

# La carrera contra el Ransomware

El camino comprobado para una seguridad efectiva

## Ransomware

Un obstáculo en el camino que llegó para quedarse

Mientras que nuevos tipos de ataques, como el cryptomining han entrado en la carrera, el ransomware sigue siendo el mayor obstáculo para las empresas. Conozca cómo los clientes de Cisco han mantenido la delantera ante este tipo de amenazas.

"Redujimos el tiempo para detectar amenazas por más de un mes con Cisco Email Security."<sup>1</sup>  
— Muscogee County School District<sup>2</sup>

La alerta y preocupación que generan los ataques de ransomware de gran escala como NotPetya, que la Casa Blanca denominó como "el ataque cibernético más destructivo y costoso de la historia", se ha calmado.<sup>2</sup> Sin embargo, la realidad actual del ransomware continúa siendo bastante intimidante.

CADA  
**14**  
SEGUNDOS

Al finalizar el 2019, las empresas serán víctimas de algún tipo de ciberataque cada 14 segundos.<sup>3</sup>

Bienvenidos a la Ciudad de Aspen, Colorado<sup>1</sup>  
Población: 6,658

"Hemos visto una reducción en las infecciones de malware. Pasaron de ser varias a la semana a prácticamente cero [con Cisco Umbrella]."

**\$11.5**  
BILLONES

Se predicen pérdidas de \$11.5 billones a nivel global por daños a causa de ransomware para el 2019.<sup>3</sup>

## Topes a la Seguridad

¿Qué nos está deteniendo?

El crecimiento masivo de dispositivos conectados a Internet, el aumento de nuevas formas de ataque y la escasez de profesionales calificados han contribuido al aumento del ransomware.

Algunas de las más grandes y prestigiosas organizaciones han tenido que detener sus operaciones debido al ransomware en los últimos años.

**69%**

de las organizaciones no creen que sus soluciones de antivirus provean una protección adecuada.<sup>5</sup>

**40%**

Más del 40% de las empresas tienen archivos confidenciales que están desprotegidos y disponibles a todos los empleados.<sup>4</sup>

## Conduciendo hacia adelante:

¿A dónde vamos ahora?

Los sofisticados ciberataques de hoy requieren un enfoque de seguridad completo y en capas. No hay una tecnología única que elimine todos los obstáculos del ransomware.

Al mismo tiempo, lanzar una multitud de soluciones, desconectadas y sin comunicación de unas con otras, tampoco despejará el camino ni resolverá el problema.

Las organizaciones deben pensar en la seguridad de manera más integral y adoptar soluciones que se complementen entre sí y que trabajen juntas para desviar a los atacantes y el malware fuera del camino.

Cisco ofrece un enfoque múltiple de Defensa contra el Ransomware para poner su seguridad a toda marcha.

"Cisco AMP para dispositivos nos ha permitido detectar malware y ransomware que con otros productos antivirus que habíamos usado anteriormente habían pasado por alto".

— Nichiei International<sup>1</sup>

"Cisco AMP para Endpoints aumentó la visibilidad en un 90% en todos los dispositivos endpoint, detectó un 90% más de amenazas y redujo el tiempo de respuesta a incidentes a menos de un día."

— Guardia Nacional de Arabia Saudita

## Cisco prepara el camino

En la carrera contra el ransomware, tener los mejores autos y conductores es vital. Sin embargo, aún pueden ocurrir incidentes, por lo que es bueno contar también con la mejor respuesta dentro de su equipo de pits.

"Hemos tenido cero infecciones desde la implementación de Cisco Umbrella hace tres años."

— Mid-Sized Financial Services Company<sup>1</sup>

## Defensa contra el Ransomware de Cisco



### Cisco AMP

Descubra, contenga y elimine a tiempo malware avanzado, ataques de día cero y amenazas persistentes.



### Cisco Email Security

Evite que el phishing, ransomware y el correo no deseado pongan en peligro su entorno, al bloquear y contener cualquier correo o anexo malicioso



### Cisco Umbrella

Obtenga la primera línea de defensa contra amenazas en Internet, ya sea que los usuarios estén dentro o fuera de la red corporativa



## Prueba de manejo Defensa contra el Ransomware de Cisco

Comenzar



© 2018 Cisco y/o sus filiales. Todos los derechos reservados. Cisco y el logo de Cisco son marcas o marcas registradas de Cisco y/o sus filiales en los Estados Unidos y otros países. Para ver una lista de las marcas de Cisco, visite el siguiente URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Las marcas de terceros mencionadas son propiedad de sus respectivos dueños. El uso de la palabra socio no implica una asociación entre Cisco y cualquier otra compañía.

1. TechValidate, <https://www.techvalidate.com/vendor-research/cisco>. 2. The White House, Statement from the Press Secretary, February 2018. 3. Cybersecurity Ventures, "Global Ransomware Damage Costs Predicted To Hit \$11.5 Billion By 2019," November 2017. 4. TechRepublic, "Report: 41% of companies have 1,000+ sensitive files open to every employee," April 2018. 5. Ponemon Institute, The 2017 State of Endpoint Security Risk, November 2017.