Solución integrada para la seguridad de endpoints

Cómo construir defensas sólidas con recursos limitados

kaspersky

Obtenga más información en kaspersky.com
#bringonthefuture

Introducción

Ahora, la mayoría de las empresas, independientemente de su tamaño, ubicación o disciplina, comprenden que cuando se trata de un ciberataque, la pregunta no es si ocurrirá, sino cuándo. Ahora nadie debería considerarse inmune.

Pero contar con el tiempo, los recursos o (para ser sinceros) la motivación para navegar con eficacia el panorama actual de amenazas y seguridad, bueno, esa es otra cuestión.

La mayoría de los analistas de seguridad de la información, y no hay suficientes para cubrir todas las necesidades, están saturados de trabajo. Cuidar de los nuevos empleados y sus dispositivos, comprender nuevas leyes y problemas de cumplimiento, y leer sobre las amenazas más recientes, todo esto debe abordarse antes de llegar realmente al asunto principal de la protección corporativa.

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

Aquí es donde entran los proveedores de ciberseguridad, junto con sus productos y soluciones. Nuestro trabajo es ayudarle a proteger completamente su infraestructura y mantener a sus usuarios seguros con el menor gasto posible en términos de recursos, incluyendo tiempo y dinero, así como experiencia costosa y difícil de obtener.

Los desafíos

Primero, demos un vistazo a algunos de los problemas que enfrentan la TI y los administradores de seguridad de TI actualmente.

El 91%[1] de empresas han sufrido por lo menos un ataque en el transcurso de un año.

1 de cada 10[1] empresas se enfrentaron a un ataque dirigido (hasta donde saben) durante el mismo periodo.

El 30%[1] de las empresas aún no han implementado completamente el software antimalware

Aumento en la amenaza de recibir un ataque avanzado o dirigido

Los ataques dirigidos y las amenazas complejas son un gran problema y están en aumento. Las herramientas de los cibercriminales están volviéndose tan baratas y accesibles que ahora básicamente cualquier persona que tenga una computadora puede lanzar un ataque avanzado. Esto significa que las empresas que alguna vez creyeron que estaban "fuera del radar" en términos de amenazas avanzadas, están descubriendo de la manera difícil que las cosas han cambiado.

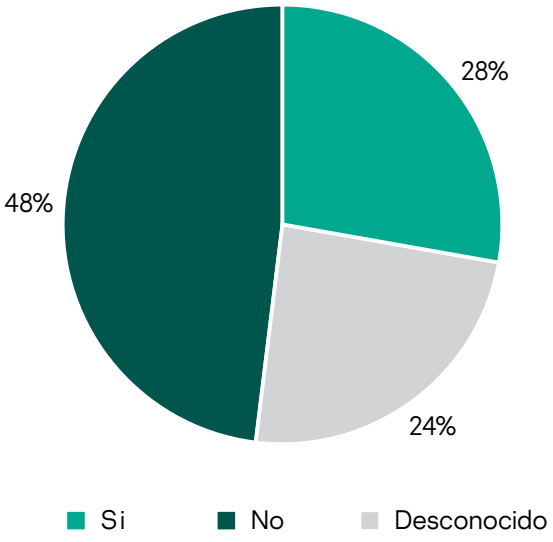
Es decir, las amenazas a los productos básicos también siguen siendo un problema. Actualmente, el enorme volumen de estas es un gran problema en el mundo.

La gran mayoría de las ciberamenazas entran por los endpoints o están diseñadas para activarse allí (o ambos casos).

Entonces, una de las mejores maneras de proteger sus activos es proteger sus endpoints.

Según un estudio del instituto SANS2, el 28% de las empresas encuestadas han tenido endpoints accedidos por los atacantes, y el 24% no sabe si fueron vulnerados.

Tasas de compromiso de endpoint



1 Informe global de riesgos de TI de Kaspersky, Kaspersky, 2019

2 Encuesta de SANS 2019 sobre los riesgos y protecciones para endpoints de última generación, The SANS Institute, 2019

3 Estudio sobre la fuerza de trabajo en la ciberseguridad, (ISC)2 2019,

4 Informe oficial anual de empleos en ciberseguridad, Empresas dedicadas a la ciberseguridad en el 2019

Error humano

Desafortunadamente, el componente más vulnerable en la infraestructura de cualquier empresa se encuentra estrechamente vinculado a la mayoría de sus endpoints: el usuario. Sus usuarios pueden acceder regularmente a sus datos empresariales de forma remota y en sus propios dispositivos, y muchos crecieron interactuando en línea, adquiriendo malos hábitos y demasiada confianza en el camino. Y ellos, así como todo lo demás, también deben mantenerse a salvo.

Por lo tanto, detectar y prevenir comportamientos inseguros en los complejos entornos de TI actuales se convierte en otro trabajo para el especialista en seguridad, que ya de por sí se siente presionado.

Y los profesionales de TI también pueden cometer errores, después de todo somos humanos, que pueden atraer ataques, por ejemplo, mediante vulnerabilidades en los dispositivos personales o de la empresa que tengan parches irregulares.

2 de cada 3[3] empresas experimentan una falta de personal en seguridad de la información.

Se espera que para el 20213.5 millones[4] de trabajos de ciberseguridad no se completarán.

Recursos y la falta de ellos

Entonces, claramente el especialista de TI tiene mucho que hacer.

Incluso para las empresas más pequeñas, hay un volumen cada vez mayor de eventos de seguridad que deben evaluar, analizar y responder a diario, lo cual es difícil de hacer de manera eficiente y oportuna. Los cibercriminales saben que las empresas tienen dificultades con ello y se aprovechan al máximo.

E incluso para aquellos que tienen la suerte de contar con bastante presupuesto, hay una escasez global de profesionales capacitados en ciberseguridad. Este problema no es nuevo, pero de acuerdo con la cantidad de especialistas que se capacitan cada año, no desaparecerá pronto.

Mantener felices y enfocados a sus especialistas de seguridad en estas circunstancias, o simplemente mantenerlos, resulta un desafío. El agotamiento es un gran problema, especialmente si su equipo alta y costosamente capacitado pasa todo el día lidiando con tareas rutinarias.

Además, por supuesto, está el problema de los recursos financieros. Y la potencia del procesador. Y todo lo que se necesita para optimizar su seguridad sin afectar la velocidad del procesamiento, la productividad de los empleados, la satisfacción del usuario o los presupuestos.

La solución

Entonces, ¿cuáles son las respuestas?

Protección eficaz

En primer lugar, todo se basa en la protección eficaz de los endpoints y una Plataforma de protección de endpoints (EPP) sólida, es así de simple. La prevención de las amenazas a nivel de endpoints antes de que puedan desencadenar alertas, reduce el estrés en los recursos, reduce el riesgo de que un ataque tenga éxito y ayuda a que la empresa funcione sin problemas y de forma segura. Esto aplica tanto en los ataques a los productos básicos, que ocurren la mayor parte del tiempo, como a los ataques más complejos, e incluso a los dirigidos, que tienen más probabilidades de lograr el éxito y causar mayor daño.

Nuestro enfoque recomendado es una combinación de defensas de varias capas de los endpoints – una sólida protección de referencia contra amenazas a los productos básicos y defensas polifacéticas en capas contra las amenazas más recientes y complejas.

Además, es importante recordar que algunas amenazas están diseñadas específicamente para evadir a las EPP, y para ello deben utilizarse diferentes métodos de detección, como elsandboxing automatizado.

La EDR (detección y respuesta de endpoints) proporciona la siguiente capa de seguridad esencial. La EPP proporciona identificación y protección iniciales, mientras

que la EDR ofrece visibilidad y opciones de análisis más profundas, lo cual permite ver cómo comenzó el ataque y en qué etapa se encuentra en este momento. Además de la detección, la EDR también ofrece varias opciones de respuesta, de modo que la amenaza descubierta puede contenerse de manera rápida y eficaz.

La EDR solo puede ser eficaz en combinación con una base de protección sólida. Entre más incidentes pueda evitar su solución EPP, menos tendrá que lidiar con su solución EDR y podrá concentrar más recursos en ello.

Abordar el comportamiento humano

Desde la perspectiva del usuario, una de las mejores formas de evitar errores humanos es, por supuesto, eliminar las oportunidades y tentaciones mediante controles de **aplicaciones, web y dispositivos.** Los controles eficaces, lejos de actuar como una restricción para las empresas, en realidad pueden aumentar la productividad, ya que bloquean por ejemplo el desperdicio de tiempo, los sitios web de entretenimiento y las redes sociales potencialmente peligrosas.

Pero aquí, la educación del usuario realmente es la clave. Los c**onocimientos adecuados sobre ciberseguridad** pueden causar un profundo efecto en el comportamiento de los empleados, cambiando la cultura empresarial, reduciendo significativamente el riesgo de la empresa y reduciendo drásticamente la carga de trabajo del departamento de TI.

El retorno de su inversión

Finalmente, cualquier enfoque debe ser capaz de justificarse financieramente en términos del ROI y funcionar ahora y en el futuro en entornos que tengan recursos limitados, lo cual puede incluir experiencia limitada de especialistas en seguridad.

Automatización y optimización

En vista del creciente volumen de amenazas y la escasez de especialistas en seguridad disponibles para trabajar en ellas, **la automatización de las tareas de seguridad,** donde sea posible, se vuelve esencial. Esto permite que sus especialistas en seguridad utilicen su valioso tiempo y habilidades para hacer frente a los incidentes que realmente requieren aportes humanos y experiencia (y como resultado, los mantiene más felices y motivados).

La automatización de las tareas también elimina el riesgo de error humano. Priorizar automáticamente e implementar el parcheo de vulnerabilidades del sistema, por ejemplo, es mucho más eficaz que confiar en que los operadores humanos encuentren el tiempo para emprender esta actividad esencial, pero nada emocionante.

La implementación directa y una consola de administración centralizada y simplificada también ahorran tiempo y recursos. Cambiar consolas entre operaciones y buscar comandos no solo toma mucho tiempo y es frustrante, sino que también da entrada a la oportunidad de cometer errores administrativos y omisiones.

Una nota sobre la protección de varias capas

Hemos dicho que cualquier solución destinada a proteger contra todas las formas de ciberamenazas, incluidos los ataques avanzados y dirigidos, debe tener varias capas.

En primer lugar, la solución debe ofrecer u**na protección de endpoints con base sólida**, incluyendo los controles de los endpoints (con capacidades de bloqueo y restricción de aplicaciones, dispositivos y web) y un motor antimalware reforzado. También es preferible contar con funciones automatizadas para la administración de parches y evaluación de vulnerabilidades, con el fin de ahorrar tiempo y esfuerzo al personal de TI para llevar a cabo tareas rutinarias.

Pero con el malware avanzado se plantean desafíos adicionales que requieren más capas de seguridad. El malware puede estar diseñado específicamente para evitar incluso los mecanismos de detección en los endpoints más sofisticados, y permanecer oculto y latente hasta que surja la oportunidad correcta para su ejecución. La respuesta es persuadir al malware para que se revele a sí mismo y se active en un ambiente seguro y controlado. Aquí es donde interviene un **sandbox**, el cual preferiblemente debe ser capaz, no solo de detectar, sino de responder ante las amenazas de una manera altamente automatizada.

La detección de comportamientos complejos en los endpoints también es el enfoque de la **EDR**. Al igual que la EPP, la EDR idealmente debe combinar la automatización con las herramientas y la visibilidad para ser compatible con la aportación humana cuando sea necesario. El oficial de seguridad debe ser capaz de realizar un análisis de la causa raíz de los incidentes y responder ante las amenazas de manera oportuna, de forma manual o utilizando opciones con respuestas automatizadas.

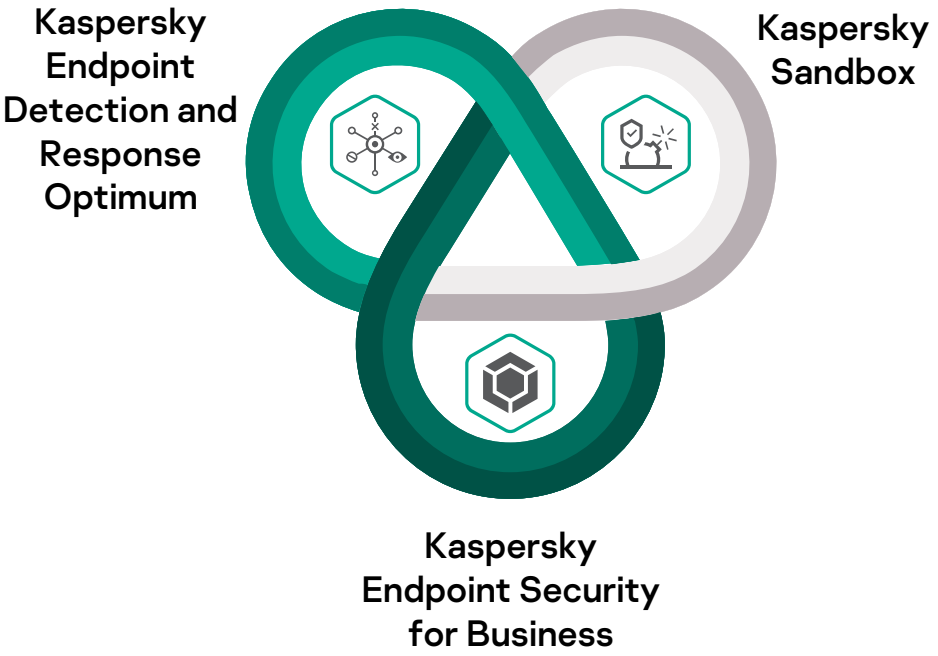
Al unir las tecnologías EPP, Sandbox y EDR, el malware de productos básicos puede abordarse de manera rápida y eficaz, limita las oportunidades de que ocurran errores humanos y reduce el riesgo de sufrir un ataque avanzado o dirigido exitoso, detectando y respondiendo incluso ante amenazas nuevas, desconocidas y de día cero.

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

La solución de Kaspersky

Todos los problemas que se mencionaron anteriormente se resuelven de manera óptima mediante la solución de seguridad integrada para endpoints de Kaspersky, una solución altamente automatizada que incluye protección y controles para endpoints, un sandbox automatizado y EDR integrados. Estos tres componentes trabajan en conjunto desde la base de una EPP sólida. Demos un vistazo más detallado a cada componente, ya que ofrecen más incluso que la resolución de los problemas que se describieron anteriormente.

Sólida protección de referencia para endpoints



Kaspersky Endpoint Security for Business está bien establecido como un proveedor de EPP extraordinariamente sólido (que incluye la protección contra ransomware y ataques sin archivos) utilizando el motor antimalware con más experiencia y reconocimiento del mercado.

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

- Nuestro reconocido motor antimalware, mejorado con aprendizaje automático
- Detección del ransomware
- Detección del comportamiento con reversión automática, el cual identifica y bloquea las amenazas avanzadas, incluyendo el malware sin archivos y la toma de control de la cuenta de administrador, y revierte cualquier cambio que se haya realizado.
- Prevención de vulnerabilidades
- Defensas contra amenazas para dispositivos móviles e integración de EMM
- Prevención contra intrusos basada en el host (HIPS)
- Firewall y administración del firewall en el sistema operativo
- Inteligencia contra amenazas automatizada (Kaspersky Security Network)
- Cifrado, incluyendo la administración del cifrado integrada en el sistema operativo
- Asesor de políticas de seguridad - Modificaciones optimizadas para la supervisión de las configuraciones de seguridad
- Administración de parches y evaluación de vulnerabilidades
- Instalación de sistemas operativos y software de terceros
- Integración de sistemas SIEM

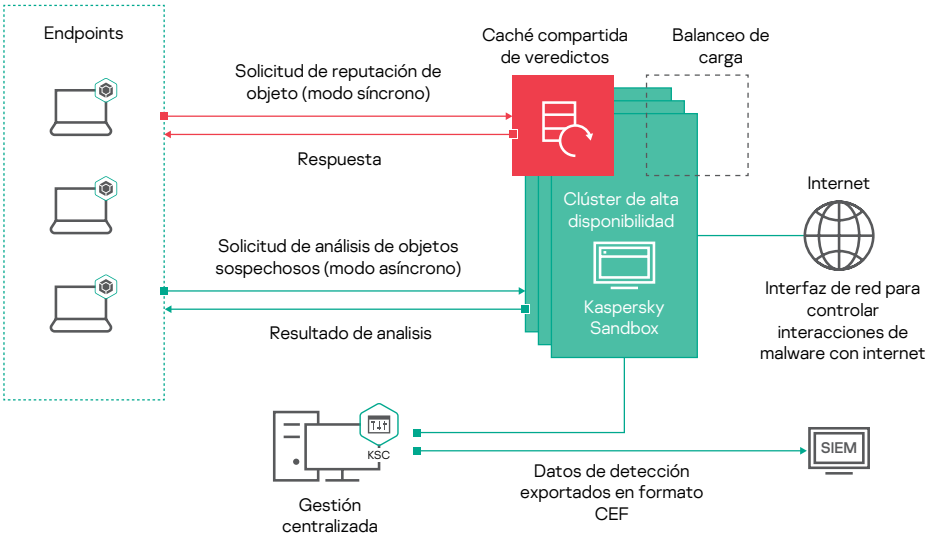
Fortalecimiento de los sistemas y mitigación de errores humanos, proporcionados mediante controles que incluyen:

- Control de aplicaciones con listas blancas basadas en categorías
- Control adaptativo de anomalías que supervisa y bloquea acciones sospechosas que no son típicas de las computadoras en la red de una empresa
- Control de dispositivos – controla y bloquea los complementos de dispositivos externos
- Control web – bloquea o restringe el acceso a sitios potencialmente peligrosos, que hacen perder el tiempo o que son inapropiados

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

Sandbox automatizado

La solución Kaspersky Sandbox detecta y responde automáticamente ante las amenazas que fueron diseñadas para evitar la protección de endpoints, sin necesidad de que haya intervención humana.



Flujo de trabajo de Kaspersky

Los objetos que se escanean son ejecutados por los servidores del espacio aislado y se agrupan en una máquina virtual aislada que simula una estación de trabajo. El componente recibe una solicitud para el análisis del archivo proveniente del agente Kaspersky Endpoint Security for Business que está instalado en la máquina del usuario final, después de lo cual el objeto se pone en fila en uno de los servidores de la agrupación. Cuando el archivo se envía para su procesamiento, Kaspersky Sandbox lo ejecuta y registra todas las acciones que realiza. El componente analiza los datos obtenidos por actividades maliciosas y sospechosas, y devuelve el veredicto al agente de Kaspersky Endpoint Security for Business que solicitó el análisis. El veredicto también se envía al caché operativo, lo cual permite que otros hosts recuperen rápidamente la información sobre el objeto escaneado sin tener que analizarlo de nuevo. Esto reduce la carga en los servidores de Kaspersky Sandbox y mejora el tiempo de respuesta ante amenazas.

Una vez que el archivo es detectado 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 de todas las demás máquinas de la red.

Las técnicas que utiliza Kaspersky Sandbox incluyen:

- Supervisión de la interacción con recursos de Internet
- Carga de módulos
- Modos de escaneo sincrónico y asincrónico
- Técnicas contra la evasión
- Aplicación de diferentes modos de emulación
- Modelado de acciones del usuario
- Generación automática del IoC y escaneo de la infraestructura
- Prevención automática

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

- El 52% de las empresas considera que los empleados son la mayor amenaza para la ciberseguridad empresarial6
- El 60% de los empleados tienen acceso a datos confidenciales en su dispositivo empresarial (datos financieros, bases de datos de correos electrónicos, etc.)
- El 30% de los empleados admiten que comparten con sus colegas los detalles de inicio de sesión y la contraseña de su computadora de trabajo8

6 El costo de una vulneración de los datos, Kaspersky, 2018

* Existen algunas restricciones en el rango de características y funciones que pueden administrarse mediante la consola en la nube. Para obtener toda la información, consulte la ayuda en línea.

EDR optimizado

Kaspersky Endpoint Detection and Response Optimum es un complemento para Kaspersky Endpoint Security for Business que brinda visibilidad completa y la capacidad de aplicar análisis de causa raíz, con el fin de obtener una comprensión completa del estado de las defensas de la empresa contra amenazas avanzadas.

El especialista en seguridad de TI contará con la información y los conocimientos necesarios para llevar a cabo una investigación efectiva y una respuesta rápida y precisa ante los incidentes, antes de que se produzca cualquier daño.

Al trabajar como parte de nuestra solución integrada de Endpoint Security, Kaspersky Endpoint Detection and Response Optimum permite que el análisis de causa raíz pueda llevarse a cabo utilizando:

- Visualización de la ruta de propagación del ataque, que muestra cómo se desarrolló la amenaza en el endpoint
- Información sobre el archivo, incluyendo metadatos, origen del archivo, datos de modificación, firma digital, etc.
- Información sobre el host y el usuario
- Información sobre la detección
- Introducción del proceso
- Arrastre de archivos
- Modificaciones de la clave del registro
- Conexiones

Después de detectar una amenaza, hay varias opciones disponibles de respuestas automatizadas y de "un solo clic", que incluyen:

- Aislamiento del host
- Iniciar un escaneo del host
- Eliminación de archivos (cuarentena)
- Eliminación de procesos
- Impedir que el proceso se ejecute

Para llevar a cabo una mayor investigación, están disponibles funciones como importar lox IoC o generarlos con base en detecciones, y el escaneo para buscar dichos IoC con opciones de respuesta automatizadas preestablecidas.

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

Kaspersky Endpoint Detection and Response Optimum está disponible tanto de forma local como en la nube*.

Control y administración

Todos los componentes de nuestra solución se crean internamente y se administran mediante la misma consola única, y utilizan el mismo agente para endpoints multipropósito. Por lo tanto, la administración diaria es centralizada, directa y eficaz.

Conocimientos sobre seguridad

También ofrecemos productos de capacitación basados en computadora que combinan la experiencia en ciberseguridad con las tecnologías y prácticas educativas más conocidas. Este enfoque cambia el comportamiento de los usuarios y ayuda a crear un entorno de ciberseguridad en toda la empresa.

Kaspersky Security Awareness desarrolla una cultura de comportamiento ciberseguro:

enseñando a los usuarios sobre cuándo alertar a los administradores si hay señales de una amenaza potencial genuina
reduciendo los errores que comete el usuario como resultado de la ignorancia o la ingenuidad
disminuyendo el número de alertas de seguridad que los administradores deben clasificar

Puede seguir el progreso de sus aprendices mediante el sencillo panel de control, que incluye el seguimiento de datos, tendencias y pronósticos en vivo, junto con recomendaciones sobre cómo mejorar sus resultados.

Para obtener más información sobre Kaspersky Security Awareness, visite nuestro čėëüġØÏ

Según un estudio de Forrester, uno de los principales requisitos de las empresas que entrevistaron, es que su solución de seguridad se implemente con poca o ninguna interrupción para los usuarios. Este principio está en el núcleo de la seguridad de endpoints integrada

7 The Total Economic Impact™ de Kaspersky Security Solutions, un estudio encargado realizado por Forrester Consulting, enero del 2020
8 La clasificación de un desastre digital, Kaspersky, 2019

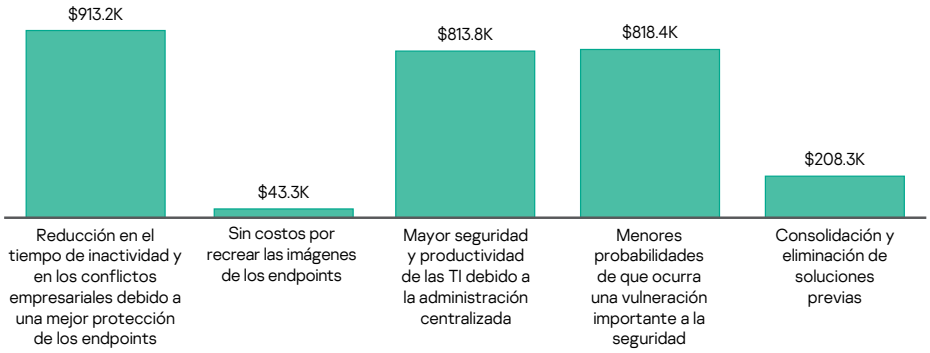
Su ROI

Al igual que con cualquier solución, los costos son tan importantes como los beneficios que ofrecemos. A continuación, se muestra un ejemplo de rentabilidad de la inversión para las soluciones de Kaspersky, el cual está basado en un estudio de Forrester con respecto a una solución de seguridad de Kaspersky que está integrada en Kaspersky Endpoint Security for Business y en Kaspersky Endpoint Detection and Response.

Riesgo ajustado del valor actual (VA) que experimentaron las empresas que fueron entrevistadas para el estudio de Forrester:

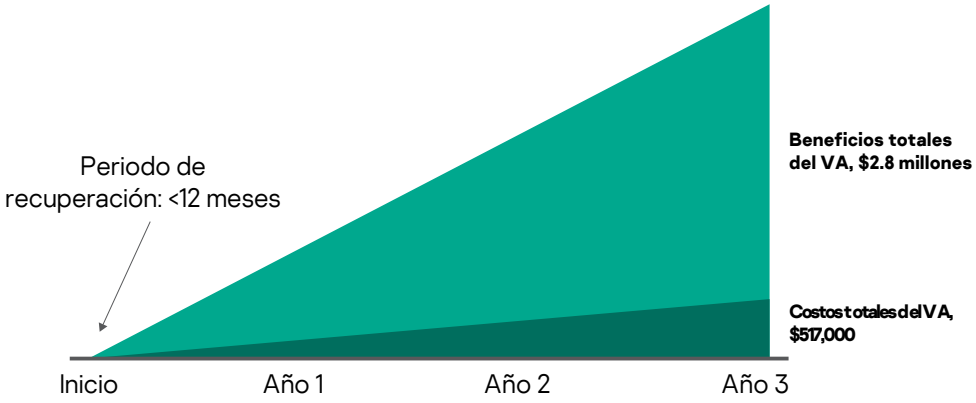
- **Casi $1 millón:** el impacto en los ingresos por la optimización de los tiempos de actividad del endpoint, debido a que ocurren menos interrupciones.
- **Más de $40,000:** ya que ocurren menos incidentes relacionados con la seguridad, lo cual aumenta la productividad de las TI y disminuye la necesidad de recrear imágenes de los endpoints.
- **Más de $800,000:** la administración se simplificó debido a que pueden utilizarse varias soluciones de seguridad mediante la consola de administración centralizada, lo cual propició que aumentara la productividad.
- **Más de $800,000:** hubo una mejora importante en el plan de seguridad general, lo cual redujo la posibilidad de que ocurriera una vulneración "crítica" a la seguridad.
- Más de $200,000: el ahorro en los costos asociados con la migración a Kaspersky.

Beneficios (durante los siguientes tres años)



En las entrevistas que realizó Forrester a los clientes actuales y en análisis financieros posteriores, se encontró que una empresa, según las empresas que fueron entrevistadas, obtendría beneficios por $2.8 millones en el transcurso de los siguientes tres años, en comparación con los costos por más de $500,000, lo cual agrega un valor actual neto (VAN) de $2.3 millones y un ROI del 441%.

Resumen financiero



7 The Total Economic Impact™ Of Kaspersky Security Solutions, a commissioned study conducted by Forrester Consulting, January 2020

8 Sorting out a Digital Clutter, Kaspersky, 2019

En resumen

La protección de endpoints es vital para mantener su empresa segura en el panorama de amenazas moderno. Y la mejor manera de proteger sus endpoints es utilizar una solución de varias capas, que utilice diferentes técnicas para detectar y responder ante amenazas de manera altamente automatizada, y que a la vez permita la contribución humana para llevar a cabo tareas más complicadas y tomar decisiones importantes.

La solución de seguridad integrada de Kaspersky fue diseñada específicamente para resolver las necesidades que tienen las empresas de recibir protección contra amenazas en productos básicos, ataques avanzados y dirigidos, y errores humanos, todo esto mediante:

- la implementación de una estrategia de protección, detección y respuesta integradas de varias capas
- la automatización de sus defensas y la reducción del tiempo y el esfuerzo necesarios para responder incluso ante ataques dirigidos y avanzados
- la obtención de tasas de detección más altas
- el fomento de una cultura de ciberseguridad mediante controles y conocimientos en seguridad
- la garantía de un retorno sustancial de su inversión

Lo anterior significa que podrá disfrutar de los niveles más altos de seguridad, incluso contra las ciberamenazas más complejas, sin tener que utilizar recursos valiosos.

Para obtener más información sobre cómo seguridad de endpoints integrada puede ayudar a proteger su empresa contra ataques complejos sin ejercer presión sobre sus recursos, visite nuestro sitio web.

www.kaspersky.com