Solución integrada para seguridad de endpoints

Construir defensas sólidas con recursos limitados

kaspersky

Obtenga más información en kaspersky.es
#bringonthefuture

Introducción

La mayoría de las organizaciones, independientemente del tamaño, la ubicación o la disciplina, ahora entienden que cuando se trata de un ciberataque, la cuestión no es si les sucederá, sino cuándo. Nadie debería considerarse inmune en la actualidad.

Pero tener el tiempo, los recursos, o (para ser franco) la motivación para navegar con eficacia el panorama actual de amenazas y seguridad... ese es otro tema.

La mayoría de los analistas de seguridad de la información (y casi que no hay suficientes para abarcarlo todo) están sobrecargados tal como están. Prestar atención a los nuevos empleados y sus dispositivos, averiguar nuevas leyes y problemas de cumplimiento, leer información sobre las últimas amenazas, todo esto debe abordarse antes de llegar realmente al negocio principal de la protección corporativa.

Básicamente, muy pocos profesionales de la seguridad, si los hay, pueden disfrutar del lujo de pasar todo su tiempo buscando amenazas nuevas y exóticas y respondiendo a ellas.

En este punto entran en el mercado los proveedores de ciberseguridad y sus productos y soluciones. Nuestro trabajo es ayudarle a proteger completamente su infraestructura y a mantener a sus usuarios seguros, con el menor gasto posible en recursos, incluyendo tiempo y dinero, así como una experiencia cara y difícil de obtener.

Los desafíos

El 91 %[1] de las organizaciones ha sufrido al menos un ataque en el transcurso de un año.

1 de cada 10[1] organizaciones se ha enfrentado a un ataque dirigido (del que sea consciente) durante el mismo período.

El 30 %[1] de las organizaciones aún no ha implementado completamente software antimalware

En primer lugar, echemos un vistazo a algunos de los problemas a los que se enfrentan los administradores de IT y de seguridad de IT de hoy en día.

Mayor número de amenazas de un ataque dirigido o avanzado

Los ataques dirigidos y las amenazas complejas son un problema enorme y van en aumento. Las herramientas de cibercriminales se están volviendo tan baratas y accesibles que básicamente cualquier persona con un ordenador puede lanzar ahora un ataque avanzado. Lo que significa que las organizaciones que una vez asumieron que estaban «bajo el radar» en términos de amenazas avanzadas están descubriendo por las malas que las cosas han cambiado.

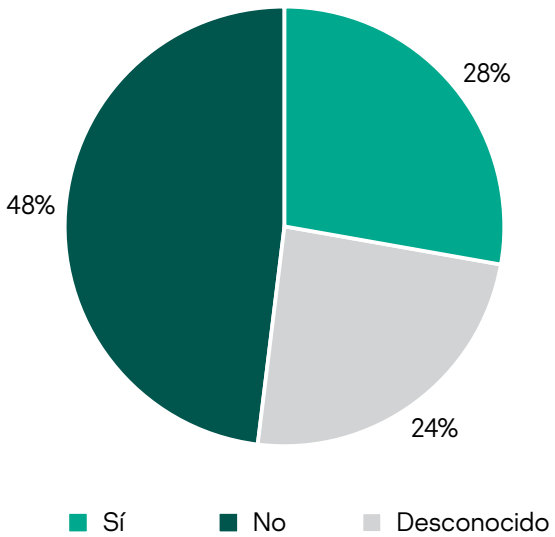
Dicho esto, las amenazas genéricas también siguen siendo un problema: el volumen total de estas amenazas es un problema enorme en el mundo actual.

La gran mayoría de las ciberamenazas entran en el endpoint o están diseñadas para desencadenarse allí (o ambas).

Por lo tanto, una de las mejores formas de proteger sus activos es proteger sus endpoints.

Según un estudio del instituto SANS[2], el 28 % de las organizaciones encuestadas han tenido acceso a los endpoints por parte de los atacantes, y el 24 % no sabe si han sufrido una brecha de seguridad.

Índices de compromiso de endpoints



1 Informe de riesgos de IT globales de Kaspersky, Kaspersky, 2019

2 Encuesta SANS de 2019 sobre riesgos y protecciones de endpoints de próxima generación, The SANS Institute, 2019

3 Estudio de trabajadores de ciberseguridad, (ISC)² 2019

4 Informe anual oficial de trabajos de ciberseguridad, CyberSecurity Ventures, 2019

Error humano

Desafortunadamente, conectado a la mayoría de los endpoints está el componente más vulnerable de la infraestructura de cualquier organización: el usuario. Los usuarios pueden acceder regularmente a los datos de la empresa de forma remota y en sus propios dispositivos, y muchos de ellos habrán crecido en línea, acostumbrados a los malos hábitos y confiando demasiado por el camino. Y ellos, así como todo lo demás, también deben mantenerse seguros.

Por lo tanto, detectar y prevenir comportamientos inseguros en los complejos entornos de IT actuales se convierte en otro trabajo más para el especialista en seguridad, que se ve muy presionado.

Además, los profesionales de IT también pueden cometer errores (todos somos humanos, después de todo) que pueden dar lugar a ataques a través de vulnerabilidades en dispositivos personales o corporativos con parches de manera irregular, por ejemplo.

Los recursos y la falta de ellos

2 de cada 3[3] organizaciones están experimentando una falta de personal de seguridad de la información.

Se prevé que, para 2021, **3,5 millones**[4] puestos de trabajo de ciberseguridad estarán vacíos.

Por lo tanto, el especialista en IT tiene mucho que hacer.

Incluso en el caso de las organizaciones más pequeñas, existe un volumen cada vez mayor de eventos de seguridad que se deben pasar, analizar y responder a diario, algo difícil de seguir haciendo de forma eficiente y oportuna. Los cibercriminales saben que las empresas tienen dificultades en este aspecto y están aprovechando al máximo.

Y, incluso para aquellos que tienen la suerte de tener bolsillos profundos, hay una escasez global de profesionales de ciberseguridad capacitados. Este problema no es nuevo, pero teniendo en cuenta cuántos especialistas se forman cada año, no desaparecerá pronto.

Mantener a sus especialistas en seguridad contentos y centrados bajo estas circunstancias, o simplemente mantenerlos, es un desafío. La sobrecarga es un gran problema, en particular si su equipo altamente cualificado y en cuya formación se ha invertido pasa todo el día entre tareas mundanas.

Además, o por supuesto, está la cuestión de los recursos financieros. Y la potencia del procesador. Y todo lo necesario para optimizar la seguridad sin afectar a las velocidades de procesamiento, la productividad de los empleados, la satisfacción del usuario o los presupuestos.

La solución

Entonces, ¿cuáles son las respuestas?

Protección efectiva

En primer lugar, todo depende **de una protección de endpoint eficaz** y de una plataforma de protección de endpoints (EPP) fuerte, así de simple. La prevención de amenazas a nivel de endpoints, antes de que puedan activar alertas, reduce el estrés sobre los recursos, mitiga el riesgo de que un ataque tenga éxito y ayuda a mantener el negocio funcionando sin problemas y con seguridad. Esto se aplica tanto a los ataques generales, que ocupan la mayor parte del tiempo, como a los ataques más complejos e incluso dirigidos, que tienen más probabilidades de tener éxito y de causar mayor daño.

Nuestro enfoque recomendado es una combinación de **defensas de endpoints de varios niveles**: una sólida protección de referencia contra las amenazas generales y defensas de varios niveles y capas frente a las amenazas más recientes y complejas.

También es importante recordar que algunas amenazas están diseñadas específicamente para evadir las EPP, para ellas deben usarse diferentes métodos de detección, como **el aislamiento de procesos automatizado**.

EDR (Endpoint Detection and Response) proporciona la siguiente capa de seguridad crítica. La EPP proporciona la identificación y protección iniciales, mientras que EDR proporciona visibilidad y opciones de análisis más profundos, lo que le permite ver cómo ha comenzado el ataque y en qué fase se encuentra ahora mismo. Además de la detección, EDR también proporciona múltiples opciones de respuesta, por lo que la amenaza revelada se puede contener rápida y eficientemente.

La EDR solo puede ser eficaz en combinación con una base sólida de protección. Cuantos más incidentes pueda evitar su solución EPP por adelantado, menos tendrá que lidiar con su solución EDR y podrá dedicar más recursos a esos pocos.

Abordar el comportamiento humano

Desde el punto de vista del usuario, una de las mejores maneras de evitar el error humano es, por supuesto, eliminar la oportunidad y la tentación, a través de los **controles de aplicaciones, web y dispositivos**. Los controles eficaces, lejos de actuar como una limitación para el negocio, pueden en realidad impulsar la productividad, mediante el bloqueo de la pérdida de tiempo, así como de sitios web de entretenimiento y redes sociales potencialmente peligrosas, por ejemplo.

Pero aquí, la educación de los usuarios es la clave. La **formación adecuada sobre ciberseguridad** puede tener un efecto profundo en el comportamiento de los empleados, cambiar la cultura corporativa, reducir significativamente el riesgo corporativo y reducir drásticamente la carga de trabajo del departamento de IT.

El retorno de su inversión

Por último, cualquier enfoque tiene que ser capaz de justificarse financieramente en términos de ROI, y de funcionar ahora y en el futuro, en entornos con recursos finitos, que pueden incluir una experiencia especializada en seguridad limitada.

Automatización y optimización

En vista del aumento de los volúmenes de amenazas y de la escasez de especialistas en seguridad del sector disponibles para trabajar en ellas, **la automatización de las tareas de seguridad**, siempre que sea posible, resulta fundamental. Esto deja a sus especialistas en seguridad libres a fin de utilizar su valioso tiempo y sus habilidades para tratar con los incidentes que realmente requieren la aportación y la experiencia humana (y los mantiene más contentos y motivados como resultado).

La automatización de tareas también elimina el riesgo de errores humanos: por ejemplo, la priorización e implementación automáticas de parches para vulnerabilidades de sistemas es mucho más eficaz que confiar en que los operadores humanos encuentren el tiempo necesario para realizar esta actividad crítica pero poco emocionante.

La implementación sencilla y una **consola de gestión** centralizada y optimizada también ahorran tiempo y recursos. El cambio de consolas entre operaciones y la búsqueda de comandos no solo requiere mucho tiempo y resulta frustrante, sino que también presenta oportunidades de errores y omisiones administrativos.

Una nota sobre la protección a varios niveles

Hemos dicho que cualquier solución destinada a proteger contra todas las formas de ciberamenazas, incluidos los ataques avanzados y dirigidos, tiene que ser multicapa.

En primer lugar, la solución tiene que proporcionar una **sólida protección de referencia de endpoints**, incluidos los controles de endpoint (con funciones de restricción y bloqueo de aplicaciones y dispositivos web) y un motor antimalware reforzado. También es preferible disponer de funciones automatizadas de gestión de parches y evaluación de vulnerabilidades para ahorrar tiempo y esfuerzo al personal de IT en la realización de tareas rutinarias.

Sin embargo, el malware avanzado plantea retos adicionales que requieren capas de seguridad adicionales. El malware puede estar diseñado específicamente para evitar incluso los mecanismos de detección de endpoints más sofisticados, permaneciendo oculto e inactivo hasta que surja la oportunidad correcta. La respuesta es persuadir al malware para que se revele y se active en un entorno seguro y controlado. Aquí es donde entra el **aislamiento de procesos**, uno que preferiblemente no solo debe ser capaz de detectar, sino de responder a las amenazas de una manera altamente automatizada.

La detección de comportamientos complejos en los endpoints también es el centro de atención de **EDR.** Al igual que la EPP, el EDR debería combinar idealmente la automatización con las herramientas y la visibilidad para apoyar la entrada humana cuando sea necesario. El oficial de seguridad debe ser capaz de realizar un análisis de la causa raíz de los incidentes y responder a las amenazas de forma oportuna, manualmente o mediante el uso de opciones de respuesta automatizadas.

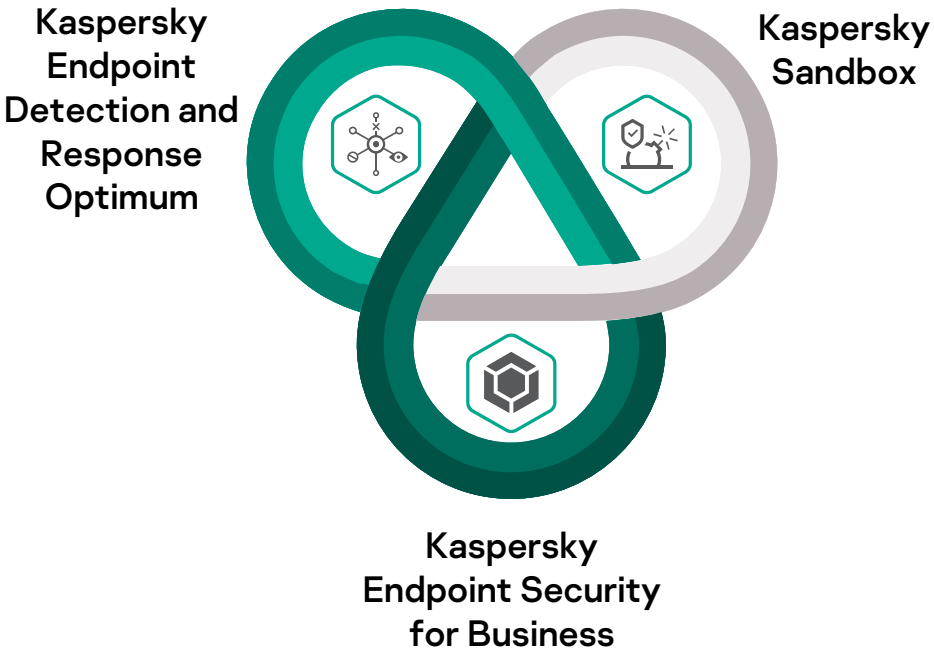
La combinación de las tecnologías de EPP, Sandbox y EDR permite abordar el malware general de forma rápida y eficaz, limita las oportunidades de error humano y reduce el riesgo de un ataque avanzado o dirigido con éxito al detectar y responder incluso a amenazas nuevas, desconocidas y de día cero.

Y tener una solución integrada para todo esto significa que no hay brechas entre las diferentes herramientas, que los hackers y los atacantes puedan explotar.

Solución de Kaspersky

Todos los problemas mencionados anteriormente se resuelven de la forma óptima mediante la solución Integrated Endpoint Security de Kaspersky, una solución altamente automatizada que consta de protección y controles de endpoints integrados, un aislamiento de procesos automatizado y EDR. Todos estos tres componentes funcionan juntos desde la base de una EPP fuerte. Echemos un vistazo más detalladamente a cada componente, ya que ofrecen aún más que la resolución de los problemas descritos anteriormente.

Sólida protección de endpoints de referencia



Kaspersky Endpoint Security for Business cuenta con una sólida base de datos EPP (incluida la protección contra ransomware y ataques sin archivos) que utiliza el motor antimalware más probado y galardonado del mercado.

Las capas de protección de endpoints proporcionadas por Kaspersky Endpoint Security for Business incluyen:

- Nuestro galardonado motor antimalware mejorado con aprendizaje automático
- Detección de ransomware
- Detección de comportamiento con reversión automática: identificación y bloqueo de amenazas avanzadas, incluidas malware sin archivos y apropiaciones de cuentas administrativas e inversión de los cambios ya realizados.
- Prevención de exploits
- Defensas contra amenazas móviles e integración de EMM
- Prevención de intrusiones basada en host (HIPS)
- Firewall y gestión de firewall de sistemas operativos
- Inteligencia automatizada frente a amenazas (Kaspersky Security Network)
- Cifrado: incluida la gestión de cifrado integrado en el sistema operativo
- Asesor de políticas de seguridad: supervisión de las modificaciones de la configuración de seguridad optimizada
- Valoración de las vulnerabilidades y gestión de parches
- Instalación de software de sistemas operativos y de terceros
- Integración de sistemas SIEM

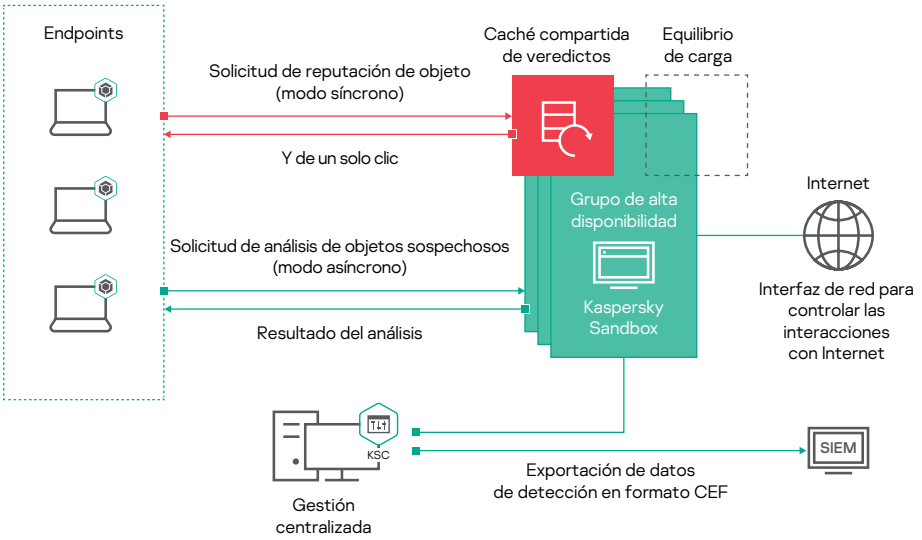
El endurecimiento de los sistemas y la mitigación de errores humanos se proporcionan a través de controles que incluyen:

- Control de aplicaciones con marcado en lista blanca basado en categorías
- Control adaptativo de anomalías que supervisa y bloquea acciones sospechosas que no son típicas de los equipos de la red de una empresa
- Control de dispositivos: controla y bloquea el plug-in de dispositivos externos
- Control web: bloquea o restringe el acceso a sitios potencialmente peligrosos, que desperdician tiempo o que no son apropiados

Para obtener más información sobre Kaspersky Endpoint Security for Business, visite nuestro sitio web.

Sandbox automatizado

Kaspersky Sandbox detecta y responde automáticamente a las amenazas diseñadas para burlar la protección de endpoints, sin necesidad de intervención humana.



Flujo de trabajo de Kaspersky Sandbox

Los servidores del sandbox agrupados ejecutan los objetos que se van a analizar en una máquina virtual aislada que simula una estación de trabajo. El componente recibe una solicitud de análisis de archivos del agente Kaspersky Endpoint Security for Business instalado en la máquina del usuario final, tras lo cual el objeto se pone en cola en uno de los servidores del grupo. Cuando se envía el archivo para su procesamiento, Kaspersky Sandbox lo ejecuta y registra todas las acciones que realiza. El componente, analiza los datos obtenidos en busca de actividad maliciosa o sospechosa y devuelve el veredicto al agente de Kaspersky Endpoint Security for Business que solicitó el análisis. El veredicto también se envía a la caché operativa, lo que permite a otros hosts recuperar rápidamente información sobre el objeto analizado sin tener que volver a analizarlo. Esto reduce la carga de los servidores de Kaspersky Sandbox y mejora el tiempo de respuesta a las amenazas.

Una vez detectado el archivo como malicioso, el motor de Kaspersky Endpoint Security for Business puede utilizar su indicador de compromiso (IoC) para iniciar una tarea de corrección automática con el fin de eliminar el archivo del resto de equipos de la red.

Las técnicas utilizadas por Kaspersky Sandbox incluyen:

- Supervisión de la interacción con los recursos de Internet
- Carga del módulo
- Modos de exploración síncrono y asíncrono
- Contrarrestar técnicas de evasión
- Aplicación de diferentes modos de emulación
- Modelado de acciones de usuarios
- Generación automática de IoC y análisis de la infraestructura
- Prevención automática

Para obtener más información sobre Kaspersky Sandbox, visite nuestro sitio web.

EDR optimizado

El nuevo Kaspersky Endpoint Detection and Response Optimum complementa nuestro producto Kaspersky Endpoint Security for Business, ofrece visibilidad completa y la capacidad de aplicar un análisis de causas raíz para comprender plenamente el estado de las defensas corporativas contra las amenazas avanzadas.

El especialista en seguridad de IT recibe la información y los conocimientos necesarios para una investigación eficaz y una respuesta rápida y precisa a los incidentes antes de que pueda producirse el daño.

Kaspersky Endpoint Detection and Response Optimum, que forma parte de nuestra solución integrada de seguridad de endpoints, permite realizar análisis de la causa raíz mediante:

- Visualización de la ruta de propagación de ataques, que muestra cómo se desarrolló la amenaza en el endpoint
- Información sobre el archivo, incluidos metadatos, origen del archivo, datos de modificación, firma digital, etc.
- Información sobre el host y el usuario
- Información sobre la detección
- Incursiones en procesos
- Instalaciones de archivos
- Modificaciones de claves de registro
- Conexiones

Después de detectar una amenaza, hay disponibles varias opciones de respuesta automatizadas y con un solo clic, entre las que se incluyen:

- Aislar el host
- Iniciar el análisis del host
- Eliminar archivo (cuarentena)
- Destruir el proceso
- Impedir que se ejecute el proceso

Para una investigación más detallada, hay disponibles funciones como importar IoC o generarlos en función de las detecciones, así como el análisis de los IoC con opciones de respuesta automatizada predefinidas.

Según un estudio de Forrester, uno de los principales requisitos de las empresas entrevistadas es que su solución de seguridad se implemente con poca o ninguna interrupción para los usuarios. Este principio es el núcleo de Integrated Endpoint Security

Para obtener más información sobre Kaspersky Endpoint Detection and Response Optimum, visite nuestro sitio web.

Kaspersky Endpoint Detection and Response Optimum está disponible tanto en las instalaciones como en la nube*.

Gestión y administración

Todos los componentes de nuestra solución se crean internamente y se administran a través de la misma consola única, y utilizan el mismo agente de endpoints multiuso. Por lo tanto, la gestión diaria es centralizada, directa y eficiente.

Concienciación sobre seguridad

- **El 52 %** de las empresas considera a los empleados la mayor amenaza para la ciberseguridad empresarial[6]
- **El 60 %** de los empleados tiene datos confidenciales en su dispositivo corporativo (datos económicos, base de datos de correo electrónico, etc.)
- **El 30 %** de los empleados admite que comparte los datos de inicio de sesión y contraseña del PC de su trabajo con los compañeros[8]

También ofrecemos productos de formación por ordenador que combinan la experiencia en ciberseguridad con técnicas y tecnologías educativas que siguen las prácticas recomendadas. Este enfoque cambia el comportamiento de los usuarios y ayuda a crear un entorno de ciberseguridad en toda la organización.

Kaspersky Security Awareness desarrolla una cultura de comportamiento de ciberseguridad:

- Formación para que los usuarios sepan cuándo deben alertar a los administradores de los signos de una amenaza potencial real
- Reducción de los errores de usuario resultantes de la ignorancia o la ingenuidad
- Disminución del número de alertas de seguridad ante los cuales los administradores deben reaccionar

Puede seguir el progreso de sus alumnos a través del panel intuitivo, con seguimiento de datos en directo, tendencias y pronósticos, junto con recomendaciones sobre cómo mejorar sus resultados.

Para obtener más información sobre Kaspersky Security Awareness, visite nuestro sitio web.

6 "The cost of a data breach", Kaspersky, 2018

* Existen algunas restricciones en cuanto a la gama de funciones y funcionalidades que se pueden gestionar a través de la consola en la nube. Para obtener información completa, consulte la ayuda en línea.

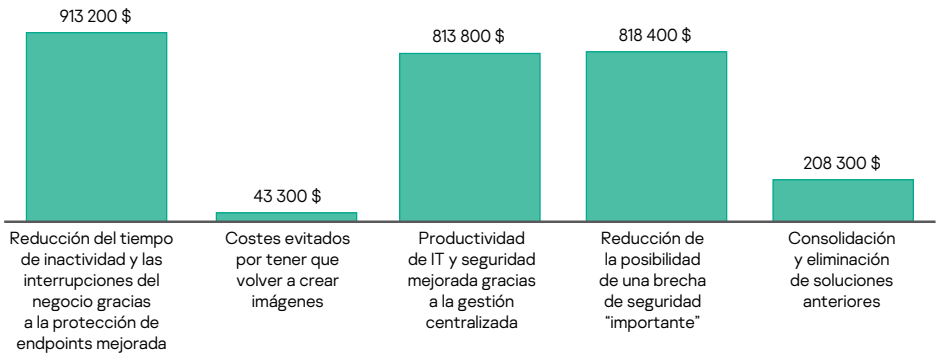
Su ROI

Al igual que con cualquier solución, los costes son tan importantes como los beneficios que ofrecemos. A continuación verá un ejemplo del aspecto del retorno de la inversión en las soluciones de Kaspersky, basado en un estudio de Forrester[7] de una solución de seguridad de Kaspersky basada en Kaspersky Endpoint Security for Business y Kaspersky Endpoint Detection and Response.

Beneficios cuantificados de valor actual (PV) ajustado al riesgo experimentados por las empresas entrevistadas para el estudio de Forrester:

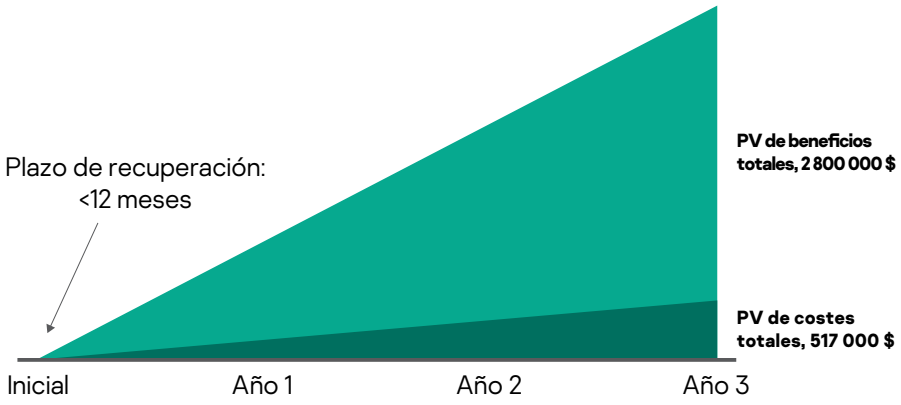
- **Cerca de 1 millón de USD:** el impacto de los ingresos de un tiempo de actividad mejorado en el endpoint debido a un menor número de interrupciones.
- **Más de 40 000 USD:** menos incidentes relacionados con la seguridad ahorraron productividad de IT al reducir la necesidad de volver a crear imágenes de los endpoints.
- **Más de 800 000 USD:** la gestión facilitada de varias soluciones de seguridad a través de la consola de gestión centralizada permitió ahorrar en productividad.
- **Más de 800 000 USD:** un aumento importante de la postura de seguridad general redujo la posibilidad de una brecha de seguridad "importante".
- **Más de 200 000 USD:** el ahorro de costes asociado a la migración a Kaspersky.

Beneficios (en tres años)



Las entrevistas de Forrester con los clientes existentes y el posterior análisis financiero encontraron que una organización basada en estas organizaciones entrevistadas experimentaría beneficiosde 2,8 millones de USD en tres años frente a los costes de más de 500 000 USD, sumando un valor actual neto (VAN) de 2,3 millones de USD y un retorno de la inversión del 441 %.

Resumen financiero



7 The total Economic Impact™ de Kaspersky Security Solutions, un estudio encargado realizado por Forrester Consulting en enero de 2020

8 "Sorting out a Digital Clutter", Kaspersky, 2019

En resumen,

La protección de endpoints es vital para mantener la seguridad de su organización en el panorama actual de amenazas. Y la mejor manera de proteger sus endpoints es una solución de varios niveles que utiliza diferentes técnicas para detectar y responder a las amenazas de forma altamente automatizada, al tiempo que permite la entrada de datos humanos para tareas más complicadas y decisiones importantes.

La solución integrada Endpoint Security de Kaspersky se ha diseñado específicamente para satisfacer las necesidades de las organizaciones de protección contra amenazas generales, amenazas avanzadas y complejas y errores humanos mediante:

- implementación de una estrategia de **protección, detección y respuesta integrada en varios niveles**
- **automatización** de las defensas, reduciendo el tiempo y el esfuerzo necesarios para responder incluso a ataques dirigidos y avanzados
- obtención de los **índices de detección más altos**
- fomento de una **cultura cibersegura a través de controles y concienciación sobre la seguridad**
- garantía de un **retorno sustancial de su inversión**

Todo esto significa que puede disfrutar de los más altos niveles de seguridad incluso frente a las ciberamenazas más complejas sin necesidad de dedicar valiosos recursos.

Para obtener más información sobre cómo Integrated Endpoint Security puede ayudar a proteger a su empresa frente a ataques complejos sin ejercer presión sobre sus recursos, visite nuestro sitio web.

www.kaspersky.es