KASPERSKY lab

Kaspersky Enterprise Cybersecurity
#TrueCybersecurity

Kaspersky Security Solutions for Enterprise

2017

Proteción de la empresa

Las amenazas cibernéticas son cada vez más sofisticadas. Sin soluciones eficaces para mitigarlas, las empresas se exponen a ciberataques que mermarán sus recursos financieros, interrumpirán la continuidad del negocio, dejarán al descubierto datos confidenciales y causarán daños a su reputación. Que un ataque tenga éxito resulta sumamente perjudicial para la empresa, con independencia del sector en el que opere.

LA SEGURIDAD DE LA EMPRESA ES ALGO SERIO

Los costes de una brecha de seguridad son importantes: en la encuesta de Kaspersky Lab sobre riesgos de seguridad de IT globales de 2015, hallamos que el coste medio directo de recuperación de las empresas ascendía a 551 000 $, con unos costes indirectos medios de 69 000 $. Para evitar estos costes y los trastornos que se derivan de ellos, las empresas deben reforzar tanto el tipo como el nivel de protección en su infraestructura de TI.

A partir de una inteligencia de seguridad que es el fundamento de todos nuestros productos y servicios, las soluciones de Kaspersky Lab brindan funciones de predicción, prevención, detección y respuesta a través de diferentes segmentos de la infraestructura empresarial y de tecnologías emergentes: endpoints, tecnologías online y móviles, infraestructuras virtuales, centros de datos, sistemas de control industrial, etc.

Kaspersky Lab es una empresa pionera en ayudar a las empresas a actualizar sus estrategias de seguridad para defenderse mejor de las últimas amenazas avanzadas y los ataques dirigidos. Ofrecemos una combinación única de tecnologías y servicios, respaldada por una inteligencia de seguridad líder en todo el mundo, para ayudar a las empresas a detectar ataques dirigidos y mitigar riesgos en una etapa inicial, antes de que los daños sean graves.

Al abordar todas las posibles etapas de los incidentes de IT, las soluciones de Kaspersky Lab ofrecen un enfoque integral, flexible y estratégico de la seguridad empresarial. Nuestra filosofía es sencilla: una inteligencia superior combinada con las tecnologías más vanguardistas ofrece la mejor protección.

Anti Targeted Attack

Solución especializada centrada en la inteligencia contra ataques dirigidos

Los ataques dirigidos son procesos a largo plazo que ponen en riesgo la seguridad y dan al atacante el control de la infraestructura de IT de la víctima. Además, evitan la detección mediante tecnologías de seguridad tradicionales.

Aunque algunos atacantes utilizan amenazas persistentes avanzadas (APT), que pueden ser muy eficaces pero cuya implementación resulta cara, otros ataques dirigidos pueden organizarse de forma más económica y tienen la misma capacidad de destrucción. Es posible que estos ataques dirigidos llevados a cabo mediante técnicas básicas (ingeniería social, robo de credenciales de empleados, software legítimo o incluso malware oculto por un certificado robado) no ocupen los titulares, pero están en todas partes.

La mayoría de las empresas ha realizado ya grandes inversiones en soluciones de seguridad de IT tradicionales, principalmente en el nivel de la pasarela. Sin embargo, aunque estas tecnologías de seguridad preventivas pueden ser muy eficaces en la protección contra amenazas comunes, como el malware, la filtración de datos, los ataques a la red, etc., es evidente que no son suficientes: el número total de incidentes y brechas de seguridad empresarial no ha disminuido ni un ápice.

Hoy en día, incluso con tecnologías innovadoras como sandbox, EDR y otras soluciones modernas, el desafío sigue siendo el mismo: cómo elegir el incidente adecuado y qué incidente está relacionado con las amenazas más críticas. Las soluciones de detección especializadas desempeñan un papel fundamental en la identificación de los incidentes que más justifican una investigación y una respuesta mayor.

Las amenazas avanzadas y dirigidas pueden pasar inadvertidas durante 200 días o más, mientras los cibercriminales recopilan información valiosa sigilosamente o producen un impacto en los procesos empresariales vitales.

Según las estadísticas de Kaspersky Lab, incluso un solo ataque dirigido puede costar a una empresa más de 2,5 millones de $ en comparación con un punto de partida de 80 000 $ para la pequeña y mediana empresa típica.

Si un ataque dirigido no se comprueba, puede causar graves daños en la empresa con una alta probabilidad, incluidos los siguientes:

- Pérdidas económicas significativas
- Pérdida de datos esenciales
- Control remoto por parte del atacante de procesos empresariales aparentemente "autorizados"
- Manipulación oculta de datos

En una encuesta realizada a empresas grandes por Kaspersky Lab en 2015, 1 de cada 4 organizaciones (23 %) confirmó que ya habría sufrido al menos un ataque dirigido.

LA SOLUCIÓN: KASPERSKY ANTI TARGETED ATTACK PLATFORM

Kaspersky Anti Targeted Attack Platform forma parte de un enfoque integrado y flexible de la seguridad empresarial. La supervisión del tráfico de red, combinada con la tecnología sandbox de objetos y el análisis de comportamiento del endpoint, ofrece una visión detallada de lo que sucede exactamente en toda la infraestructura de IT de una empresa. El enfoque de seguridad adaptable protege a las empresas contra las amenazas más sofisticadas, los ataques dirigidos, el nuevo malware (como el ransomware y el crimeware) y, por supuesto, las APT.

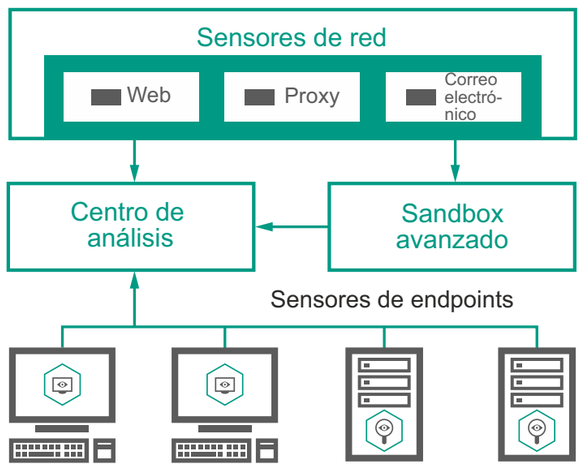
Al correlacionar eventos de diferentes niveles, como la red, los endpoints y el panorama de amenazas global, Kaspersky Anti Targeted Attack Platform ofrece detección de amenazas complejas prácticamente en tiempo real, así como la generación de datos forenses esenciales para potenciar el proceso de investigación.

Nuestra inteligencia de seguridad global líder del sector es una de las razones por las que podemos ofrecer este rendimiento superior en la detección. Ningún otro proveedor de seguridad puede igualar la calidad y la amplitud de nuestra inteligencia de seguridad, que nos permite proteger a las empresas de una creciente variedad de amenazas.

Sin embargo, la inteligencia de seguridad global es solo el inicio; Kaspersky Anti Targeted Attack Platform también incorpora potentes tecnologías de detección y análisis, como:

- Arquitectura multicapa de sensores: para aportar una visibilidad total. Gracias a una combinación de sensores de red, sensores de Web y correo electrónico y sensores de endpoints, Kaspersky Anti Targeted Attack Platform brinda funciones de detección avanzadas en todos los niveles de la infraestructura de IT corporativa.
- Sandbox avanzado: para evaluar nuevas amenazas. Nuestro sandbox avanzado es el resultado de más de 10 años de desarrollo continuo y ofrece un entorno virtualizado aislado para que los objetos sospechosos puedan ejecutarse de forma segura y sea posible observar su comportamiento.
- Potentes motores de análisis: para veredictos rápidos y menos falsos positivos. Nuestro analizador de ataques dirigidos evalúa los datos de los sensores de red y endpoints, y genera rápidamente veredictos de detección de amenazas para su equipo de seguridad.

Kaspersky Anti Targeted Attack Platform



Kaspersky Private Security Network

Todos los beneficios de la inteligencia de amenazas basada en la nube dentro de su perímetro

Las soluciones de seguridad estándar tardan hasta cuatro horas en recibir la información necesaria para identificar y bloquear los casi 310 000 programas maliciosos nuevos que detecta Kaspersky Lab cada día. El intercambio de inteligencia de amenazas a través de Kaspersky Private Security Network proporciona esta información en 30-40 segundos.

El cibercrimen está creciendo no solo en volumen sino también en sofisticación; aunque el 70 % de las amenazas a las que se enfrentan las empresas cada día son conocidas, el 30 % engloba amenazas desconocidas y avanzadas que la seguridad tradicional basada en firmas no puede combatir por sí sola.

Kaspersky Security Network proporciona la inteligencia de seguridad de Kaspersky Lab a cada sistema conectado a Internet, lo que garantiza los tiempos de reacción más rápidos y las tasas de falsos positivos más bajas, y mantiene el máximo nivel de protección, incluso contra amenazas desconocidas y avanzadas.

Aunque toda la información procesada por Kaspersky Security Network es totalmente anónima y está desvinculada de su origen, sabemos que algunas empresas requieren un bloqueo de datos completo. Tradicionalmente, este hecho significaba que dichas empresas no podían beneficiarse de las soluciones de seguridad basadas en la nube.

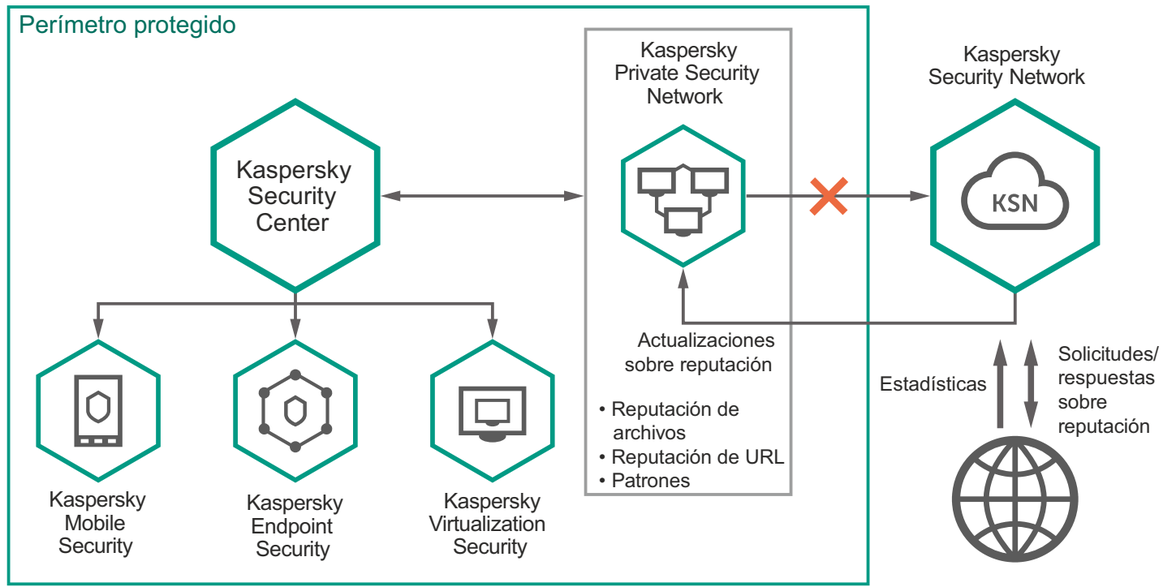
LA SOLUCIÓN: KASPERSKY PRIVATE SECURITY NETWORK

Para los clientes con estas necesidades tan especializadas, Kaspersky Lab ha desarrollado Kaspersky Private Security Network, que permite a las empresas aprovechar la mayoría de las ventajas que ofrece la seguridad con asistencia en la nube sin que dato alguno abandone su 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 Private Security Network:

- 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).
- Reduce el número de falsos positivos.
- Cumple los estrictos estándares normativos, de seguridad y privacidad.

Kaspersky Private Security Network aplica nuestra exclusiva inteligencia de amenazas y la información no solo a las soluciones de seguridad de Kaspersky Lab, sino a otras soluciones que la empresa pueda estar utilizando, entre las que se incluyen SIEM, gestión de riesgos y cumplimiento normativo. Todas estas funciones pueden integrarse mediante SDK, las llamadas directas y la API de Kaspersky Private Security Network, lo que ofrece una visión única de la seguridad de su empresa y de su nivel de preparación para enfrentarse a las amenazas.



Endpoint Security

Protección multicapa de próxima generación contra las últimas amenazas avanzadas y sofisticadas dirigidas a sus endpoints

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.

Con el crecimiento de la empresa digital, los entornos de IT empresariales son cada vez más complejos. Mientras tanto, los cibercriminales adoptan métodos de ataque de mayor sofisticación, lo que genera nuevas formas de infiltrarse en la infraestructura empresarial.

La mayoría de los ataques cibernéticos a las empresas se inician a través del endpoint. Sin un aprendizaje mecánico y una inteligencia de amenazas global eficaces, las tecnologías de seguridad tradicionales no ofrecen protección contra las amenazas altamente sofisticadas.

Ofrecemos una protección inmediata contra las amenazas desconocidas y sofisticadas, así como frente a los ataques dirigidos, a través de nuestras tecnologías de detección avanzadas, que se basan en una combinación de inteligencia de amenazas y aprendizaje mecánico.

La protección contra amenazas avanzadas se mejora aún más gracias a las potentes herramientas de protección de datos y control, como el cifrado integrado, la aplicación automática de parches y la protección de endpoints móviles, todo ello gestionado a través de Kaspersky Security Center.

Todos los componentes se desarrollan internamente y constituyen una plataforma común que puede adaptarse fácilmente a las necesidades cambiantes de la empresa.

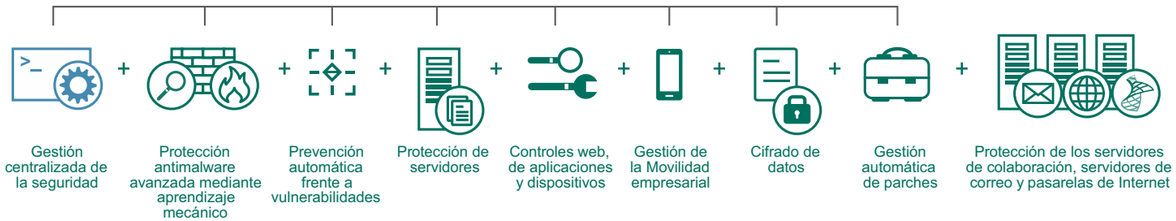
LA SOLUCIÓN: KASPERSKY ENDPOINT SECURITY

Es esencial proteger los endpoints contra todo tipo de ciberamenazas avanzadas. La protección antivirus tradicional no es en absoluto suficiente. Solo mediante el uso de una plataforma de seguridad de vanguardia, incluido el aprendizaje mecánico para la detección dinámica y estática, así como de la adopción de un enfoque multicapa es posible proteger completamente cada endpoint dentro y fuera del perímetro.

Basadas en fuentes inigualables de inteligencia de amenazas en tiempo real, nuestras tecnologías evolucionan constantemente para proteger a su empresa incluso frente a las amenazas más sofisticadas y recientes, incluidos los exploits de día cero. Mediante la alineación de su estrategia de seguridad con los líderes mundiales en detección de amenazas avanzadas, adoptará la mejor protección de endpoints, ahora y en el futuro.

No hay mejor postura de seguridad para su empresa.

Kaspersky Endpoint Security



Protección demostrada sin precedentes para todos los tipos de endpoint
Nuestras tecnologías de protección avanzadas protegen a empresas grandes y sus infraestructuras de IT, con independencia de la complejidad, incluidos todos los endpoints, desde servidores y escritorios físicos y virtuales hasta dispositivos móviles.

Análisis de comportamiento mediante aprendizaje mecánico para proteger su empresa
Nuestra solución utiliza el aprendizaje mecánico basado en las tecnologías de datos estáticos y dinámicos. Así es como le protegemos frente a futuras amenazas.

Potente inteligencia de amenazas global
Todas nuestras tecnologías están basadas en nuestra inteligencia de amenazas global demostrada. Hemos detectado más ATP que ningún otro proveedor de seguridad, por lo que disponemos de una comprensión inigualable de la naturaleza de las amenazas modernas y podemos ayudarle a protegerse mejor frente a ellas.

Respuesta automática en tiempo real
En el momento en el que se detecta una amenaza, el sistema revierte automáticamente cualquier cambio que el malware haya iniciado, según lo detectado por nuestro motor de control del comportamiento dinámico.

Protección dinámica continua contra amenazas y exploits de día cero
La protección automática frente a vulnerabilidades se ha desarrollado para evitar que los cibercriminales ataquen las vulnerabilidades de las aplicaciones en máquinas protegidas. La gestión automática de parches añade un nivel adicional de seguridad.

Protección de datos con certificación FIPS 140-2
El potente cifrado transparente para los usuarios protege totalmente los datos delicados y confidenciales en movilidad, en dispositivos portátiles y en reposo.

Protección fiable frente al ransomware
Proteja sus datos, evite la financiación de los cibercriminales a través de pagos de rescates y proteja sus carpetas compartidas contra bloqueadores de cifrado avanzados con nuestras tecnologías antiransomware.

Coste total de propiedad (TCO) inferior y retorno de la inversión (ROI) superior mediante una gestión centralizada y unificada
Gestione varias plataformas y todos los endpoints desde la misma consola, aumentando así la visibilidad y el control sin necesidad de realizar inversiones adicionales en software, equipos ni recursos humanos.

Embedded Systems Security

Protección eficaz específicamente diseñada para 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.

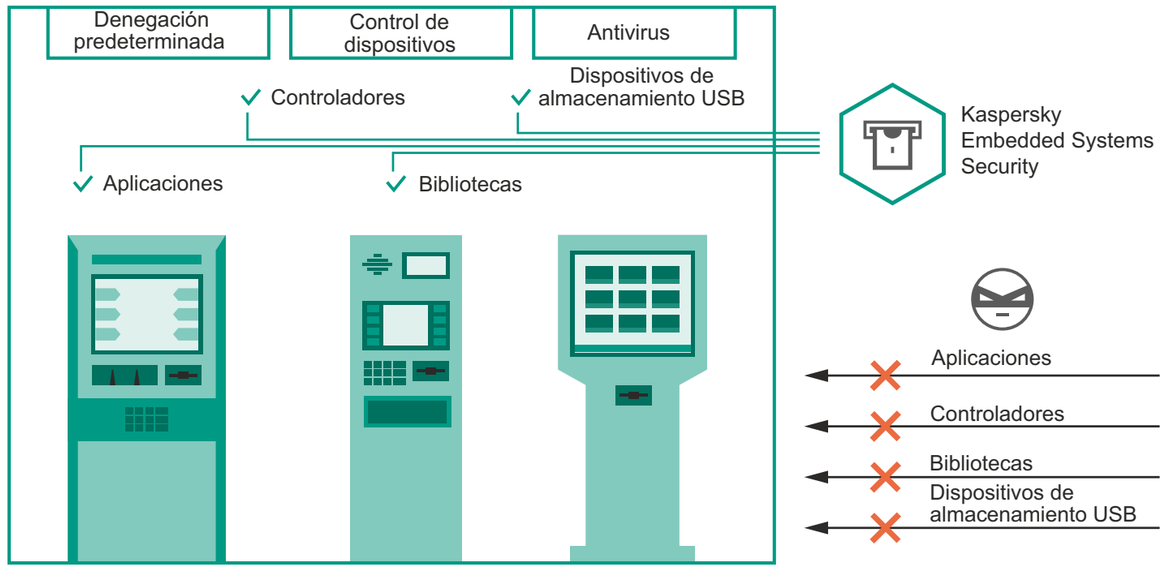
Kaspersky Embedded Systems Security ofrece el modo operativo "Solo denegación predeterminada", en el que los requisitos del sistema van desde 256 MB de RAM y 50 MB de espacio en el disco duro para Windows XP para sistemas de hardware de gama baja.

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.



Security Intelligence Services

Líder en inteligencia de amenazas, servicios expertos y formación en seguridad

El 60 % de las grandes empresas piensan utilizar los servicios de inteligencia de amenazas en su estrategia de seguridad.

Constantemente surgen amenazas sofisticadas y los cibercriminales están desarrollando técnicas innovadoras para superar las tecnologías de seguridad establecidas. Las soluciones de seguridad tradicionales, como los antivirus, los firewalls y los sistemas de prevención de intrusiones ya no son suficientes por sí solos para lograr una protección integral: hoy en día, es necesario un nuevo enfoque de la seguridad basado en la inteligencia de amenazas y una amplia experiencia para cubrir esta brecha de seguridad.

Al compartir nuestra inteligencia más actualizada con nuestros clientes, Kaspersky Lab ayuda a las empresas a protegerse contra las amenazas. Nuestra amplia gama de servicios de inteligencia ayuda a garantizar que su centro de operaciones de seguridad (SOC) o su equipo de seguridad de IT está equipado para proteger a la empresa frente a las últimas amenazas online.

FORMACIÓN SOBRE CIBERSEGURIDAD

La formación y la concienciación sobre la ciberseguridad son aspectos fundamentales para las empresas, que deben enfrentarse a un número cada vez mayor de amenazas que no dejan de evolucionar.

Los especialistas en seguridad internos deben conocer las técnicas avanzadas de seguridad que constituyen un componente fundamental de las estrategias de mitigación y gestión eficaces de amenazas empresariales. Al mismo tiempo, todos los empleados deben tener conocimientos básicos acerca de los peligros existentes y sobre los métodos de trabajo seguro.

Ofrecemos una cartera de formación relativa a la concienciación sobre la ciberseguridad, además de una serie de programas de formación que abarcan desde el nivel básico al experto en análisis de malware y ciencia forense digital.

- La concienciación en materia de ciberseguridad ayuda a las empresas a mejorar las habilidades de seguridad de sus empleados y, como consecuencia, su seguridad corporativa.
- La formación sobre seguridad para profesionales de seguridad de IT, para todos los niveles, mejora las habilidades de los expertos en seguridad internos y minimiza el riesgo de incidentes.

INTELIGENCIA FRENTE A AMENAZAS

¿Cuenta su sistema SIEM con capacidades de detección de ciberamenazas adecuadas? ¿Puede estar seguro de que se le avisará a tiempo de las amenazas más peligrosas? Nuestra cartera de servicios de inteligencia de amenazas está diseñada para equipar a las empresas a la hora de gestionar estos riesgos:

- Fuente de datos de amenazas: mejore su solución SIEM y sus capacidades analíticas con los datos de ciberamenazas actualizados al minuto.
- Los informes de inteligencia de APT ofrecen acceso exclusivo y proactivo a descripciones de campañas de ciberespionaje de alto nivel y a indicadores de compromiso (IOC).
- Los informes de inteligencia de amenazas específicos para cada cliente identifican componentes críticos de su red disponibles de forma externa.

SERVICIOS EXPERTOS

¿Los conocimientos de sus expertos son suficientes para resolver un ciberincidente? ¿Su infraestructura de IT y sus aplicaciones específicas están totalmente protegidas contra posibles ciberataques? Nuestros servicios expertos están diseñados para mitigar y resolver estos riesgos:

- Pruebas de introducción: aprenda a identificar los puntos más vulnerables de su infraestructura y evite los daños causados por los ataques cibernéticos. Garantice el cumplimiento de los estándares gubernamentales, industriales y corporativos (por ejemplo, PCI DSS).
- Evaluación de seguridad de aplicaciones: detecte vulnerabilidades en aplicaciones, desde soluciones basadas en la nube de gran envergadura, sistemas ERP, servicios bancarios online y otras aplicaciones específicas de su empresa hasta aplicaciones móviles e integradas para diferentes plataformas.
- Análisis de malware y ciencia forense digital: elabore una imagen detallada de cualquier incidente mediante exhaustivos informes con medidas para su corrección.

Concienciación sobre la ciberseguridad

Creación de un ciberentorno corporativo seguro con formación amena

Más del 80 % de los ciberincidentes se debe a errores humanos. De media, las empresas pagan 551 000 $ para recuperarse de una brecha de seguridad, mientras que las pymes invierten 38 000 $. 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 ha lanzado una familia de productos de formación basados en ordenador 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

ENFOQUE GALARDONADO

- 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.

Security For Data Centers

Protección y rendimiento perfectamente equilibrados para centros de datos híbridos

Los centros de datos definidos por software necesitan el mismo nivel de protección que sus homólogos tradicionales. Si no tiene esto en cuenta, sus sistemas virtualizados y almacenamientos de datos se convierten en el eslabón más débil de la cadena de seguridad de su centro de datos.

Las grandes empresas procesan niveles de datos cada vez mayores. Para seguir el ritmo de este aumento, las organizaciones deben replantearse no solo cómo almacenar y acceder a los datos, sino también cómo preservar su seguridad e integridad. Cuanto mayor sea la infraestructura, mayor será la cantidad conservada de datos confidenciales de la empresa, y mayor será también la potencia y fiabilidad que se exija a la solución de seguridad que los protege.

Con independencia de si opera su propio centro de datos o utiliza los servicios de terceros (a través de la infraestructura como servicio o IaaS), su solución de seguridad no solo debe proteger todos los datos esenciales de forma eficaz e ininterrumpida, sino que también debe preservar el rendimiento de la infraestructura del centro de datos.

Cualquier centro de datos ofrece numerosas superficies de ataque vulnerables a la explotación. A medida que aumenta el tamaño de su centro de datos, aumenta también su complejidad, lo que ofrece más oportunidades para la fraternidad cibercriminal. Su solución de seguridad debe estar a la altura del desafío y adaptarse de forma eficaz, lo que significa una integración completa con su entorno de IT actual, ya que, de lo contrario, disminuirán los niveles de rendimiento del centro de datos y se reducirá la eficiencia operativa global a medida que crezca.

LA SOLUCIÓN: KASPERSKY SECURITY FOR DATA CENTERS

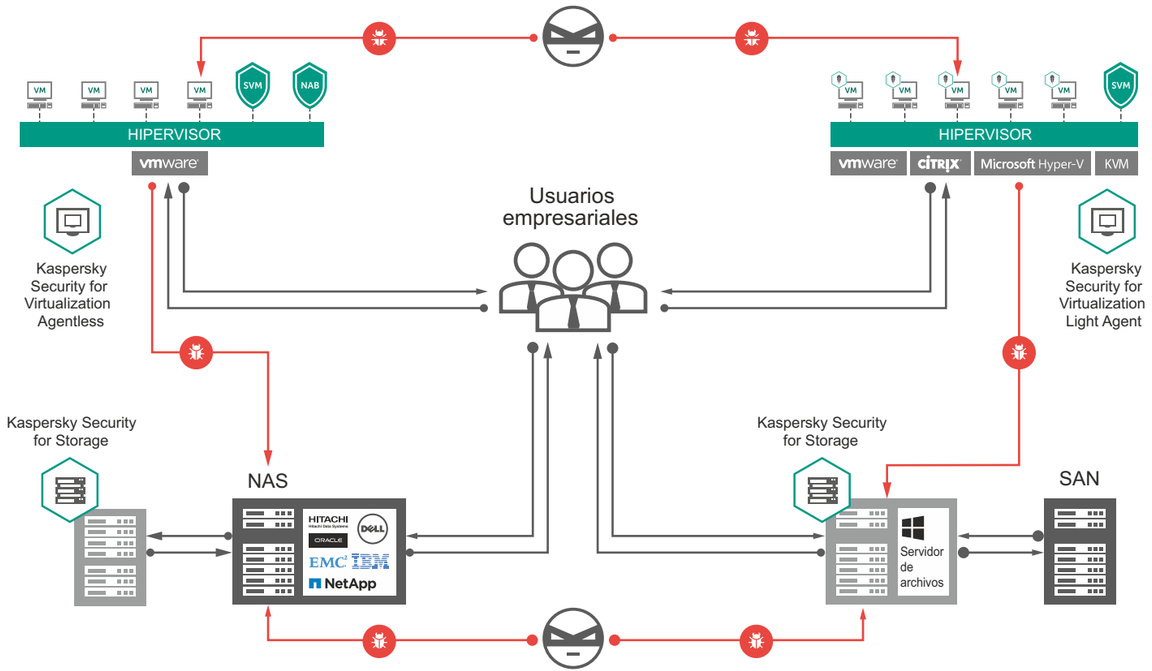
Ofrecemos soluciones que se centran en la protección de los dos ámbitos esenciales de su centro de datos: la infraestructura virtual y los sistemas de almacenamiento de datos. Ideal para entornos con varios hipervisores y sistemas de almacenamiento, la solución de Kaspersky Lab incluye lo siguiente:

- Seguridad específicamente diseñada para las principales plataformas de virtualización, como VMware con NSX, Citrix, Microsoft y KVM.
- Seguridad de los sistemas de almacenamiento conectado a la red (NAS), como EMC, NetApp, DELL, IBM, Hitachi y Oracle.

Kaspersky Security for Data Centers se basa en nuestro motor de seguridad galardonado y opera como una única plataforma integrada, por lo que es fácil de gestionar y de integrar en diferentes configuraciones de centros de datos. La administración centralizada significa que su equipo puede aplicar políticas de seguridad unificadas en todo el centro de datos, algo que contribuye a reducir los costes operativos.

Esta completa solución:

- Protege sus datos y sistemas contra los ciberataques.
- Proporciona herramientas eficaces para el mantenimiento de los altos niveles de rendimiento y continuidad empresarial.
- Permite a su equipo gestionar la seguridad de todas las máquinas virtuales y físicas en el centro de datos desde una única consola centralizada.



Virtualization Security

Protección superior, flexible y eficiente para servidores virtuales y VDI

Cuando se trata de la seguridad de los sistemas virtuales, las empresas buscan el equilibrio adecuado entre la protección y el rendimiento, así como las funciones de seguridad más avanzadas para proteger los procesos fundamentales de la empresa.

A medida que las empresas implementan entornos virtualizados en más partes de su entorno de IT, aumenta la necesidad de una seguridad diseñada específicamente para la virtualización. Sin embargo, no resulta sencillo buscar una solución que proporcione capacidades de seguridad a su creciente infraestructura de escritorio virtual (VDI) y su entorno de servidor virtual, y que mantenga a la vez todos los beneficios de la virtualización con respecto al rendimiento. Con todas sus ventajas, la virtualización también genera más "superficies de ataque", lo que otorga a los cibercriminales más oportunidades para atacar a las grandes empresas.

La solución que protege su infraestructura virtualizada debe ofrecer una protección ininterrumpida y proporcionar una funcionalidad mejorada a la vez que sigue conservando la eficiencia de su infraestructura virtual.

La singular arquitectura de la solución especializada de Kaspersky Lab proporciona una eficaz protección multicapa de las máquinas virtuales sin sacrificar el rendimiento. El resultado son unos ratios de consolidación mucho mayores que los de las soluciones antimalware tradicionales. Ahora se eliminan los análisis simultáneos y la sobrecarga de actualizaciones, junto con los márgenes de vulnerabilidad y las brechas de seguridad instantáneas. Con niveles adicionales de protección combinados con mecanismos de prevención de intrusiones, la solución de Kaspersky Lab lleva la seguridad de la plataforma de virtualización empresarial a un nuevo nivel.

De media, los robos de datos relacionados con sistemas virtuales costaron dos veces más que los relacionados con las máquinas físicas.

Fuente: Encuesta de riesgos globales de 2015 de KasperskyLab

Para una empresa grande, el coste medio asociado a la recuperación de una brecha de seguridad virtual es de más de 940 000 $, el doble en comparación con un incidente en el que solo se ve afectada la infraestructura física.

Si bien un ataque a los nodos físicos conduce a la pérdida temporal de acceso a la información crítica para la empresa en el 36 % de los incidentes denunciados, esta cifra se eleva al 66 % cuando la brecha afecta a los servidores y escritorios virtuales.

LA SOLUCIÓN: KASPERSKY SECURITY FOR VIRTUALIZATION

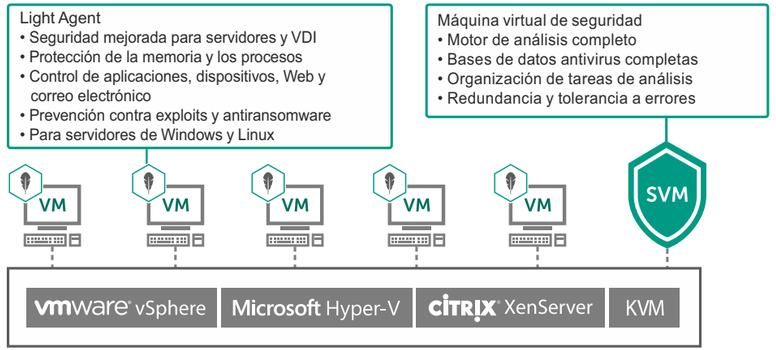
Kaspersky Lab ofrece dos tecnologías que le permiten alcanzar ese equilibrio perfecto entre seguridad óptima y rendimiento preservado.

Nuestra solución sin agentes funciona junto con tecnologías de hipervisor fundamentales (como VMware NSX), y nuestra solución de agente ligero ofrece niveles adicionales de protección para cada máquina virtual.

Si desean proteger las máquinas virtuales, las empresas solo tienen que implementar una única máquina virtual de seguridad en la que se pueden descargar las tareas de análisis de archivos. Esta máquina virtual de seguridad proporciona protección antimalware centralizada para todas las máquinas virtuales en el host sin generar un consumo adicional de recursos. La tolerancia a errores y la redundancia integradas confieren a su solución de seguridad la fiabilidad que necesita para conseguir el éxito de las operaciones empresariales.

Además, implementar un agente ligero en cada máquina virtual permite añadir una protección multicapa y controles de seguridad con muchas funciones. La seguridad de sus máquinas virtuales, ya sean sin agentes, con agente ligero o ambos, puede gestionarse junto con los servidores de endpoints físicos y los dispositivos móviles desde una única consola.

Tecnología exclusiva de agente ligero de Kaspersky Lab



Kaspersky Security for Virtualization se integra plenamente con las plataformas de virtualización más populares: VMware vSphere con NSX, KVM, Microsoft Hyper-V y Citrix XenServer. Nuestra solución de seguridad está optimizada para proteger el rendimiento de la plataforma mediante la explotación de sus tecnologías de hipervisor fundamentales, lo que complementa y mejora la seguridad en VMware Horizon y Citrix XenDesktop, entre otros.

Kaspersky Security for Virtualization cuenta con dos tipos de licencias, en función de las necesidades de la empresa y las características de su infraestructura virtual: según el número de máquinas virtuales (escritorios más servidores) o según el número de núcleos de procesadores físicos del servidor host.

Mobile Security

Seguridad sofisticada, gestión y control de smartphones y tablets

En un periodo de tres meses en 2016, detectamos más de 3,5 millones de paquetes de instalación maliciosos, más de 83 000 troyanos de ransomware y más de 27 000 troyanos bancarios, todos dirigidos a los dispositivos móviles de nuestros clientes.

El software malicioso y los ataques de phishing y de sitios web dirigidos a los dispositivos móviles no dejan de proliferar, mientras que las capacidades de los dispositivos móviles están todavía en desarrollo. 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 empresariales (tendencia BYOD o "traiga su propio dispositivo") ha ampliado la variedad de dispositivos que operan en la red corporativa, lo que 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 de una empresa. 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.

NINGUNA PLATAFORMA ES SEGURA

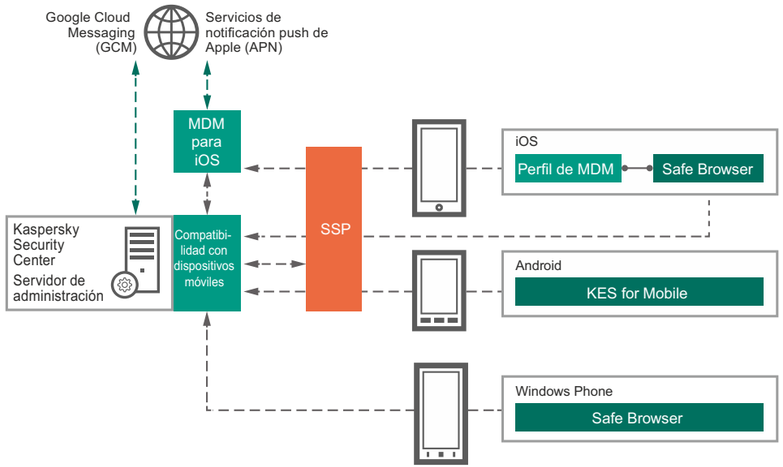
Los cibercriminales utilizan distintos métodos para lograr acceso no autorizado a dispositivos móviles, como aplicaciones infectadas, redes Wi-Fi públicas con bajos niveles de seguridad, ataques de phishing y mensajes de texto infectados. Cuando un usuario visita un sitio web malicioso sin querer, o 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 una protección multicapa y una amplia gama de funciones de gestión de dispositivos móviles (MDM) y gestión de aplicaciones móviles (MAM). Así se reduce significativamente el tiempo necesario para el mantenimiento de los dispositivos móviles y se brinda acceso móvil seguro a los sistemas corporativos.

- Seguridad móvil: nuestras tecnologías de seguridad móvil ofrecen una protección multicapa contra las amenazas móviles más recientes, además de un conjunto completo de funciones antirrobo que se pueden activar de forma remota.
- Gestión de dispositivos móviles: la integración con las principales plataformas permite analizar y controlar los dispositivos de forma inalámbrica, algo que mejora considerablemente la protección y la gestión de los dispositivos móviles con Android, iOS y Windows Phone.
- Gestión de aplicaciones móviles: los contenedores aislados para aplicaciones y la opción de borrado selectivo de la memoria del dispositivo permiten que la información personal y empresarial almacenada en el dispositivo del empleado esté protegida.

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.



Arquitectura de la solución

DDoS Protection

Protección total contra todo tipo de ataques DDoS

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.

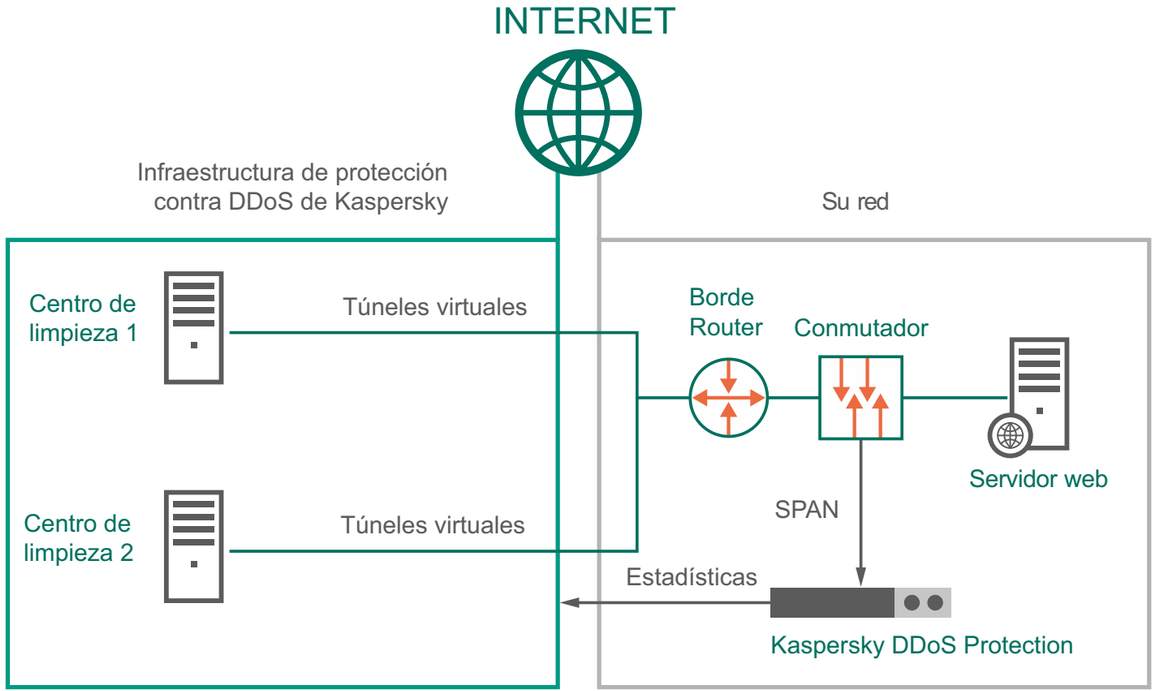
En cuanto se identifica un posible caso de ataque, el Centro de operaciones de seguridad (SOC) de Kaspersky Lab recibe una alerta. En los escenarios de implementación de Kaspersky DDoS Protection Connect y Connect+, la mitigación se inicia automáticamente mientras nuestros ingenieros ejecutan de inmediato 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 big data
- Protección y asistencia rápidas ininterrumpidas por parte del equipo de respuesta a emergencias



Esquema de Kaspersky DDos Protection Control

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. Una investigación reciente ha descubierto que los ciberataques provocaron el 35 % de los incidentes de funcionamiento incorrecto en la red industrial.

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 tecnológicos detectando y evitando acciones (intencionales o accidentales) que puedan interrumpir o detener servicios vitales.

LA SOLUCIÓN: KASPERSKY INDUSTRIAL CYBERSECURITY

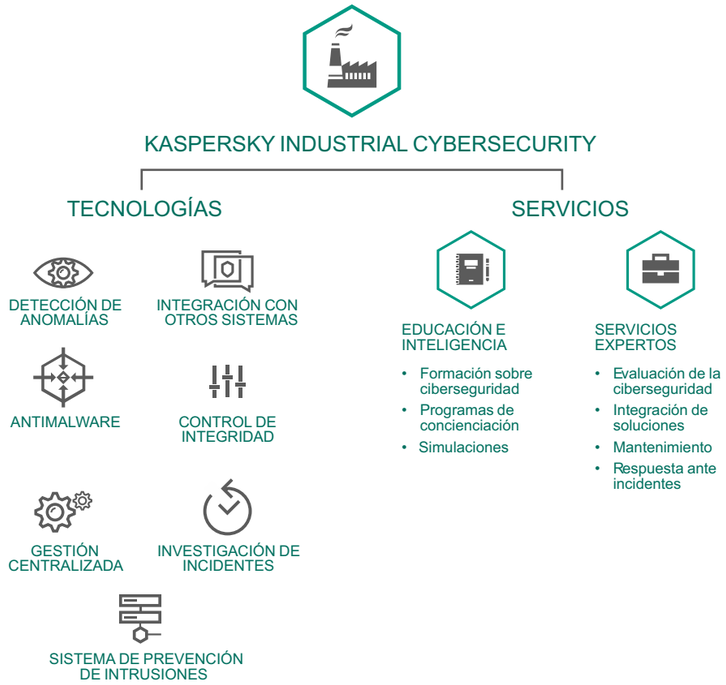
Kaspersky Industrial CyberSecurity es una cartera de tecnologías y servicios diseñada para proteger cada nivel industrial, lo que incluye servidores SCADA, paneles HMI, estaciones de trabajo de ingeniería, PLC, conexiones de red y personas, sin afectar a la continuidad operativa ni a la coherencia de los procesos tecnológicos. 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 tecnológico.



Fraud Prevention

Crecimiento de la banca digital sin preocupaciones sobre la seguridad ni problemas de uso

Hoy en día, la banca digital es uno de los elementos clave necesarios para el crecimiento de las empresas de servicios financieros y la adquisición de clientes. Sin embargo, la banca digital resulta un sector tentador no solo para los clientes, sino también para los estafadores.

Los cibercriminales son cada vez más expertos en el desarrollo de herramientas sofisticadas que superan la protección tradicional, facilitan una ruta de entrada a los sistemas bancarios, obtienen acceso a las cuentas de los clientes y permiten a los atacantes iniciar y falsificar transacciones.

La reacción a los ataques fraudulentos una vez que se producen puede que fuera aceptable hace unos años, pero a día de hoy esto no ofrece la protección que exigen los bancos y los clientes.

Deloitte cree que el sector de los servicios financieros se está enfrentando al mayor riesgo económico en relación con la ciberseguridad y está obligado a destinar mayores recursos a la mejora de la seguridad, la vigilancia y la resiliencia de su modelo de ciberseguridad.

LA SOLUCIÓN: KASPERSKY FRAUD PREVENTION

Kaspersky Fraud Prevention potencia el sistema de seguridad existente de un banco y aporta un nuevo nivel de protección contra el fraude. La solución protege los equipos, los dispositivos móviles y las cuentas digitales de los usuarios, así como los sistemas del banco. Al proteger las cuentas y las transacciones de los clientes, Kaspersky Fraud Prevention ayuda a los bancos a aumentar la fidelidad de los clientes.

Kaspersky Fraud Prevention pertenece a una nueva generación de sistemas, que permite el análisis en tiempo real del comportamiento, los dispositivos y el entorno del usuario. Gracias al aprendizaje mecánico, la solución detecta escenarios de fraude y blanqueo de dinero avanzados. También permite que el equipo antifraude del banco recopile información precisa sobre cada incidente, incluidos los detalles utilizados para obtener acceso a las cuentas.

Esta información puede revelar, por ejemplo, que el banco no es responsable de un incidente de fraude, lo cual contribuye a reducir los costes de compensación por daños y perjuicios.

Kaspersky Fraud Prevention añade un nivel de defensa fundamental a la protección contra el fraude existente del banco.

- Kaspersky Fraud Prevention Clientless Malware Detection proporciona tecnologías de servidor que protegen a todos los clientes con independencia del dispositivo o la plataforma que utilicen. El sistema permite a su banco detectar el acceso de clientes infectados lo antes posible.
- Kaspersky Fraud Prevention for Mobile ayuda a proteger a los usuarios que acceden a sus cuentas bancarias a través de dispositivos móviles (Android, iOS y Windows Phone).
- Kaspersky Fraud Prevention for Endpoints se ejecuta en los ordenadores de los clientes (Windows o Mac) y proporciona una eficaz protección contra las causas del malware y los ataques en Internet.
- Kaspersky Fraud Prevention Cloud es un producto para la detección de fraudes en la banca online y móvil. Entre las funciones principales se incluyen la autenticación basada en riesgos, el análisis del comportamiento, la detección de anomalías en sesiones continuas y la biometría pasiva, basadas en el aprendizaje mecánico y los modelos estadísticos.

Esta completa solución de prevención contra el fraude:

- Añade seguridad en diferentes canales a la banca digital y los pagos.
- Detecta de forma proactiva los fraudes avanzados en tiempo real antes de procesar las transacciones.
- Ayuda a proteger a todo tipo de usuarios, con independencia del dispositivo.
- Ofrece una seguridad fluida para que también lo sea la experiencia del usuario.
- Ayuda a los bancos a aumentar la retención de clientes, atraer a nuevos clientes y aumentar la adopción y el uso de la banca online y móvil de alto margen.
- Reduce los costes mediante la automatización y el aprendizaje mecánico.

Asistencia premium y servicios profesionales

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

Cuando un incidente de seguridad se traduce en tiempo de inactividad del sistema de IT, las consecuencias pueden afectar a todos los aspectos de las operaciones de una empresa. Para evitar esta situación, Kaspersky Lab proporciona una gran variedad de programas de asistencia premium que tratan sus problemas de seguridad de IT con una alta prioridad, lo que le permite mantener su negocio en marcha sin problemas.

ASISTENCIA PREMIUM: MSA ENTERPRISE

Los programas de acuerdos de servicio de mantenimiento (MSA) de Kaspersky Lab están destinados a empresas que dependen de su infraestructura de IT para la continuidad del negocio y la entrega continua de procesos críticos. MSA Enterprise está diseñado específicamente para grandes empresas con entornos complejos que requieren una asistencia especializada, personalizada y proactiva al momento.

SERVICIOS PROFESIONALES

Siguiendo siempre las prácticas recomendadas y las metodologías establecidas, nuestros 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 y para trabajar con su política de control de cambios.

- Implementation Service: le ofrece asesoramiento y asistencia de expertos para que la implementación de los productos de Kaspersky Lab se efectúe sin problemas y a la perfección, y para garantizar que sus actividades se realizan conforme a las prácticas recomendadas con una configuración óptima y sacando el máximo partido del software de gestión centralizada de Kaspersky Lab.
- Health Check Service: tras una auditoría completa de su entorno de red y de la configuración de los productos, nuestros expertos le ofrecen un informe exhaustivo con recomendaciones sobre cómo mejorar la seguridad o la eficacia al gestionar los sistemas.

La asistencia premium y los servicios profesionales de Kaspersky permiten recurrir a expertos en seguridad que conocen la forma más rápida, segura y eficaz de resolver sus problemas, así como:

- SLA de respuesta ante incidentes
- Parches personalizados
- Respuesta prioritaria a incidentes con malware
- Supervisión y generación de informes
- Único punto de contacto

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 de 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. En concreto, nos encontramos entre los cuatro principales proveedores de soluciones de seguridad para usuarios de endpoints y seguimos mejorando nuestra posición en el mercado. Nuestra compañía está considerada "líder" en materia de protección para endpoints por las tres mayores agencias de analistas (Gartner, IDC y Forrester).

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

Notas