Este es el coste medio que supone para una empresa un incidente de seguridad que incluya exploits o pérdidas de datos a través de dispositivos móviles

El software malicioso y los ataques de phishing y de sitios web dirigidos a los dispositivos móviles no dejan de proliferar, mientras que las funciones de los dispositivos móviles todavía se están desarrollando. Puesto que son una importante herramienta de productividad tanto en casa como en el trabajo, los dispositivos móviles resultan un objetivo tentador para los cibercriminales. El uso en alza de dispositivos personales para fines laborales (tendencia BYOD o "traiga su propio dispositivo") amplía la variedad de tipos de dispositivos y plataformas en la red corporativa, y plantea nuevos desafíos para los administradores de IT que tratan de gestionar y controlar sus infraestructuras.

Los dispositivos personales de los empleados suponen un riesgo empresarial

Los empleados que utilizan sus dispositivos móviles para un uso personal y laboral incrementan las probabilidades de brechas en la seguridad de IT. Una vez que los hackers consiguen llegar a la información personal no segura de un dispositivo móvil, les resulta muy sencillo acceder a los sistemas corporativos y los datos empresariales de los usuarios.

Ninguna plataforma es segura

Los cibercriminales utilizan distintos métodos para lograr acceso no autorizado a dispositivos móviles, como aplicaciones infectadas, redes Wi-Fi públicas con bajos niveles de seguridad, ataques de phishing y mensajes de texto infectados. Cuando un usuario visita un sitio web malicioso sin querer, o incluso un sitio web legítimo con código malicioso, pone en peligro la seguridad de su dispositivo y los datos que este contiene. Incluso conectar un iPhone a un Mac para cargar la batería puede transferir amenazas maliciosas desde el Mac al iPhone. (Estas amenazas se aplican a todas las plataformas móviles: Android, iOS y Windows Phone).

La solución: Kaspersky Security for Mobile

Kaspersky Security for Mobile resuelve estos problemas al ofrecer Mobile Threat Defense (MTD) multicapa y funciones de gestión de dispositivos móviles. La combinación de estas capacidades permite a los equipos de seguridad adoptar un enfoque proactivo para la gestión de amenazas móviles.

Todas las funcionalidades para dispositivos móviles y endpoints se pueden gestionar desde la misma consola para luchar así de forma eficaz contra el cibercrimen corporativo.

La combinación del cifrado y la protección funcionales contra malware permiten que Kaspersky Security for Mobile proteja los dispositivos móviles de forma proactiva, en lugar de limitarse a aislar un dispositivo y sus datos.

Protección avanzada para dispositivos móviles

Las funciones antimalware se combinan con la inteligencia sobre amenazas con asistencia en la nube y el aprendizaje automático para proteger frente a las amenazas móviles sofisticadas.

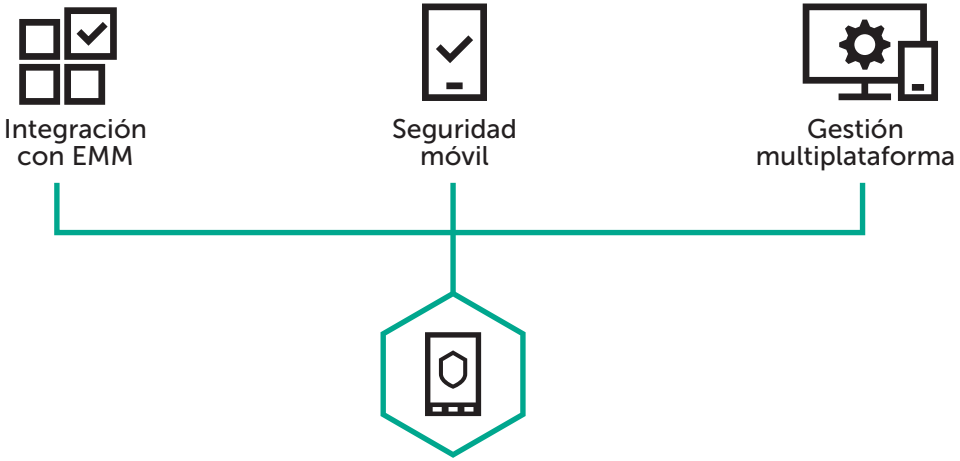
Control web, antiphishing y antispam

Las potentes tecnologías de control web, antiphishing y antispam protegen de ataques de phishing, y ayudan a descartar los sitios web, las llamadas y los mensajes de texto no deseados.

Integración con plataformas EMM

Implementación y gestión completas de la seguridad móvil a través de su consola EMM (VMware AirWatch, Citrix XenMobile).

Protección avanzada para dispositivos móviles



Hybrid Cloud Security

Seguridad sin fronteras diseñada para entornos de varias nubes

Nuestra solución Hybrid Cloud Security proporciona protección unificada y a varios niveles para entornos basados en la nube. Dondequiera que procese y almacene los datos empresariales importantes (en una nube privada, pública o en ambas), le ofrecemos una combinación perfectamente equilibrada de seguridad continua y ágil, con una eficacia superior, que protege sus datos frente a las amenazas actuales y futuras más sofisticadas sin poner en peligro el rendimiento de los sistemas.

El aprovisionamiento simplificado se logra a través de la integración de la API nativa, mientras que se garantiza el consumo de recursos más bajo posible y se proporcionan funciones precisas para defender los entornos de nube híbrida contra todas las formas de ciberamenazas. Todo con la organización y gestión de seguridad unificadas.

Ciberseguridad de próxima generación para cualquier nube

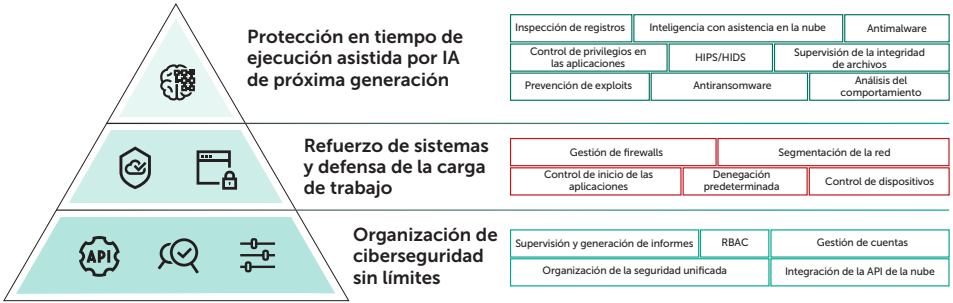
Abordamos la necesidad de proteger lo que implementa en nubes públicas como parte de su responsabilidad compartida en materia de seguridad. La integración con las API de la nube nos permite ofrecer las premiadas tecnologías de ciberseguridad para cada carga de trabajo en la nube.

Organización y transparencia unificadas

La capacidad de gestión, flexibilidad y visibilidad sin límites se proporcionan a través de una consola de organización de seguridad de nivel empresarial. Una transparencia extraordinaria significa que usted sabe exactamente lo que está pasando en su entorno de nube híbrida. Esta visibilidad, junto con el aprovisionamiento totalmente automatizado de funciones de ciberseguridad, permite la organización perfecta de una seguridad que es mejor y más rápida en su entorno de nube.

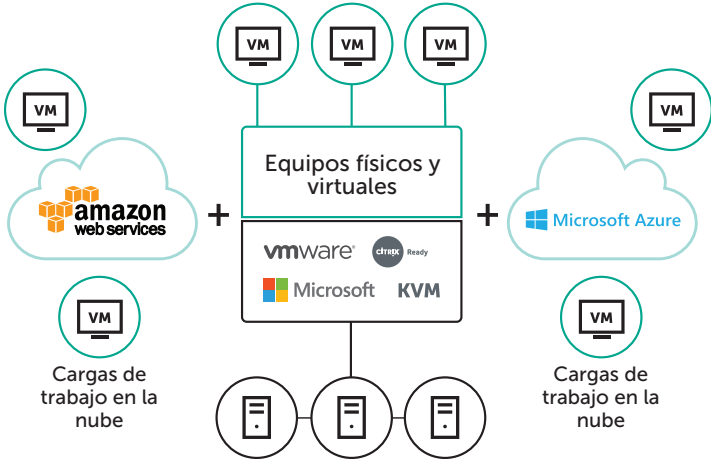
Para entornos de nube flexibles y seguros

Seguridad probada para servidores físicos y virtuales, implementación de VDI, sistemas de almacenamiento, e incluso canales de datos. La arquitectura y las funciones de integración patentadas ayudan a construir la ciberseguridad en el núcleo de su entorno de IT, a la vez que se mantiene la eficacia operativa de los sistemas esenciales de la empresa.



Kaspersky Hybrid Cloud Security

Kaspersky Hybrid Cloud Security le ofrece todo lo necesario para construir un ecosistema de ciberseguridad perfectamente organizado y adaptable. Ofrece las funciones precisas que necesitan las cargas de trabajo en la nube híbrida, mientras que la eficacia de los recursos y una organización perfecta siguen siendo primordiales. Kaspersky Hybrid Cloud Security se ha diseñado para proteger aplicaciones y datos en las cargas de trabajo físicas, virtuales y en la nube. Así se garantiza la sostenibilidad empresarial y se acelera el cumplimiento en todo su entorno de nube híbrida.



En su centro de datos privado, donde las cargas de trabajo corporativas se ejecutan en servidores físicos o virtuales, o incluso en entornos VDI, deben tenerse en cuenta un número de factores como parte de una estrategia de transformación digital exitosa:

- **Proteger el acceso a los datos y su procesamiento** independientemente de la plataforma de virtualización o el entorno físico en los que se ejecutan las cargas de trabajo.
- **Interoperabilidad entre IT y los niveles de seguridad** mediante el uso de API nativas para garantizar tiempos de respuesta prácticamente nulos ante las amenazas sofisticadas.
- **Operación eficaz de los recursos** para mejorar el rendimiento de IT y mantener la productividad de los sistemas esenciales de la empresa.

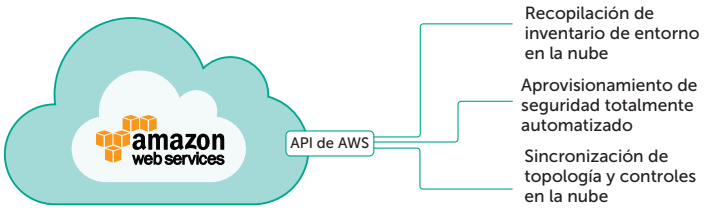
Kaspersky Hybrid Cloud Security ofrece una excelencia demostrada en la protección de centros de datos definidos por software diseñados en las plataformas de virtualización VMware NSX, Citrix XenServer y XenDesktop, MS Hyper-V y KVM, lo que elimina la complejidad en la gestión de entornos empresariales. La integración con IT básica a través de API nativas ayuda a abordar las necesidades de seguridad con un impacto casi nulo sobre el valioso rendimiento del sistema.

- La seguridad integrada sin agentes para VMware NSX para vSphere permite que los niveles de seguridad e IT interoperen para ofrecer mayor protección.
- Protección de agentes ligeros patentada para servidores virtuales y plataformas VDI con un uso eficaz de los recursos y un funcionamiento con tolerancia a errores.
- Seguridad a varios niveles tradicional para servidores físicos que incorpora tecnologías antiransomware, de prevención de exploits y detección del comportamiento.

Ciberseguridad automatizada para las nubes públicas

La creciente adopción de un modelo de servicios en la nube, donde los recursos del centro de datos privados se amplían instantáneamente a petición y en función de las necesidades a las nubes externas, proporciona una flexibilidad sin precedentes, agilidad y beneficios económicos claros. Sin embargo, el modelo de responsabilidad compartida en materia de seguridad dicta la necesidad de utilizar funciones adicionales, lo que permite un nivel de ciberseguridad flexible que cubre todo su entorno en la nube y protege sus cargas de trabajo de Amazon Web Services (AWS) o Microsoft Azure.

Integración con Amazon Web Services (AWS)



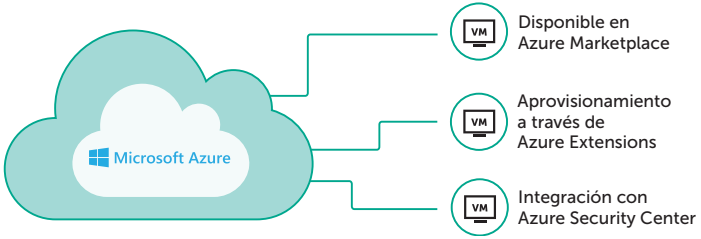
Kaspersky Hybrid Cloud Security ayuda a defender los activos en la nube y aborda la necesidad de proteger cualquier elemento implementado en la nube pública como parte de su responsabilidad compartida en materia de seguridad. Kaspersky Hybrid Cloud Security ofrece una protección a varios niveles que se integra con la API en la nube y está disponible a través de los mercados para ofrecer técnicas de ciberseguridad premiadas para todas las cargas de trabajo en la nube con agilidad y capacidad de gestión mayores. Así se ofrece una experiencia de organización de ciberseguridad de la nube híbrida de calidad superior.

- Ciberseguridad líder del sector que protege sus cargas de trabajo en las nubes públicas mediante el uso de la integración nativa a través de la API de la nube con Amazon Web Services (AWS) y Microsoft Azure Extensions.
- Complementa las funciones de seguridad nativas de la nube y ayuda a proteger las aplicaciones, los sistemas operativos, los datos y los usuarios en la nube, a la vez que respalda el cumplimiento con el GDPR.
- La arquitectura inteligente y la integración de la API minimizan el impacto en los recursos de la nube, y automatiza el aprovisionamiento del inventario y la seguridad.

Proporciona incluso más protección

Complementamos las herramientas nativas de la nube con funciones proactivas de ciberseguridad, prevención de exploits, supervisión de la integridad, inspección de registros, controles de aplicaciones, e incluso funciones de protección en tiempo de ejecución asistida por IA y antiransomware. Un producto para luchar contra todo tipo de ciberamenazas.

Diseñado para Microsoft Azure



Seguridad imparable para cualquier nube

La adopción de la nube nunca ha sido tan perfecta y segura a la vez. Con Kaspersky Hybrid Cloud Security, la integración a través de API nativas facilita el aprovisionamiento de la seguridad automatizada y el inventario de la infraestructura de nube pública en todas sus instancias ubicadas en AWS y Microsoft Azure.

Kaspersky Hybrid Cloud Security ofrece varias tecnologías de seguridad reconocidas por el sector para respaldar y simplificar la transformación de su entorno de IT mediante la protección de su migración del entorno físico al virtual y a la nube, mientras que la visibilidad y transparencia garantizan una experiencia de organización de la seguridad sin fisuras.

Kaspersky Security for Storage

Kaspersky Security for Storage proporciona una protección sólida, de alto rendimiento y escalable para los valiosos datos confidenciales que se ubican en dispositivos de almacenamiento conectados a la red (NAS) y servidores de archivos corporativos.

La integración fluida a través de protocolos rápidos, incluidos ICAP y RPC, preserva la eficacia de los sistemas de almacenamiento para mantener una protección fiable y eficaz en el uso de los recursos, así como una experiencia de usuario final optimizada. Protección en tiempo real fiable del almacenamiento, incluidas funciones de autoprotección para una óptima continuidad.

Protección de datos fiable y transparente

- La integración nativa se traduce en flexibilidad, escalabilidad y eficiencia operativa excepcionales, sin ningún efecto adverso sobre el rendimiento y la productividad de los sistemas de almacenamiento de datos y la productividad.
- Las tecnologías innovadoras ofrecen las funciones de protección más avanzadas y una tolerancia a errores excepcional, e incluso puede protegerle de ataques de ransomware.

Protege sus datos independientemente de la ubicación en la que estén almacenados

- Se integra de forma nativa con los últimos dispositivos NAS y funciona en servidores de archivos corporativos
- Todos los archivos ubicados en sistemas de almacenamiento de datos son seguros, sin necesidad de comprobar el análisis antimalware en los endpoints o dispositivos móviles
- Configuración granular y flexible para las tareas de análisis antimalware por acceso y a petición
- Funciones de autoprotección para una continuidad operativa óptima

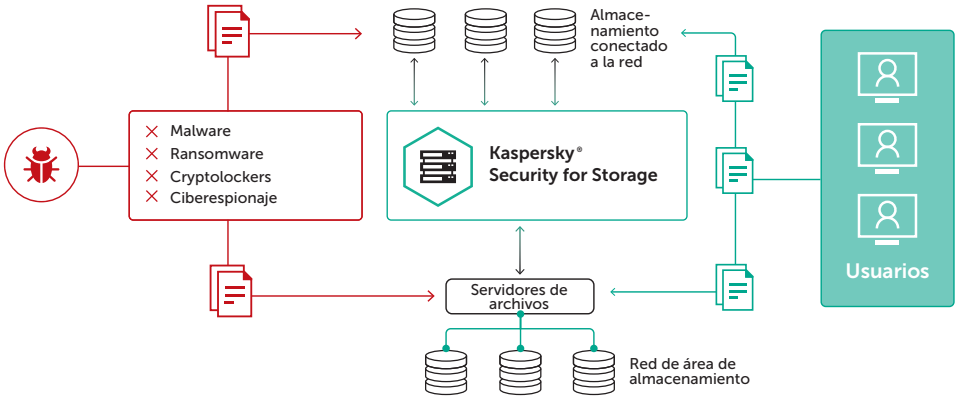
Combate el malware y el ransomware

- Nuestro premiado motor de análisis antimalware protege todos los archivos contra los ataques más sofisticados
- Protección antiransomware en tiempo real para dispositivos NAS de NetApp a través de FPolicy (Kaspersky Lab ha sido el pionero en aplicar esta protección)
- Asistencia para una amplia gama de dispositivos de almacenamiento gracias a la integración a través de diversos protocolos

Ofrece seguridad ligera, pero fiable

- La integración a través de la API nativa se traduce en una mayor seguridad con un impacto menor en la productividad del usuario final
- El equilibrio de carga y la tolerancia a errores garantiza una protección ininterrumpida
- Visibilidad completa de ciberseguridad de los archivos de datos activada en toda su infraestructura de almacenamiento

Kaspersky Security for Storage puede combinarse con Kaspersky Hybrid Cloud Security para aplicar una protección excelente sobre los componentes tanto físicos como virtualizados de su centro de datos corporativo.



Kaspersky DDoS Protection

El impacto financiero de un solo ataque DDoS puede oscilar entre 106 000 y 1 600 000 $ dependiendo del tamaño de la empresa. ¿Cuánto cuesta organizar un ataque DDoS? Unos 20 $.

Puesto que el coste de lanzar un ataque de denegación de servicio distribuido (DDoS) ha disminuido, el número de ataques ha aumentado. Los ataques se han vuelto más sofisticados y difíciles de evitar. La naturaleza cambiante de estos tipos de ataques exige una protección más rigurosa.

A diferencia de los ataques de malware que tienden a propagarse automáticamente, los ataques DDoS se basan en la experiencia y los conocimientos humanos. El atacante investigará a la empresa que haya establecido como blanco, evaluará sus vulnerabilidades y elegirá cuidadosamente las herramientas de ataque más adecuadas para lograr sus objetivos. Entonces, los cibercriminales, que trabajan en tiempo real durante el ataque, cambian constantemente de táctica y seleccionan diferentes herramientas para maximizar el daño que infligen.

Para protegerse contra los ataques DDoS, la empresa necesita una solución que los detecte tan rápidamente como sea posible.

La solución: Kaspersky DDoS Protection

Kaspersky DDoS Protection ofrece una solución de protección y mitigación contra ataques DDoS completa que se ocupa de todas las fases de la defensa de su empresa contra todo tipo de ataques DDoS. Hay disponibles tres opciones de implementación: Connect, Connect+ y Control.

En cuanto se identifica un posible caso de ataque, el Centro de operaciones de seguridad (SOC) de Kaspersky Lab recibe una alerta. En los escenarios de implementación de Kaspersky DDoS Protection Connect y Connect+, la mitigación se inicia automáticamente mientras nuestros ingenieros ejecutan de inmediato minuciosas comprobaciones para optimizar la mitigación en función del tamaño, el tipo y el grado de sofisticación de los ataques DDoS. Con Kaspersky DDoS Protection Control, usted decide cuándo iniciar la mitigación teniendo en cuenta su política de ciberseguridad, sus objetivos empresariales y su infraestructura.

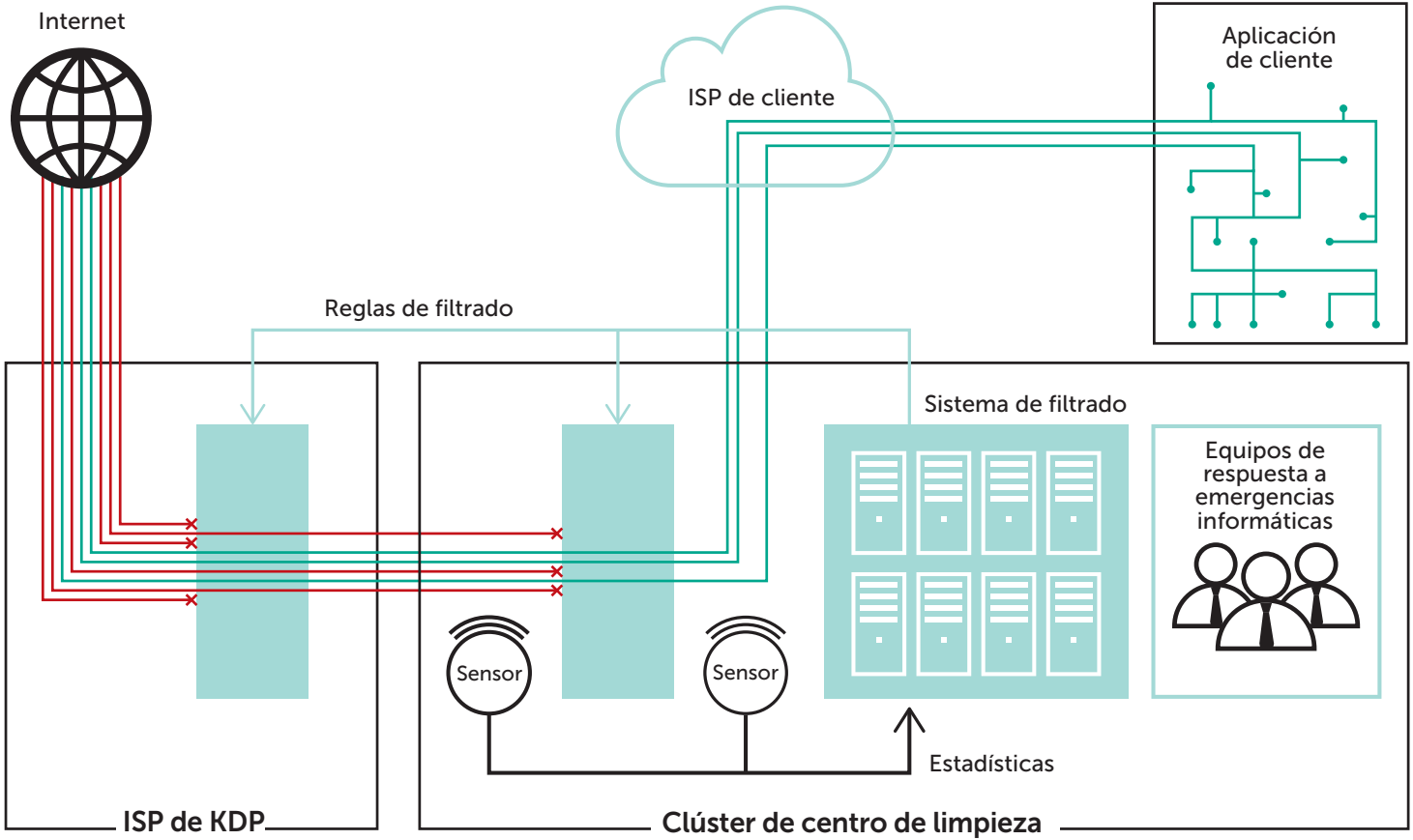
Con la flexibilidad para adaptarnos a diferentes configuraciones, podemos garantizar que satisfacemos las necesidades de su negocio y de sus activos online.

Arquitectura de Kaspersky DDoS Protection

Esta solución completa de defensa proporciona:

- Protección integral de las infraestructuras de red y los recursos online vitales para la empresa
- Opciones flexibles de implementación: Kaspersky DDoS Protection Connect, Connect+ y Control
- Centros de limpieza altamente escalables en toda Europa
- Inteligencia de DDoS global en tiempo real basada en análisis de seguridad de la información
- Protección y asistencia rápidas ininterrumpidas por parte del equipo de respuesta a emergencias.

Kaspersky DDos Protection



Threat Management and Defense

Protección avanzada e inteligencia sobre amenazas

La protección de infraestructuras altamente digitalizadas ofrece importantes desafíos empresariales nuevos:

- La necesidad de realizar un gran volumen de tareas manuales para ofrecer una respuesta ante incidentes
- La falta de personal en el equipo de seguridad de IT, y la falta de experiencia de alto nivel
- Demasiados eventos de seguridad que se deben procesar, analizar, controlar y corregir con eficacia dentro de un periodo de tiempo limitado
- Problemas de confianza y cumplimiento del uso compartido de datos a medida que la infraestructura digital amplía su alcance.
- Falta de visibilidad y desafíos relacionados con la recopilación de pruebas para el análisis posterior a la detección de brechas

Valor empresarial de la inversión en defensa y gestión de amenazas:

- Reducción de los daños financieros y operativos causados por el cibercrimen
- Reducción de la complejidad a través de una sencilla interfaz de gestión orientada a la empresa
- Reducción de los costes administrativos mediante la automatización de tareas y procesos de cumplimiento de seguridad simplificados
- Aumento del retorno de la inversión (ROI) gracias a la perfecta automatización del flujo de trabajo sin interrumpir los procesos empresariales
- Mitigación del riesgo de amenazas sofisticadas mediante la detección rápida

Transformación digital: un nuevo papel para la ciberseguridad

La transformación digital es un factor clave en el crecimiento corporativo, y proporciona a las organizaciones muchas nuevas oportunidades, Sin embargo, conlleva riesgos asociados con garantizar la seguridad de la infraestructura de IT, el cumplimiento y el uso seguro de los datos. Los ataques dirigidos y las amenazas complejas, incluidas las amenazas persistentes avanzadas (APT), ahora se encuentran entre los riesgos más peligrosos a los que se enfrentan las empresas. **Threat Management and Defense de Kaspersky**, una solución unificada para ayudar a acelerar la innovación en la transformación digital, se adapta a las características específicas de la organización y de sus procesos en curso a través de una combinación única de tecnologías de seguridad y servicios de ciberseguridad líderes en el sector. Esto le permite desarrollar una metodología unificada para completar la protección corporativa frente a las amenazas sofisticadas y los ataques dirigidos exclusivos.

Kaspersky Threat Management and Defense respalda el desarrollo o aumento de la estrategia de gestión de amenazas de la organización y permite la recopilación automatizada de información y pruebas digitales, simplifica la detección manual y automatiza los análisis de incidentes, todo ello respaldado por el aprendizaje automático. El conjunto de datos enriquecido permite la investigación de incidentes complejos y proporciona la experiencia y el respaldo necesarios para combatir incluso las amenazas más sofisticadas.

Kaspersky Threat Management and Defense ofrece una combinación exclusiva de los principales servicios y tecnologías que permiten implementar una estrategia de seguridad adaptable, lo que facilita la posibilidad de evitar la mayoría de los ataques, detectar rápidamente nuevas amenazas concretas, responder a incidentes inmediatos y predecir amenazas futuras. Kaspersky Threat Management and Defense incluye los siguientes componentes:

- **Kaspersky Anti Targeted Attack**, basado en inteligencia de seguridad líder del sector y tecnologías de aprendizaje automático avanzadas, todo ello combinado con la supervisión de redes y endpoints, tecnología de sandbox avanzada y análisis basado en inteligencia sobre amenazas. Kaspersky Anti Targeted Attack correlaciona eventos diferentes y prioriza los incidentes para ayudar a las organizaciones a detectar los ataques dirigidos, las amenazas sofisticadas y los sistemas ya vulnerados.

- **Kaspersky Endpoint Detection and Response** ayuda a obtener visibilidad de las amenazas de los endpoints mediante la adición y el almacenamiento centralizado automáticos de datos forenses. Kaspersky Endpoint Detection and Response utiliza la misma interfaz que Kaspersky Anti Targeted Attack y el mismo agente que Kaspersky Endpoint Security, lo que proporciona un enfoque multidisciplinar para revelar, reconocer y detectar ataques dirigidos complejos. Las empresas se centran en la detección de amenazas mediante el uso de tecnologías avanzadas, respondiendo de forma oportuna a los ataques y evitando acciones maliciosas al detectar amenazas en los endpoints.

- **Kaspersky Cybersecurity Services** ofrece asistencia rápida y profesional durante un incidente en curso y, posteriormente, ayuda a reducir el riesgo de los datos vulnerados y minimiza los posibles daños financieros y a la reputación. Nuestra cartera de servicios de ciberseguridad incluye un amplio programa de formación sobre seguridad, inteligencia sobre amenazas actualizada, una rápida respuesta ante incidentes, evaluaciones de seguridad proactiva, servicios de búsqueda de amenazas completamente externo y asistencia premium ininterrumpida.

En función de los requisitos del cliente para funciones de prevención avanzadas y de las exigencias de sus infraestructuras específicas, incluida la necesidad de un aislamiento completo de los datos corporativos, podemos enriquecer aún más nuestra solución Threat Management and Defense con los siguientes productos. Así podremos ofrecer un enfoque verdaderamente estratégico e integrado para la mitigación de riesgos y la prevención de amenazas y ataques dirigidos sofisticados:

- **Kaspersky Endpoint Security** es una plataforma de protección de endpoints a varios niveles impulsada por las tecnologías de ciberseguridad de próxima generación que están basadas en inteligencia de HuMachine que ofrece defensas flexibles y automatizadas contra las amenazas conocidas y desconocidas más sofisticadas, incluidos los ataques sin archivos y el ransomware. Para ofrecer esta protección, utiliza motores de aprendizaje automático, detección de comportamientos sospechosos, controles, protección de datos, y mucho más.

- **Kaspersky Secure Mail Gateway** funciona como parte de un enfoque preventivo de los ataques dirigidos. Proporciona prevención de amenazas de correo electrónico automatizada y ofrece una excelente protección para el tráfico que discurre a través de los servidores de correo electrónico contra spam, phishing y amenazas de malware genéricas y sofisticadas. Kaspersky Secure Mail Gateway funciona eficazmente incluso en las infraestructuras heterogéneas más complejas, independientemente del modelo de distribución del correo que se utilice: nube, local, cifrado.

- **Kaspersky Private Security Network** ofrece una completa base de datos de inteligencia sobre amenazas para redes y entornos aislados con estrictas restricciones para el uso compartido de datos, lo que permite a las empresas aprovechar la mayoría de los beneficios de la seguridad basada en la nube sin divulgar ningún dato fuera del perímetro controlado. Se trata de una versión personal, local y totalmente privada para la empresa de Kaspersky Security Network. Kaspersky Private Security Network se enfrenta a problemas de ciberseguridad críticos para la empresa sin que los datos abandonen la red local.

Kaspersky Anti Targeted Attack

Al correlacionar eventos de diferentes niveles, como la red, los endpoints y el panorama de amenazas global, Kaspersky Anti Targeted Attack ofrece detección de amenazas complejas prácticamente en tiempo real, así como la generación de datos forenses esenciales para potenciar el proceso de investigación.

Kaspersky Anti Targeted Attack proporciona a las organizaciones:

- Continuidad empresarial integral, que se consigue mediante la incorporación de la seguridad y el cumplimiento en los procesos nuevos justo desde las primeras fases.
- Visibilidad de sistemas de IT en segundo plano y amenazas ocultas
- Máxima flexibilidad, que permite la implementación en entornos físicos y virtuales, donde la visibilidad y el control son necesarios.
- Automatización de las tareas de investigación y respuesta, que optimiza la rentabilidad de la seguridad, la respuesta ante incidentes y los equipos de SOC.
- Integración directa y sencilla con los productos de seguridad existentes, para mejorar los niveles globales de seguridad y proteger las inversiones anteriores en este ámbito.

Kaspersky Endpoint Detection and Response

Los productos de seguridad de endpoints tradicionales (por ejemplo, Kaspersky Endpoint Security) desempeñan un papel esencial en la protección contra una amplia variedad de amenazas, entre las que se incluyen ransomware, malware, botnets, etc. Sin embargo, para protegerse contra una gama aún más amplia de ciberataques sofisticados y adversarios inteligentes, las empresas ahora necesitan aplicar niveles adicionales de protección en los endpoints, incluida la detección y la respuesta en estos.

Kaspersky Endpoint Detection and Response ayuda a las organizaciones a lo siguiente:

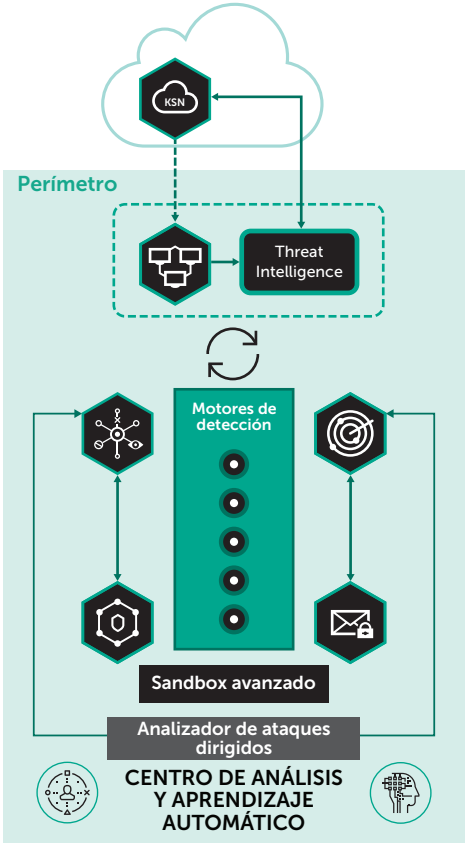
- Automatizar la identificación y respuesta ante amenazas sin interrumpir sus actividades
- Mejorar la visibilidad de endpoints y la detección de amenazas a través de tecnologías avanzadas, como aprendizaje automático, sandbox, análisis de indicadores de compromiso (IOC) e inteligencia sobre amenazas
- Mejorar la ciberseguridad con una solución empresarial fácil de usar para la respuesta ante incidentes
- Establecer procesos de búsqueda de amenazas, gestión de incidentes y respuesta unificados y eficaces.

Kaspersky Secure Mail Gateway

Kaspersky Secure Mail Gateway es una solución de prevención de amenazas de correo electrónico automatizada que ofrece tecnologías avanzadas para proteger el tráfico de correo de cualquier tipo como parte de un enfoque único para la detección y prevención de ataques dirigidos. Kaspersky Secure Mail Gateway ofrece innovadora protección antispam basada en la nube, antiphishing y antimalware a varios niveles avanzada con funciones de día cero y antiexploit. Esta protección está basada en la inteligencia sobre amenazas, el aprendizaje automático y sandbox avanzado para proporcionar un enfoque automatizado de varios niveles para la seguridad del correo electrónico.

Kaspersky Secure Mail Gateway proporciona a las organizaciones:

- Prevención automatizada de amenazas conocidas, desconocidas y futuras
- Análisis de archivos basado en firmas y con asistencia en la nube
- Análisis de archivos mediante el uso de métodos de aprendizaje automático
- Notificación rápida de incidentes
- Mejora perfecta de la ciberseguridad empresarial



Kaspersky Private Security Network

Kaspersky Private Security Network es una versión local y completamente privada de Kaspersky Security Network (KSN) que permite a las organizaciones que no desean divulgar ningún dato fuera de su perímetro controlado aprovechar la mayoría de los beneficios de la inteligencia sobre amenazas global basada en la nube.

Kaspersky Private Security Network como tecnología patentada:

- Proporciona acceso a estadísticas globales de archivos y URL.
- Clasifica los archivos y las URL con veredictos específicos que los marcan como objetos maliciosos o incluidos en listas blancas.
- Minimiza los daños provocados por incidentes de ciberseguridad mediante la concienciación en materia de amenazas en tiempo real.
- Permite la adición de veredictos exclusivos de la fuente de amenazas externa o específica del cliente (hash de archivos).
- Cumple los estrictos estándares normativos, de seguridad y privacidad.

Servicios de ciberseguridad

Inteligencia y experiencia, lo que proporciona un nuevo nivel de ciberinmunidad

Portal de inteligencia frente a amenazas

Al compartir nuestra inteligencia actualizada con los clientes, Kaspersky Lab ofrece a las empresas una visión global de los métodos, las tácticas y las herramientas que utilizan los actores de amenazas, ayudándoles así a protegerse contra las ciberamenazas modernas. Nuestra amplia gama de servicios de inteligencia sobre amenazas ayuda a garantizar que su centro de operaciones de seguridad (SOC) o equipo de seguridad de IT está totalmente equipado para combatir incluso los ataques más sofisticados.

- **Fuentes de datos de amenazas.** Mejore sus controles de seguridad (SIEM, IDS, firewalls, etc.) y las funciones de análisis forense con nuestros datos actualizados sobre ciberamenazas, que se comparten en una amplia variedad de formatos y métodos de entrega
- **Los informes de inteligencia de APT** ofrecen acceso exclusivo y proactivo a descripciones de campañas de ciberespionaje de alto nivel, así como a indicadores de compromiso (IOC) y reglas de YARA.
- **Los informes de inteligencia sobre amenazas financieras** se centran en las amenazas dirigidas específicamente a las instituciones financieras, incluidos los ataques dirigidos, los ataques a infraestructuras específicas (por ejemplo, cajeros automáticos/puntos de venta) y las herramientas desarrolladas o vendidas por los cibercriminales para atacar a los bancos, las empresas de procesamiento de pagos, los cajeros automáticos y los sistemas de puntos de venta.
- **Informes sobre amenazas personalizados.** Inteligencia sobre amenazas adaptada a su organización o país específicos derivada de fuentes abiertas y de propiedad, incluidas las de la red profunda y oscura.
- **Búsqueda de amenazas.** Un portal web que le proporciona acceso completo a todos los conocimientos adquiridos por nosotros en Kaspersky Lab sobre indicadores de amenazas y sus relaciones.
- **El sandbox basado en la nube** le permite enviar archivos sospechosos a Kaspersky Lab, obtener una descripción detallada del comportamiento del archivo con la ayuda de nuestra tecnología líder en el mundo y ejecutar investigaciones exhaustivas y detalladas basadas en una estrecha integración con Kaspersky Threat Lookup.
- **Seguimiento de phishing.** Notificaciones en tiempo real sobre los ataques de phishing en curso dirigidos a usted y sus clientes.
- **Seguimiento de botnets.** Notificaciones en tiempo real sobre los ataques botnet en curso que amenazan a sus clientes y su reputación.

Evaluación de la seguridad

Los servicios Kaspersky Security Assessment Services ofrecen análisis de seguridad de nivel experto e investigación de vanguardia, que se combinan para probar los sistemas de información de cualquier nivel de complejidad en entornos del mundo real.

Pruebas de penetración
Simulación de adversarios basada en inteligencia sobre amenazas que demuestra posibles vectores de ataque y proporciona una descripción general de su postura de seguridad corporativa desde el punto de vista de un atacante.

Evaluación de la seguridad de las aplicaciones
Una búsqueda exhaustiva de vulnerabilidades de lógica empresarial e implementación en aplicaciones de cualquier tipo, desde grandes soluciones basadas en la nube a aplicaciones integradas y móviles.

Evaluación de la seguridad de los sistemas de pago
Un análisis completo de los componentes de hardware y software de los sistemas de pago destinado a revelar estados de fraude y vulnerabilidades potenciales que pueden dar lugar a manipulaciones de las transacciones financieras.

Evaluación de la seguridad de ICS
Modelado de amenazas de casos específicos y evaluación de vulnerabilidades de los sistemas de control industrial y sus componentes que ofrece información sobre su superficie de ataque actual y el impacto empresarial potencial que tendría un ataque.

Evaluación de la seguridad de los sistemas de transporte
Investigación especializada centrada en la identificación de los problemas de seguridad relativos a los componentes primordiales de las infraestructuras de transporte modernas, desde el sector de automoción hasta el sector aeroespacial.

Evaluación de la seguridad de las tecnologías inteligentes y la seguridad del IoT
Una evaluación detallada de los dispositivos altamente interconectados de hoy en día y su infraestructura de back-end para revelar las vulnerabilidades en el firmware, la red y las aplicaciones.

Búsqueda de amenazas

Técnicas de búsqueda de amenazas proactivas realizadas por personal altamente cualificado y profesionales de seguridad con gran experiencia para ayudar a detectar amenazas sofisticadas ocultas en el ámbito de la organización.

- **Protección gestionada de Kaspersky**
  Supervisión constante y análisis continuo de los datos de las ciberamenazas por parte de los expertos de Kaspersky Lab.
- **Targeted Attack Discovery**
  Una oferta completa que permite la identificación proactiva de cualquier señal actual o anterior de vulnerabilidad y respuesta a los ataques que no se han detectado anteriormente.

Respuesta a incidentes

Incident Response Services de Kaspersky Lab los llevan a cabo analistas e investigadores de ciberintrusiones muy experimentados. Todo el peso de nuestra experiencia práctica mundial se aplica a la resolución del incidente de seguridad.

- **Respuesta ante incidentes.** Cobertura del ciclo completo de investigación de incidentes para eliminar totalmente la amenaza dirigida a su organización.
- **Ciencia forense digital.** Análisis de las pruebas digitales relacionadas con un cibercrimen que lleva a la creación de un informe completo que expone todos los hallazgos relevantes.
- **Análisis de malware.** Proporciona una imagen completa del comportamiento y la funcionalidad de los archivos de malware específicos.

Formación en seguridad

Ofrecemos una cartera de cursos que cubre todos los aspectos, desde técnicas fundamentales hasta sofisticadas, y las herramientas utilizadas para la ciencia forense digital, el análisis de malware y la respuesta ante incidentes, lo que permite a las empresas mejorar sus conocimientos sobre ciberseguridad en estas áreas.

- **Ciencia forense digital:** Los cursos se han diseñado para cubrir brechas de experiencia: desarrollo y mejora de habilidades prácticas en la búsqueda de pistas de cibercrimen y en el análisis de diferentes tipos de datos para restaurar los plazos y fuentes de ataque.
- **Análisis de malware e ingeniería inversa:** Los cursos ofrecen los conocimientos necesarios para analizar software malicioso, recopilar IOC (indicadores de compromiso), escribir firmas para la detección de malware en los equipos infectados, y restaurar archivos y documentos infectados o cifrados.
- **Respuesta ante incidentes:** Los cursos guiarán a su equipo interno a través de todas las fases del proceso de respuesta ante incidentes y les proporcionará los amplios conocimientos necesarios para llevar a cabo acciones correctivas adecuadas para incidentes.
- **Detección de amenazas eficaz con YARA:** Los participantes aprenderán a escribir las reglas YARA más eficaces, cómo probarlas y cómo mejorarlas hasta el punto de que encuentren amenazas que no se pueden detectar mediante otros métodos.

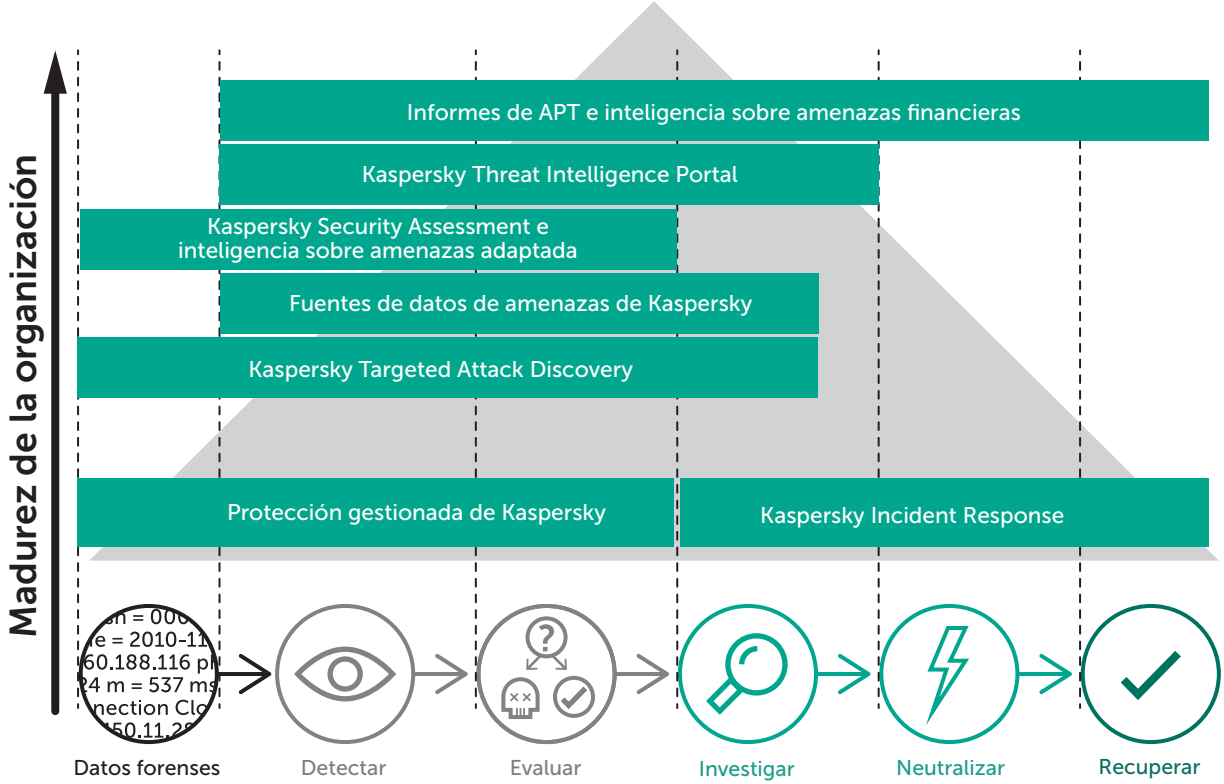
Kaspersky Cybersecurity Services

Kaspersky Security Training Programa

Ciencia forense digital avanzada y análisis avanzado de malware

Ciencia forense digital y análisis de malware

Concienciación sobre la ciberseguridad



Concienciación sobre la ciberseguridad

Creación de un ciberentorno corporativo seguro con formación lúdica

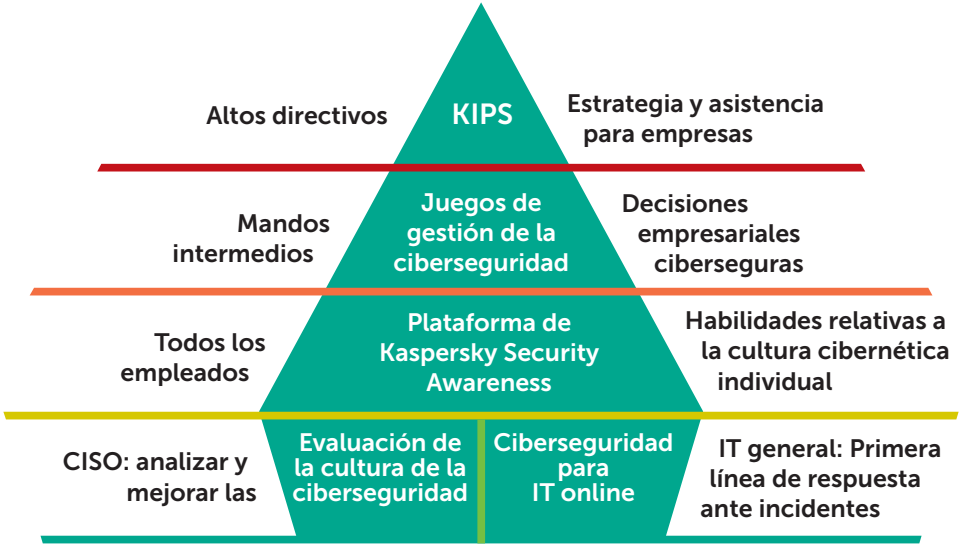
De media, las empresas deben pagar aproximadamente 1 155 000 USD para recuperarse de los ataques causados por empleados descuidados o desinformados, mientras que las pymes gastan 83 000 USD. Más del 80 % de los ciberincidentes se debe a errores humanos. Los ataques de phishing cuestan por sí solos hasta 400 $ por empleado al año.

Las empresas pierden millones para recuperarse de incidentes relacionados con el personal, pero la eficacia de los programas de formación tradicionales ideados para evitar estos problemas es limitada y, por lo general, dichos programas no logran suscitar el comportamiento ni la motivación deseados.

Kaspersky Lab ofrece una familia de productos de formación on line que aprovecha las técnicas modernas de aprendizaje y aborda todos los niveles de la estructura empresarial. Nuestro programa de formación ya ha demostrado su eficacia, tanto a los clientes como a los partners de Kaspersky Lab:

- Reducción de hasta el 90 % en el número de incidentes.
- Reducción del 50-60 % en las posibles pérdidas económicas asociadas a los ciberriesgos.
- Hasta un 93 % de probabilidad de que los conocimientos se usen en la vida diaria.
- El 86 % de los participantes recomendaría el curso a sus compañeros.

Productos de formación centrados en la concienciación sobre la seguridad de Kaspersky Lab



Enfoque premiado

- **Desarrollo del comportamiento, no solo conocimiento**: el enfoque del aprendizaje abarca la ludificación, el aprendizaje práctico, las dinámicas de grupo, los ataques simulados, los itinerarios de aprendizaje, el refuerzo automatizado de habilidades, etc. Esto se traduce en sólidos patrones de conducta y produce mejoras duraderas en la ciberseguridad.

- **Contenido práctico e importante** (basado en la potencia del I+D de Kaspersky Lab) proporcionado como una serie de ejercicios interactivos perfeccionados para satisfacer las necesidades empresariales y las preferencias de tiempo/formato de los diferentes niveles empresariales: altos directivos, superiores inmediatos o empleados medios.

- **Gestión sencilla de programas y medición en tiempo real**: el software de formación específicamente diseñado proporciona tareas de formación automatizadas, evaluaciones de las habilidades, refuerzo a través de reiterados ataques de phishing simulados e inscripción automática en módulos de formación. Los partners de Kaspersky Lab pueden gestionar y proporcionar los cursos, o incluso los propios equipos de formación y desarrollo del cliente (Kaspersky Lab ofrece programas de formación para formadores y asistencia).

Funcionamiento

- La formación abarca una amplia variedad de problemas relativos a la seguridad, desde filtraciones de datos y ransomware hasta ataques de malware en Internet, uso seguro de las redes sociales y seguridad móvil.

- La metodología de aprendizaje continuo impulsa un refuerzo constante de las habilidades y lleva la motivación hasta lo más profundo de la organización.

- Los cursos de formación que abordan diferentes niveles y funciones empresariales crean una cultura de la ciberseguridad colaborativa, compartida por todos y dirigida desde el nivel superior.

- La formación cuenta con herramientas de análisis e informes que miden las habilidades de los empleados y el progreso de su aprendizaje, así como la eficacia de los programas a nivel corporativo.

- Los planes formativos y las prácticas recomendadas por Kaspersky Lab facilitan la implementación de los programas y ayudan a los equipos de formación y desarrollo y de seguridad de IT del cliente a sacar el máximo partido de las iniciativas de concienciación sobre la seguridad.

Industrial Cybersecurity

Protección especializada para sistemas de control industrial

El aislamiento de los centros industriales con el mundo exterior solía ser suficiente para ofrecer un buen nivel de protección, sin embargo, esto ya no es así. En la era de la Industria 4.0, la mayoría de las redes industriales no esenciales están disponibles a través de Internet, sea o no por propia elección.

Los ataques maliciosos en entornos industriales han aumentado considerablemente en los últimos años. Los riesgos para la cadena de suministros y las interrupciones de las operaciones empresariales se sitúan como la principal preocupación empresarial del mundo en los últimos tres años; el riesgo de ciberincidentes es la principal preocupación emergente. En lo que respecta a las empresas con sistemas de infraestructuras industriales o vitales, los riesgos nunca han sido tan abundantes.

La seguridad industrial tiene consecuencias que van mucho más allá de la protección de las empresas y la reputación. En muchos casos, existen consideraciones ecológicas, sociales y macroeconómicas importantes que tener en cuenta a la hora de proteger los sistemas industriales de las ciberamenazas. Todas las infraestructuras vitales necesitan los niveles de protección más altos contra una variedad creciente de amenazas.

Al mismo tiempo, los entornos industriales necesitan una solución integrada que mantenga la disponibilidad de los procesos industriales detectando y evitando acciones (intencionales o accidentales) que puedan interrumpir o detener servicios vitales.

La solución: Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity es una cartera de tecnologías y servicios diseñada para proteger cada nivel industrial, lo que incluye servidores SCADA, HMI, estaciones de trabajo de ingeniería, PLC, conexiones de red y personas, sin afectar a la continuidad operativa ni a la coherencia de los procesos industriales. Sus ajustes flexibles y versátiles permiten que la solución pueda configurarse para satisfacer las necesidades y requisitos de cada una de las instalaciones industriales.

La solución se ha desarrollado para proteger las infraestructuras fundamentales y se ha integrado en diferentes sistemas de control industrial. La flexibilidad y el alcance de Kaspersky Industrial CyberSecurity permiten a las organizaciones configurar una solución en estricta conformidad con los requisitos del entorno de ICS específico. La configuración óptima de las tecnologías y los servicios de seguridad se establece mediante una auditoría completa de toda la infraestructura realizada por expertos de Kaspersky Lab.

El enfoque de Kaspersky Lab para proteger los sistemas industriales se basa en más de una década de experiencia descubriendo y analizando algunas de las amenazas industriales más sofisticadas del mundo. Nuestro profundo conocimiento y comprensión de la naturaleza de las vulnerabilidades de los sistemas, unidos a nuestra estrecha colaboración con las principales agencias gubernamentales, industriales y fuerzas de seguridad del mundo, como la Interpol, el Industrial Internet Consortium, además de varios organismos reguladores y proveedores de ICS, nos han permitido asumir un papel de liderazgo a la hora de abordar las necesidades únicas de la ciberseguridad industrial.

Esta solución altamente especializada:

- Proporciona un enfoque integral de la ciberseguridad para entornos industriales.
- Ofrece un ciclo completo de servicios de seguridad, desde la evaluación de la ciberseguridad hasta la respuesta ante incidentes.
- Suministra tecnologías de seguridad exclusiva desarrolladas específicamente para sistemas industriales.
- Minimiza el tiempo de inactividad y las demoras en el proceso industrial.

Kaspersky Industrial CyberSecurity

Tecnologías

Detección de anomalías (DPI)

Integración con otros sistemas

Antimalware

Control de integridad

Gestión centralizada

Investigación de incidentes

Sistema de detección de intrusiones

Servicios

Educación e inteligencia

- Formación sobre ciberseguridad
- Programas de concienciación
- Inteligencia sobre amenazas

Servicios expertos

- Evaluación de ciberseguridad
- Integración de soluciones
- Mantenimiento
- Respuesta ante incidentes

Fraud Prevention

La solución avanzada para una experiencia de usuario fluida y la prevención proactiva del fraude en tiempo real

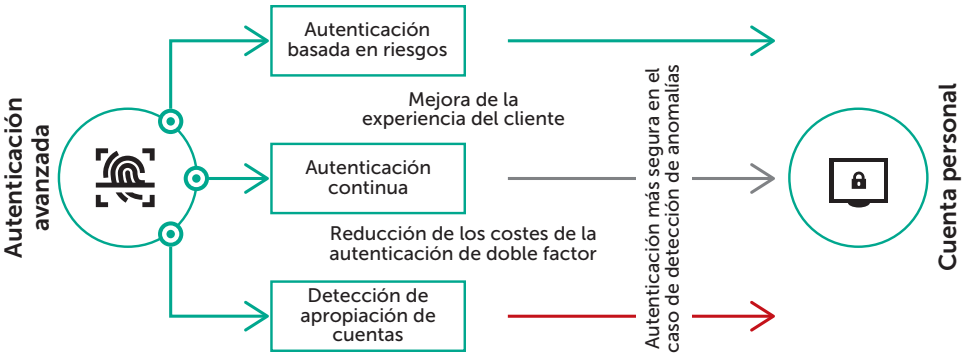
Pasarse a lo digital no es solo una tendencia: es una necesidad. Puesto que la mayoría de los clientes ya utilizan canales móviles y en línea para sus necesidades cotidianas, las empresas deben proporcionar servicios de alto nivel con una funcionalidad máxima. De forma simultánea, deben hacer malabares con la seguridad online para proporcionar una experiencia de cliente fluida. En este punto es donde Kaspersky Fraud Prevention entra en juego: permitiéndole aumentar y desarrollar sus canales móviles y en línea sin el estrés añadido de las cuestiones de seguridad y los problemas de usabilidad en línea.

La solución Kaspersky Fraud Prevention está basada en una compleja gama de tecnologías avanzadas, entre las que se incluyen el análisis de comportamientos, la biometría de comportamiento y el análisis del dispositivo y el entorno combinados en Kaspersky Fraud Prevention Cloud. El aprendizaje automático se aplica para la detección proactiva de esquemas de fraudes sofisticados en todos los canales web y móviles. Esto permite a sus sistemas de supervisión de fraudes actuales beneficiarse de contexto adicional para que la toma de decisiones se realice de forma más precisa y proactiva, así como para que se utilice una autenticación gradual de forma inteligente y adaptable.

La solución consta de dos productos completos que pueden utilizarse por separado para resolver problemas empresariales relevantes, o bien de forma conjunta para mejorar de forma significativa los niveles de seguridad y protección contra el fraude, además de mejorar la experiencia del usuario.

La **autenticación avanzada** se ha desarrollado para mejorar la experiencia del usuario, reducir los costes de la autenticación de doble factor y detectar continuamente actividades sospechosas, lo que conlleva el crecimiento empresarial y mayores niveles de seguridad.

Desde el momento del inicio de sesión, la autenticación avanzada analiza continuamente los eventos, permitiendo así el cálculo de los niveles de riesgo y la comunicación de recomendaciones apropiadas.



El **análisis de fraudes automatizado** utiliza una combinación perfectamente equilibrada de tecnologías de vanguardia con inteligencia global sobre amenazas y experiencia humana. Esta función ayuda a identificar y alertar a la organización de posibles actividades fraudulentas de antemano mediante el análisis de datos cruciales para permitir la toma de decisiones oportunas y precisas, y la detección de casos de fraude complicados.

Los eventos que suceden durante las sesiones de usuario que afectan a los usuarios, sus dispositivos y sus entornos alimentan los sistemas de gestión de fraudes con los datos necesarios para la toma de decisiones oportunas y precisas. Los incidentes listos para el uso generados en Kaspersky Fraud Prevention Cloud proporcionan información sobre casos de fraudes reales, por lo que estudian directamente la raíz del problema.

Junto con las tecnologías avanzadas y la experiencia, Kaspersky Fraud Prevention ofrece:

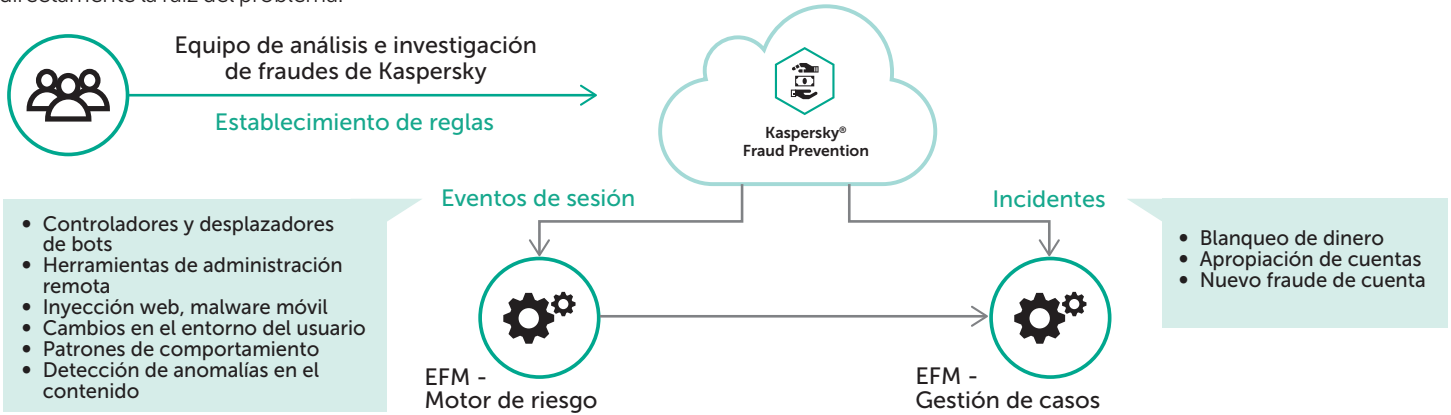
Acuerdo de servicio de mantenimiento: excelente asistencia para todas sus necesidades de seguridad al proteger su empresa con la asistencia de primera calidad de nuestros equipos locales de ingenieros certificados.

Servicios de implementación: los ingenieros de implementación especializada interconectan nuestra línea de productos con las soluciones de seguridad y prevención de fraudes existentes.

Consultoría sobre la prevención de fraudes: consultoría empresarial para ayudar a diseñar la estrategia de prevención de fraudes correcta por parte de un equipo de profesionales con una amplia gama de conjuntos de habilidades de expertos y experiencia multiindustrial.

Beneficios clave de Kaspersky Fraud Prevention:

- Crecimiento de canales online y móviles sin la tensión añadida de las preocupaciones sobre la seguridad y los problemas de facilidad de uso
- Control de los costes de prevención de fraudes y reducción de las pérdidas por fraudes
- Detección en tiempo real de fraudes sofisticados antes de que se haya producido cualquier transacción
- Enriquecimiento de las soluciones de supervisión de fraudes empresariales con datos adicionales



Seguridad del IoT

Justificación de la confianza de sus clientes mediante la protección de su privacidad

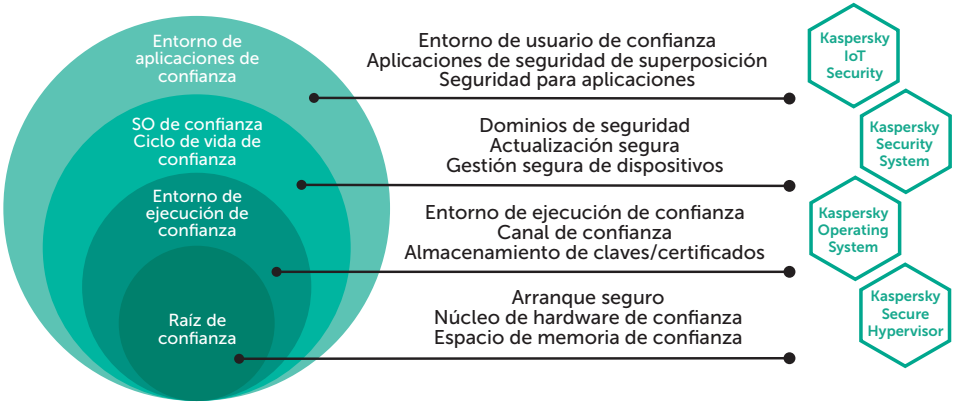
El Internet de las cosas (IoT) es un nuevo paradigma que está cambiando el mundo. Puede hacer que nuestro mundo sea más seguro, mejorar nuestra salud, ahorrarnos tiempo y dinero, reducir el despilfarro y agregar una nueva dimensión al control de la producción y a la vida en general.

La ciberseguridad se ha asociado tradicionalmente con la seguridad de los datos personales. En la era del IoT, sin embargo, esto se ha transformado en la seguridad de la privacidad. Las infracciones relacionadas con la privacidad del usuario, tales como la vigilancia remota a través de cámaras domésticas inteligentes, dispositivos multimedia o dispositivos de vigilancia de bebés, interferencias en el funcionamiento de aparatos domésticos, apagados inesperados y errores en los servicios cotidianos... Todo esto es inaceptable para el usuario final.

Al mismo tiempo, el Internet de las cosas ofrece oportunidades excepcionales para los fabricantes de dispositivos (incluidos los de componentes de hardware y software), los proveedores de servicios de telecomunicaciones y el mercado de integración de sistemas. Una falta de confianza en las soluciones del IoT entre los usuarios finales podría bloquear o ralentizar considerablemente la posibilidad de hacer realidad estas posibilidades. Por eso, la seguridad integral de las soluciones de IoT es una prioridad absoluta para todas las partes involucradas.

Tal como están las cosas, los dispositivos de perímetro de IoT y los equipos de telecomunicaciones proporcionados a los clientes pueden incorporar fácilmente infracciones de ciberseguridad. Puede que el hardware no consiga controlar correctamente la integridad del firmware, y los dispositivos a veces se envían con contraseñas preinstaladas, incluidas las contraseñas de administrador. Una configuración de seguridad de red débil o el uso de software vulnerable y antiguo también pueden ser sinónimos de problemas. Junto con la falta de procesos de actualización de software, lo que se traduce en que los dispositivos vulnerables pueden funcionar durante años sin actualizaciones, está claro que solo es cuestión de tiempo que el dispositivo sea atacado con éxito.

Garantías de confianza a nivel de dispositivo



El principio de una cadena de confianza constituye la base para garantizar el funcionamiento seguro de un dispositivo de IoT, incluidos los dispositivos de perímetro y los elementos de la infraestructura (pasarelas). Este principio comienza con el uso de una raíz de confianza en el nivel de hardware.

Esta tecnología realiza un arranque de confianza de un sistema operativo, incluida la integridad de la comprobación de imagen del sistema operativo, y la aplicación de criptografía y mecanismos de almacenamiento seguro asistido por hardware para información clave. El arranque de confianza es crucial para dispositivos de infraestructura de IoT esenciales como las pasarelas, porque garantiza que el sistema operativo arranca a partir de dispositivos predefinidos y solo después de que el equipo haya superado correctamente determinados controles de integridad.

El siguiente elemento importante en la cadena de confianza es un sistema operativo seguro que pueda garantizar la ejecución correcta del software que no se considera de confianza. Los desarrollos recientes en la tecnología informática hacen posible la implementación de un entorno a nivel de sistema operativo que restringe el comportamiento de las aplicaciones que no se consideran de confianza.

El concepto de IoT engloba una enorme variedad de aparatos, dispositivos, tecnologías, software y protocolos de comunicación. Pero este entorno heterogéneo genera muchos riesgos de seguridad que podrían obstaculizar seriamente cualquier aspecto de nuestras vidas, en las que siempre estamos conectados al IoT. Kaspersky Lab ha diseñado una serie de productos que ayudan a minimizar los riesgos asociados:

- **Embedded Systems Security**
  Refuerce y proteja sus dispositivos y ordenadores integrados basados en Microsoft Windows con una solución creada para optimizar la seguridad de los sistemas de gama baja con capacidad de memoria limitada; no requiere mantenimiento continuo ni conexión a Internet.

- **KasperskyOS**
  El sistema operativo de KasperskyOS está diseñado para proteger diversos y complejos sistemas integrados de las consecuencias de los ataques de código malicioso, virus y hackers a través de una separación sólida y la aplicación de políticas. KasperskyOS crea un entorno donde una vulnerabilidad o un código malicioso ya no es un gran problema. El componente de protección Kaspersky Security System controla las interacciones a través de todo el sistema y consigue inutilizar la explotación de vulnerabilidades.

- **Kaspersky Security System**
  Se trata de un motor de cálculo de veredictos de políticas de seguridad que puede trabajar simultáneamente con diferentes tipos de políticas de seguridad (control de acceso basado en funciones y obligatorio, lógica temporal, flujo de control, aplicación de tipo, etc.), y se puede personalizar para satisfacer las necesidades del cliente. Cuanto más precisas sean las políticas, más control y seguridad se proporcionarán a todo el sistema.

  Kaspersky Security System se puede utilizar junto con KasperskyOS (la configuración más segura), así como en una solución basada en Linux (acciones seguras en un sistema no seguro).

- **Kaspersky Secure Hypervisor**
  Kaspersky Secure Hypervisor (KSH) se ejecuta en el micronúcleo de KasperskyOS. Con KSH, los sistemas operativos invitados virtualizados potencialmente no seguros pueden separarse unos de otros, y todas las comunicaciones entre ellos se pueden controlar y ser fiables, incluso aunque se estén ejecutando físicamente en la misma plataforma de hardware. Un beneficio adicional de KSH es su capacidad para reducir los costes de mantenimiento de hardware.

- **Kaspersky Transportation Security Service**
  "Protección para seguridad" basada en la tecnología KasperskyOS incorporada: una sola pasarela segura en unidades de control electrónico (ECU), y una amplia gama de servicios de evaluación de la seguridad que satisfacen las necesidades de los vehículos conectados actuales y futuros.

- **Unidad de comunicación segura de**
  Secure Communication Unit (SCU) es una unidad de control de pasarela de comunicación conectada a varias subredes o controladores de pasarelas en las subredes dentro de la red del coche. De esta forma, la SCU es una pasarela única para las comunicaciones externas, mientras que los dispositivos internos puedan comunicarse dentro de un dominio o incluso entre dominios sin utilizar los servicios de la SCU.
  La SCU está basada en KasperskyOS y reforzada por Kaspersky Security System. KasperskyOS controla todas las interacciones dentro de la SCU en el nivel más bajo, y aplica los veredictos de la política de Kaspersky Security System. Solo las interacciones explícitamente permitidas son posibles.

Embedded Systems Security

Seguridad todo en uno diseñada específicamente para los sistemas integrados

Dado que operan con dinero real y credenciales de tarjetas de créditos, los sistemas integrados son el blanco favorito de los cibercriminales, por lo que requieren los niveles más elevados de protección inteligente especializada. Este es el momento de aplicar tecnologías de eficacia probada, como el control de dispositivos y la denegación predeterminada, como primera línea de defensa.

En la actualidad, podemos encontrar sistemas integrados en un gran número de objetos: máquinas de venta de tickets, cajeros automáticos, quioscos, sistemas de punto de venta o equipos médicos entre otros; la lista es interminable.

Los sistemas integrados constituyen un motivo de preocupación especial en materia de seguridad, ya que tienden a la dispersión desde el punto de vista geográfico, resultan difíciles de gestionar y rara vez se actualizan. No obstante, los sistemas que trabajan con dinero en efectivo y las credenciales de los clientes deben ser resistentes y contar con un diseño a prueba de errores. Los dispositivos integrados no solo tienen que estar protegidos frente a las amenazas directas, sino que además deben impedir que los cibercriminales o atacantes internos puedan acceder a ellos, ya que de lo contrario pueden convertirse en un punto de acceso a toda la red corporativa.

Generalmente, las normativas de seguridad estándar para dispositivos integrados solo cubren la protección basada en antivirus o en métodos de refuerzo del sistema, lo cual no es suficiente. Los enfoques basados íntegramente en antivirus tienen una eficacia limitada frente a las amenazas que afectan actualmente a los sistemas integrados, algo que han demostrado con creces los ataques más recientes.

La denegación predeterminada para aplicaciones, controladores y bibliotecas, respaldada por la función de control de dispositivos, es el único método que puede garantizar la seguridad de los sistemas críticos obsoletos todavía en uso.

La solución: Kaspersky Embedded Systems Security

Kaspersky Lab ha creado una solución de seguridad específica para empresas que utilizan sistemas integrados, que refleja su funcionalidad y sus requisitos de hardware, canal y SO exclusivos, a la vez que se centra en el panorama específico de amenazas al que se enfrentan estos sistemas. Además, es compatible con la familia de Windows XP.

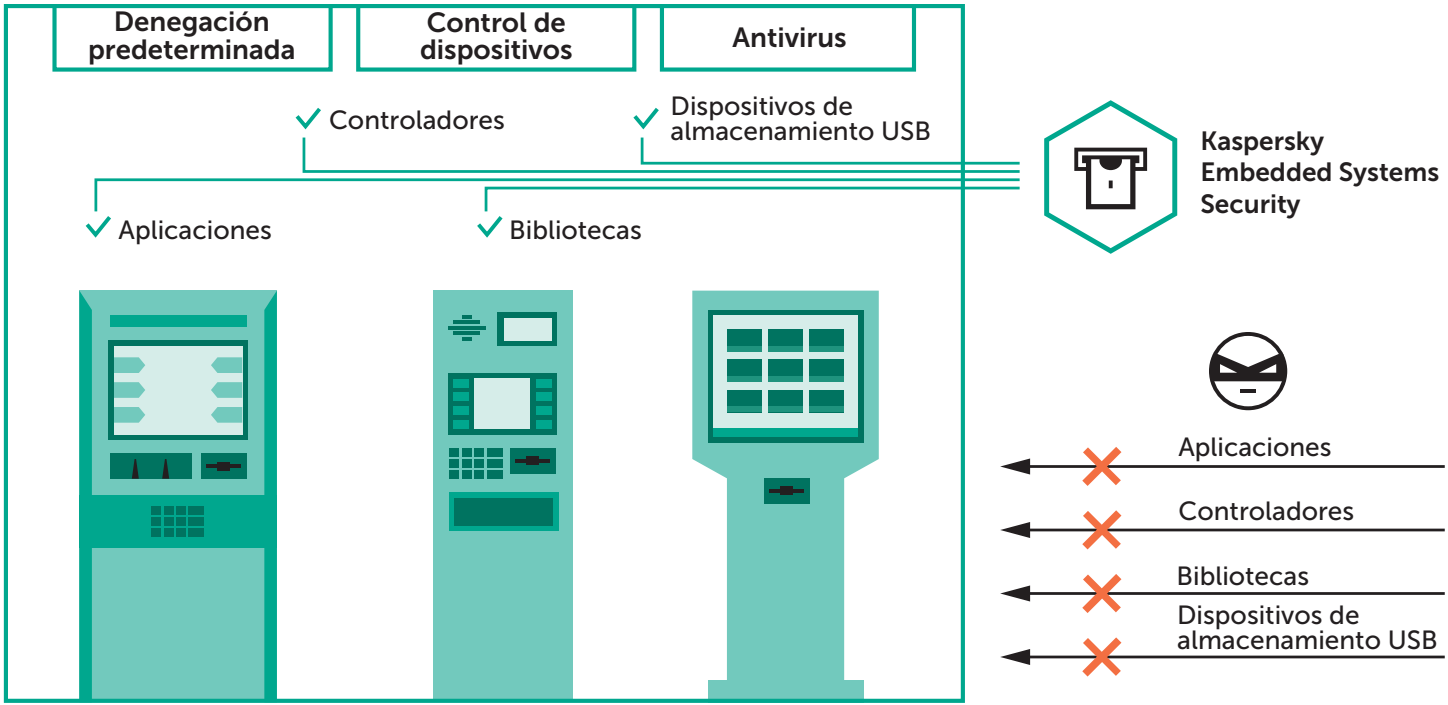
Kaspersky Embedded Systems Security ofrece el modo operativo "Solo denegación predeterminada", en el que los requisitos del sistema van desde 256 MB de RAM y 50 MB de espacio en el disco duro para Windows XP para sistemas de hardware de gama baja.

También existe un modo de análisis a petición suministrado por un módulo antivirus opcional, que incluye la gestión del firewall. Este módulo está respaldado por Kaspersky Security Network, con servicios de gestión de parches si es necesario.

Por lo tanto, esta solución única cumple tres objetivos clave:

- Seguridad efectiva para sistemas "difíciles de gestionar"
- Cumplimiento de los requisitos 5.1, 5.1.1, 5.2, 5.3 y 6.2 de la PCI DSS
- Planificación flexible para sistemas obsoletos y sustitución de hardware

La solución se ha diseñado específicamente para mitigar los riesgos asociados a la ciberseguridad de los sistemas basados en sistemas operativos integrados, y protege las superficies de ataque exclusivas de estas arquitecturas a la vez que respeta las consideraciones de eficacia y de hardware relacionadas. Una única consola intuitiva le ofrece el control y la visibilidad que necesita para gestionar eficazmente la seguridad multicapa de los endpoints, los sistemas críticos y toda la infraestructura de IT.



Asistencia premium y servicios profesionales

Una variedad de servicios para garantizar que las empresas sacan el máximo partido de los productos de Kaspersky Lab

Asistencia Premium

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 cientos de miles de dólares. Nuestros planes de asistencia premium se centran en lograr precisamente 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.

Kaspersky Lab ofrece una selección de programas de asistencia premium que tratan sus problemas de seguridad de IT como de alta prioridad en todo momento. Ayuda a mantener su negocio en marcha sin problemas, y centra toda la fuerza de la experiencia directamente en encontrar la vía más rápida y más efectiva de volver a un rendimiento pleno de forma segura.

Nuestros planes de asistencia premium incluyen:

- Responsable técnico de cuenta dedicado
- Asistencia interrumpida a través de una línea telefónica especializada
- SLA de respuesta ante incidentes
- Alertas proactivas sobre nuevas amenazas

Servicios profesionales

La ciberseguridad supone una gran inversión. Obtenga el mayor provecho posible mediante la colaboración con expertos que saben exactamente cómo puede optimizar su inversión a fin de satisfacer los requisitos únicos de la empresa.

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 Lab en su infraestructura de IT empresarial.

Los servicios Kaspersky Lab Professional Services garantizan que su respuesta al cambio y la transición sea óptima y eficaz, y no cause interrupciones indebidas en las operaciones empresariales.

Kaspersky Professional Services comprende:

- Implementación y actualización
- La configuración
- La comprobación de mantenimiento
- Formación sobre productos

Acerca de Kaspersky Lab

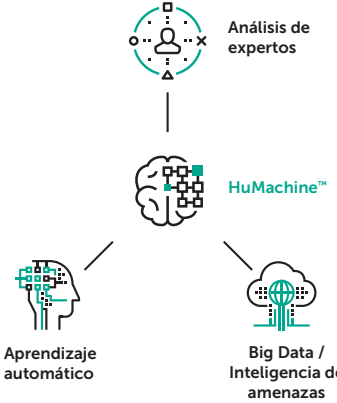
Kaspersky Lab es la mayor empresa privada de ciberseguridad del mundo y una de las de mayor crecimiento.

Nuestra independencia nos permite ser más ágiles para pensar de forma diferente y actuar con mayor rapidez. Siempre estamos innovando, ofreciendo protección eficaz, aprovechable y accesible. Nos sentimos orgullosos de ser los responsables del desarrollo de las tecnologías de seguridad líderes del mercado. Unas tecnologías que nos mantienen (a nosotros y a nuestros 400 millones de usuarios y 270 000 clientes corporativos) un paso por delante de las amenazas potenciales.

Nuestro compromiso con las personas y con la tecnología avanzada también nos mantiene por delante de la competencia.

Visite kaspersky.com/enterprise para obtener más información sobre la experiencia exclusiva de Kaspersky Lab y Security Solutions for Enterprise.

Notas



Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Noticias de ciberamenazas: **https://securelist.es**
Noticias de seguridad de IT: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.es