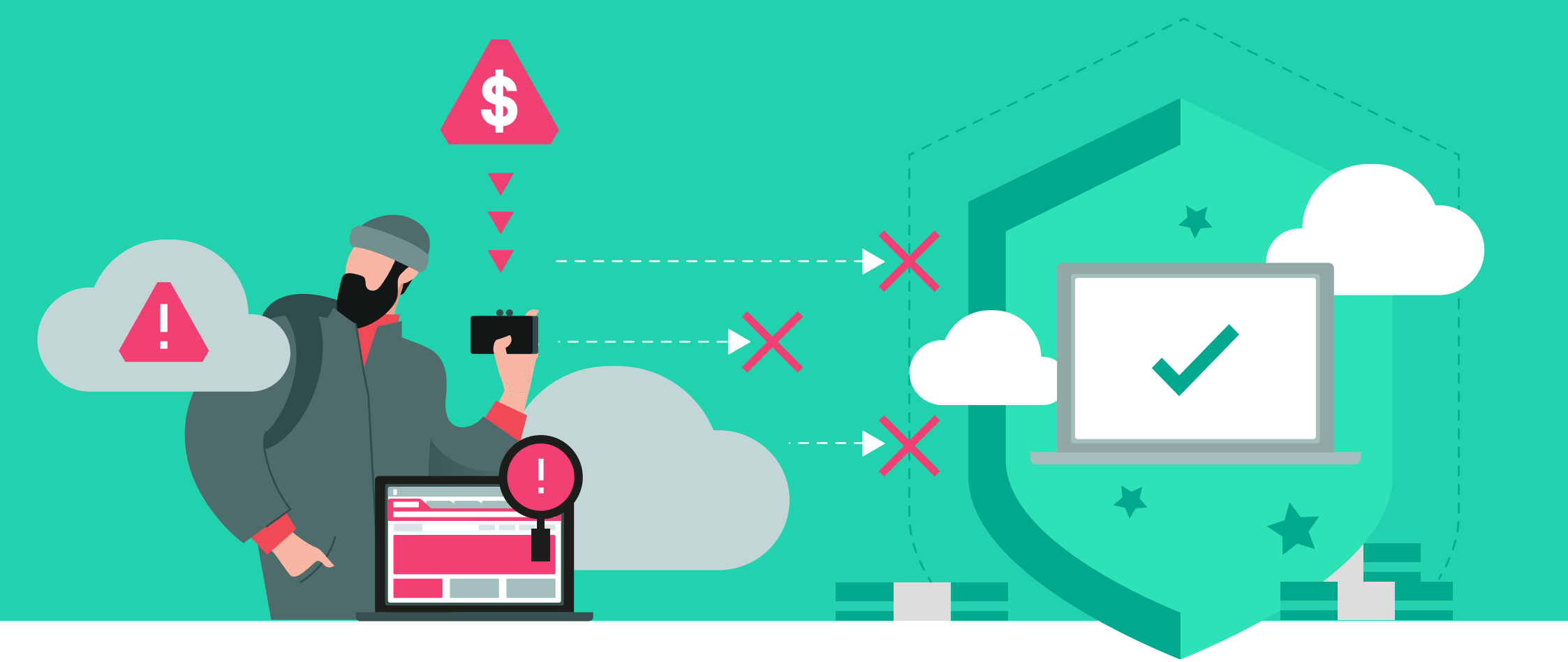
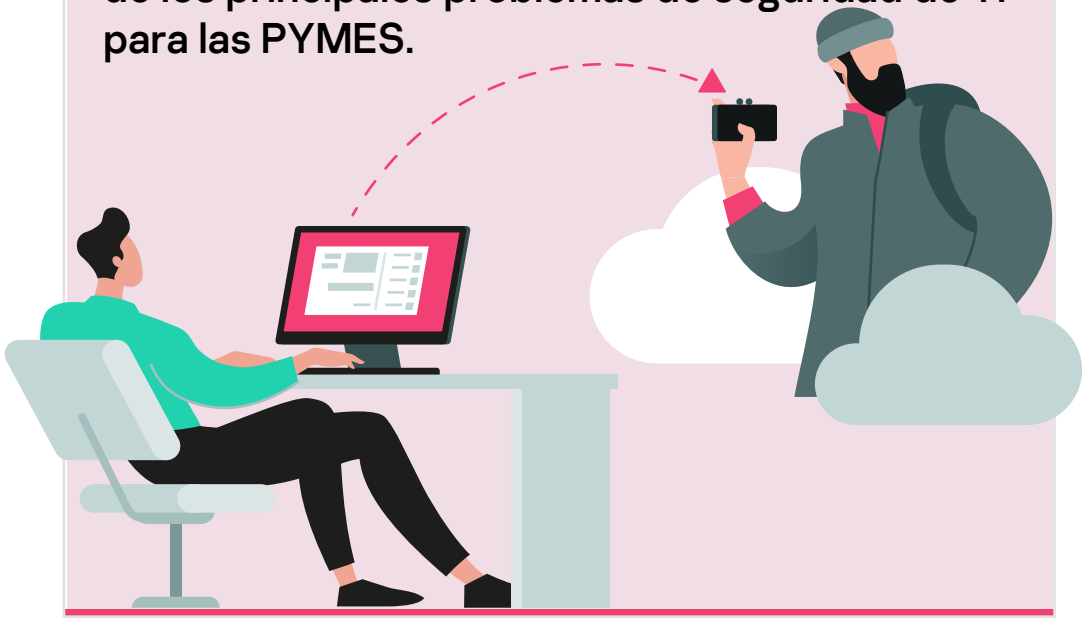


¿Por qué elegir la protección de Kaspersky contra el Ransomware?

kaspersky

El Problema

El ransomware ha sido una amenaza persistente y en constante evolución durante el 2020. Los ataques de ransomware se han vuelto más riesgosos, mucho más dirigidos contra sectores comerciales e industrias específicas, y generan rescates más costosos. Los perjudiciales costos por tiempo de inactividad han aumentado exponencialmente y el número de nuevas familias de ransomware con participantes no identificados es cada vez mayor, lo cual convierte al ransomware en uno de los principales problemas de seguridad de TI para las PYMES.



La Solución

La mejor protección de endpoints de Kaspersky está diseñada especialmente para enfrentar los desafíos del 2020 y los años por venir, ya que incorpora herramientas anti-ransomware para la detección de comportamientos asistidos por la nube, escanea y bloquea el ransomware y el malware de cifrado, protege las cargas de trabajo en la nube, los endpoints físicos y virtuales y las redes compartidas, y revierte los archivos afectados a su estado previo al cifrado.

El 2020 en cifras

$ 40 mil millones

COSTO GLOBAL ESTIMADO

de la demanda por ransomware y tiempo de inactividad en el 2020.[1]

23x

MAYORES COSTOS DE INACTIVIDAD

que el promedio de las solicitudes de rescate, según la encuesta.[2]

$ 141,000

EL COSTO PROMEDIO DEBIDO AL TIEMPO DE INACTIVIDAD OCASIONADO POR EL RANSOMWARE

en el 2019 (hubo un incremento del 200% comparado con el 2018).[3]

[1] Demandas por ransomware: $170 mil millones de dólares previstos a nivel mundial en el 2020, informe

[2] Informe de Datto sobre el estado global del canal del ransomware en el 2019

[3] Help Net Security: 1 de cada 5 PYMES han sido víctimas de un ataque de ransomware

62.4%

EMPRESAS VÍCTIMAS DEL RANSOMWARE

según la encuesta aplicada a los responsables de tomar decisiones de TI a nivel mundial en el 2019.[4]

30%

DE LOS OBJETIVOS DEL RANSOMWARE EN EL ÚLTIMO AÑO

son usuarios empresariales.[5]

20%

DE LAS PYMES FUERON VÍCTIMAS

de un ataque de ransomware en el 2019, según la encuesta[9]

[4] Statista: Porcentaje de empresas que fueron víctimas de ataques de ransomware en todo el mundo entre el 2017 y el 2019

[5] Uno de cada tres ataques de ransomware tiene como objetivo a los usuarios empresariales: Kaspersky y la INTERPOL piden copias de seguridad y protección en el Día Anti-Ransomware

[6] Uno de cada tres ataques de ransomware tiene como objetivo a los usuarios empresariales: Kaspersky y la INTERPOL piden copias de seguridad y protección en el Día Anti-Ransomware

21%

% DE WANNACRY DEL AÑO PASADO

de todos los ataques de ransomware detectados.[6]

22

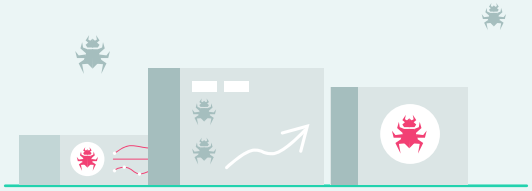
NUEVAS FAMILIAS DE RANSOMWARE

más de 46 hicieron su aparición, 156 modificaciones a cifradores.[7]

49%

DE LOS ATAQUES DE RANSOMWARE DETECTADOS EN EL PRIMER TRIMESTRE DEL 2020

son ransomware de cifrado.[8]



[7] Boletín de seguridad de Kaspersky 2019. Estadísticas

[8] Informe de KSN: Ransomware 2018-2020

[9] Informe de Datto sobre el estado global del canal del ransomware en el 2019

Las soluciones de ciberseguridad de Kaspersky proporcionan una protección demostrada contra el ransomware, tanto en la distribución como en la fase de ejecución del malware, con ayuda de sofisticadas tecnologías de protección multicapa.

EDR automatizado

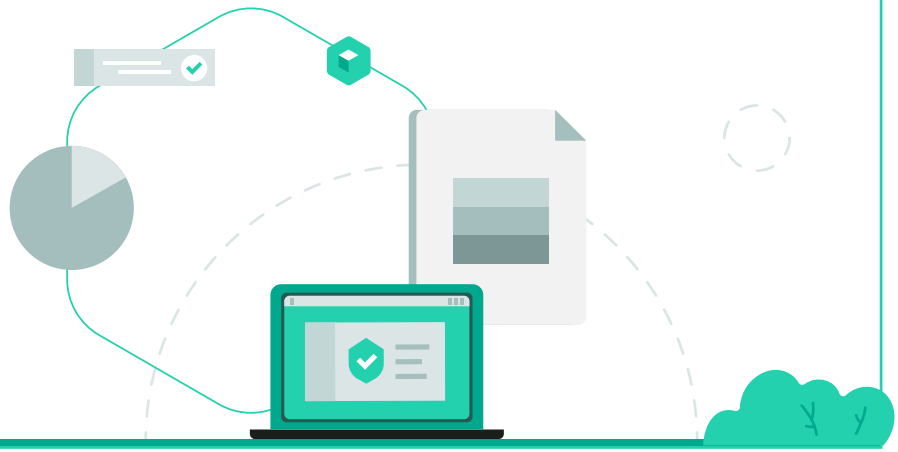
Kaspersky Endpoint Detection and Response proporciona tanto una visibilidad integral de la red como una defensa sofisticada, las cuales automatizan las tareas para descubrir, priorizar, investigar y neutralizar el ransomware y otras amenazas complejas. El EDR implementa métodos “intensivos” de detección (espacio aislado, modelos de aprendizaje profundo, correlación de eventos) además de herramientas para expertos en investigación de incidentes, búsqueda proactiva de amenazas y respuesta ante ataques.

Prevención de vulnerabilidades

La prevención de vulnerabilidades de Kaspersky detiene la penetración del malware (incluyendo el ransomware) causada por vulnerabilidades del software. El componente aplica el análisis de seguridad del comportamiento contra patrones maliciosos, desencadenado por acciones sospechosas. Incluye firmas especiales para el malware que aprovecha vulnerabilidades, lo cual permite la detección de archivos maliciosos antes de que sean abiertos. La protección proactiva permite la detección y el bloqueo de malware cuando se abre un archivo.

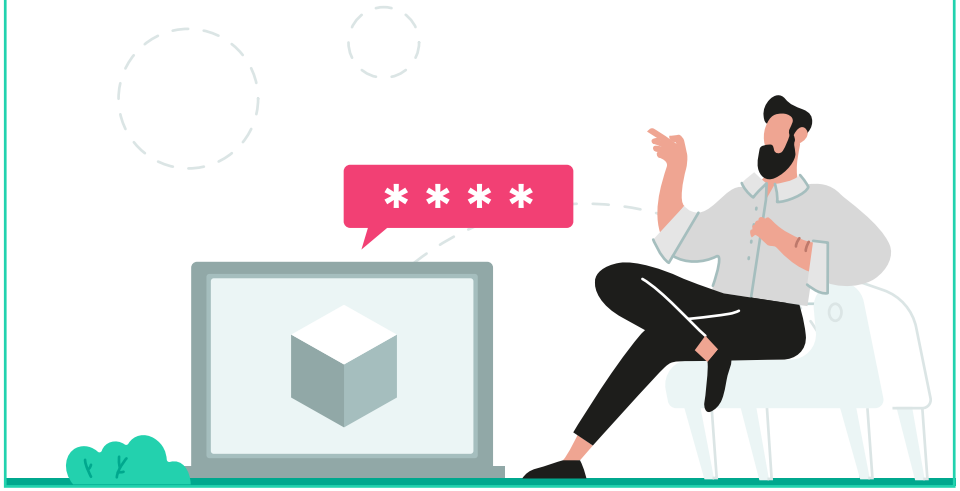
Detección del comportamiento habilitado por el aprendizaje automático (con reversión automática)

Las tecnologías de Kaspersky basadas en el aprendizaje automático detectan amenazas de malware anteriormente desconocidas (incluyendo el ransomware), “aprenden” de la inteligencia de seguridad relevante del Big Data y construyen modelos de detección efectivos, tanto en entornos locales como en los procesos de análisis de amenazas efectuados en laboratorio, aprovechando varias capas de seguridad. Kaspersky Anti-Ransomware Tool intenta revertir automáticamente las aplicaciones maliciosas (por ejemplo, restaurando los archivos modificados y el registro del sistema).



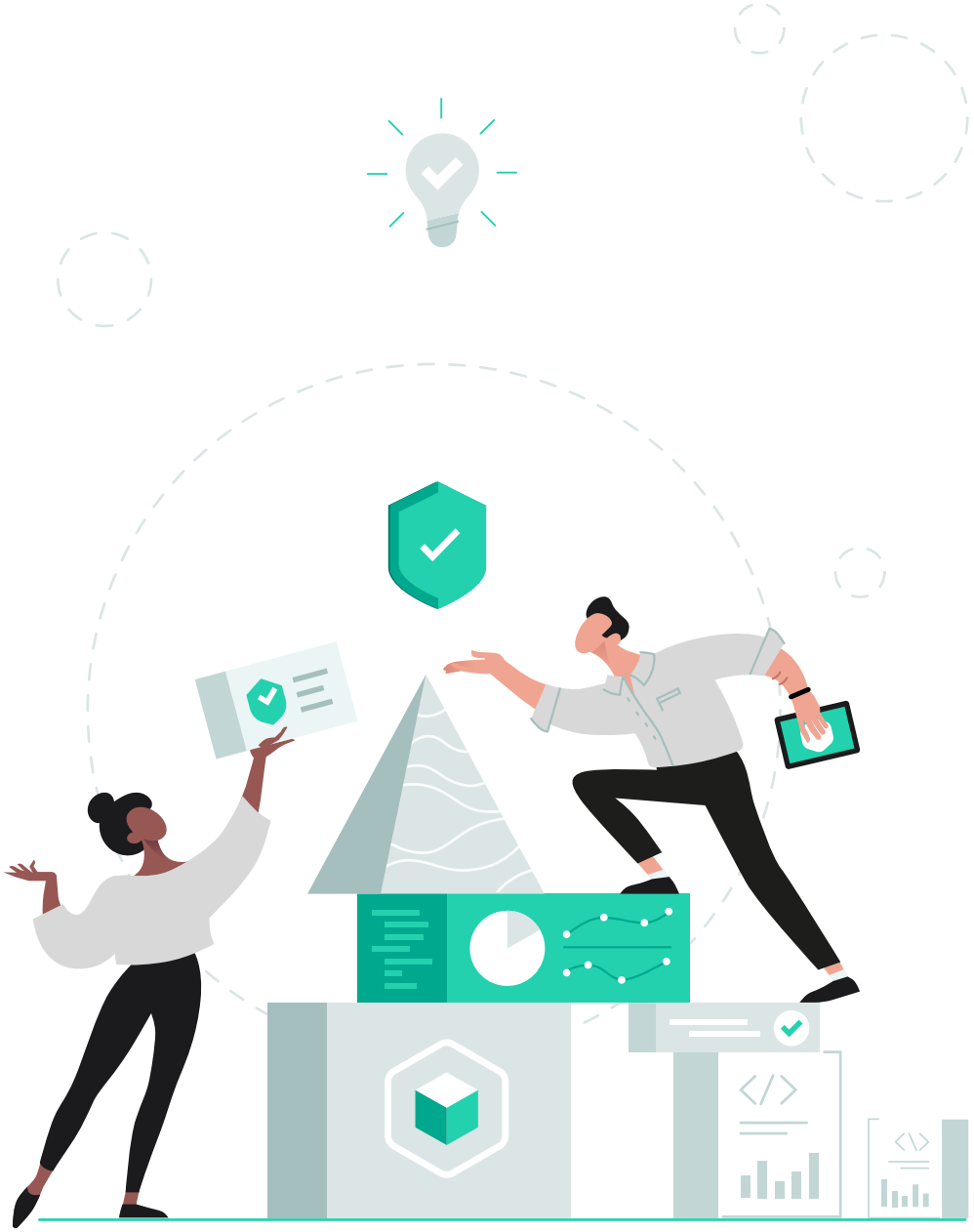
Administración del cifrado

El ransomware es un malware que cifra los archivos de la víctima. La administración del cifrado de Kaspersky configura el cifrado de los dispositivos administrados que funcionan con Windows y macOS, lo cual evita que los usuarios no autorizados obtengan acceso sin permiso a los datos almacenados. El cifrado de disco completo evita la filtración de los datos causada por la pérdida de un dispositivo. El cifrado a nivel de archivo protege los archivos que se transfieren a canales no confiables, y Crypto Disk almacena los datos del usuario cifrados en un archivo separado.



Administración de parches y evaluación de vulnerabilidades

La evaluación de vulnerabilidades y la administración de parches de Kaspersky evita que el malware, incluido el ransomware, aproveche las vulnerabilidades recientemente descubiertas y sin parches en los sistemas operativos y en las aplicaciones comunes. Permite detectar fácilmente el software vulnerable en cualquier endpoint mediante la automatización de la evaluación de vulnerabilidades, la distribución de parches y actualizaciones y la implementación de aplicaciones desde una sola consola de administración integrada.



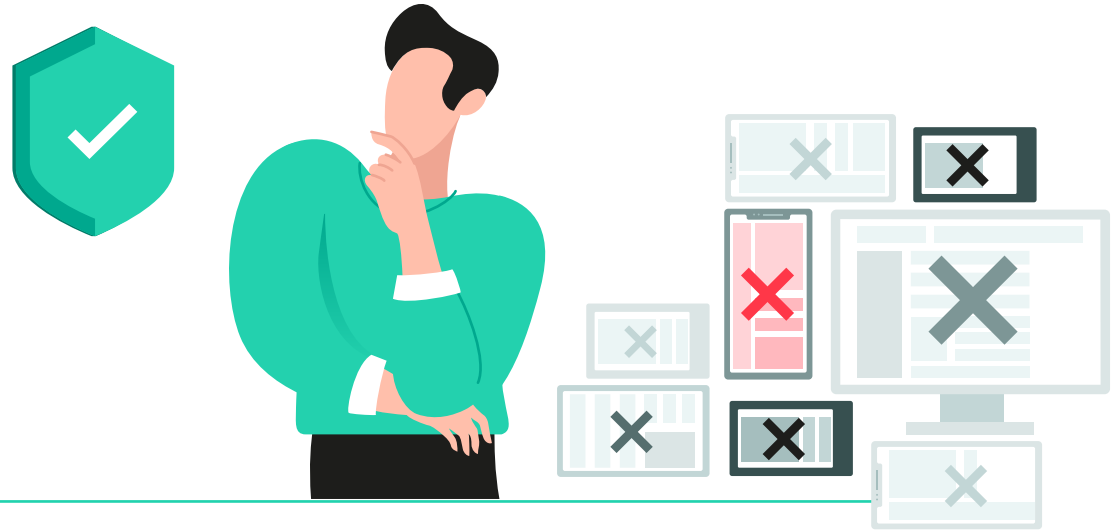
Aunque las cifras absolutas de los ataques de ransomware han disminuido en los últimos 12 meses, el impacto negativo de un ataque exitoso de ransomware a las empresas, debido a una combinación del costoso tiempo de inactividad, consecuencias negativas en la reputación y pagos de rescates, se han intensificado exponencialmente. El ransomware sigue siendo una de las ciberamenazas más temidas a las que se enfrentan empresas de cualquier tamaño y sector.

Cómo proteger los dispositivos contra el ransomware

- ✓ Las copias de seguridad deben estar listas regularmente para acceder a ellas en caso de emergencia.
- ✓ Utilice herramientas que puedan detectar automáticamente vulnerabilidades y descargue e instale los parches.
- ✓ Mantenga siempre actualizado el software y los sistemas operativos en todos los dispositivos.
- ✓ Manténgase constantemente atento ante ataques de phishing, mensajes y enlaces falsos, y archivos potencialmente maliciosos.
- ✓ Capacite a los empleados. Tome el curso de capacitación sobre cómo recibir asistencia de Kaspersky Automated Security Awareness Platform
- ✓ Instale un sistema de ciberseguridad de varias capas muy bien evaluado, como Kaspersky Endpoint Security for Business, o para dispositivos personales, como Kaspersky Security Cloud, para protegerse contra el malware de cifrado de archivos y revertir los cambios realizados por aplicaciones maliciosas.

Qué puede hacer si sus datos fueron infectados por ransomware

- ✓ Interrumpa la conexión a Internet.
- ✓ Como regla general, no pague. Un tercio de las víctimas no recuperan el acceso a los datos después de hacer el pago.
- ✓ Obtenga ayuda técnica de inmediato para recuperar sus datos.
- ✓ Póngase en contacto con la iniciativa No More Ransom para obtener recursos que incluyen más de 100 herramientas de descifrado gratuitas.



No deje sus dispositivos vulnerables a las infecciones de ransomware

Instale GRATUITAMENTE Kaspersky Anti-Ransomware Tool Gy aproveche sus funciones de vanguardia, como la detección del comportamiento asistida por la nube, para escanear y bloquear inmediatamente ataques de ransomware y malware de cifrado. Nuestra herramienta cumple con las regulaciones del RGPD y funciona en conjunto con la mayoría del software de seguridad.

Kaspersky Anti-Ransomware Tool no es el único producto de Kaspersky que cuenta con un historial ganador. Las soluciones de ciberseguridad de Kaspersky han demostrado ser consistentes en pruebas independientes:

LA PROTECCIÓN CON MÁS EXPERIENCIA Y RECONOCIMIENTO DEL MUNDO

86
EVALUACIONES/PRUEBAS REGISTRADAS

64
PRIMEROS LUGARES

81%
TRES PRIMERAS POSICIONES

Descubra los beneficios de las tecnologías de próxima generación de Kaspersky para obtener una protección integral con Kaspersky Endpoint Security for Business. . Proteja varios endpoints, dispositivos móviles y servidores de archivos, de forma remota y desde cualquier lugar, con Kaspersky Endpoint Security Cloud.

kaspersky