LIBRO ELECTRÓNICO

Proteger los terminales en todas partes

Su primera y última línea de defensa para las amenazas actuales

cisco

Contenido de este libro electrónico:

49%
de la fuerza laboral es móvil.[1]

82%
de los usuarios de computadoras portátiles corporativas eluden las VPN.[2]

70%
de aumento en el uso de SaaS en los próximos 2 años.[3]

68%
de las cargas de trabajo serán en centros de datos de nube pública antes de 2020.[4]

69%
de las sucursales tienen acceso directo a Internet.[5]

La seguridad no puede esperar más; debe evolucionar ahora.

El mundo del trabajo cambió, radicalmente. Con más dispositivos no administrados que se conectan a la red y más usuarios trabajando desde cualquier lugar, las infracciones a la seguridad se están ampliando.

Los equipos de TI tienen menos visibilidad, mientras que los empleados tienen más control que nunca sobre las aplicaciones que usan y dónde las usan. Muchas de esas aplicaciones se trasladaron a la nube, lo que permite a los empleados remotos e itinerantes eludir la VPN. Esas mismas aplicaciones en la nube facilitan la colaboración y el intercambio de información, no solo dentro de su empresa, sino también con colaboradores externos.

Con infraestructura crítica, aplicaciones y datos confidenciales ahora almacenados en la nube, los atacantes tienen aún más incentivos para llegar a los puntos finales como su punto de entrada más fácil. Mientras el ransomware aumenta y más sucursales cuentan con acceso directo a Internet, la pregunta sigue siendo: ¿por qué tratamos los nuevos desafíos de la actualidad con el enfoque a la seguridad del pasado? La seguridad no puede esperar. Es momento de actuar.

"Antes de 2018, Gartner estima que el 25% del tráfico de datos corporativos pasará por alto la seguridad del perímetro y fluirá directamente desde los dispositivos móviles a la nube".

– Predicciones de 2017: Seguridad de red y gateway

La amenaza en los terminales es masiva.

La forma en que trabajamos no es lo único que evolucionó. Las amenazas a la seguridad también cambiaron. En la actualidad, aproximadamente 70% de las violaciones se originan en dispositivos de terminales.[6] ¿Por qué son los terminales el principal punto de entrada de los ataques?

- **Infracciones a la protección.** Cuando los usuarios y los terminales están desconectados de la red, el antivirus suele ser la única protección disponible. Sin embargo, la detección de firmas y las medidas preventivas no son suficientes para manejar las amenazas avanzadas de la actualidad, incluidos los ataques de cero días.

  65% de las organizaciones dicen que los ataques evadieron las herramientas preventivas.[7]

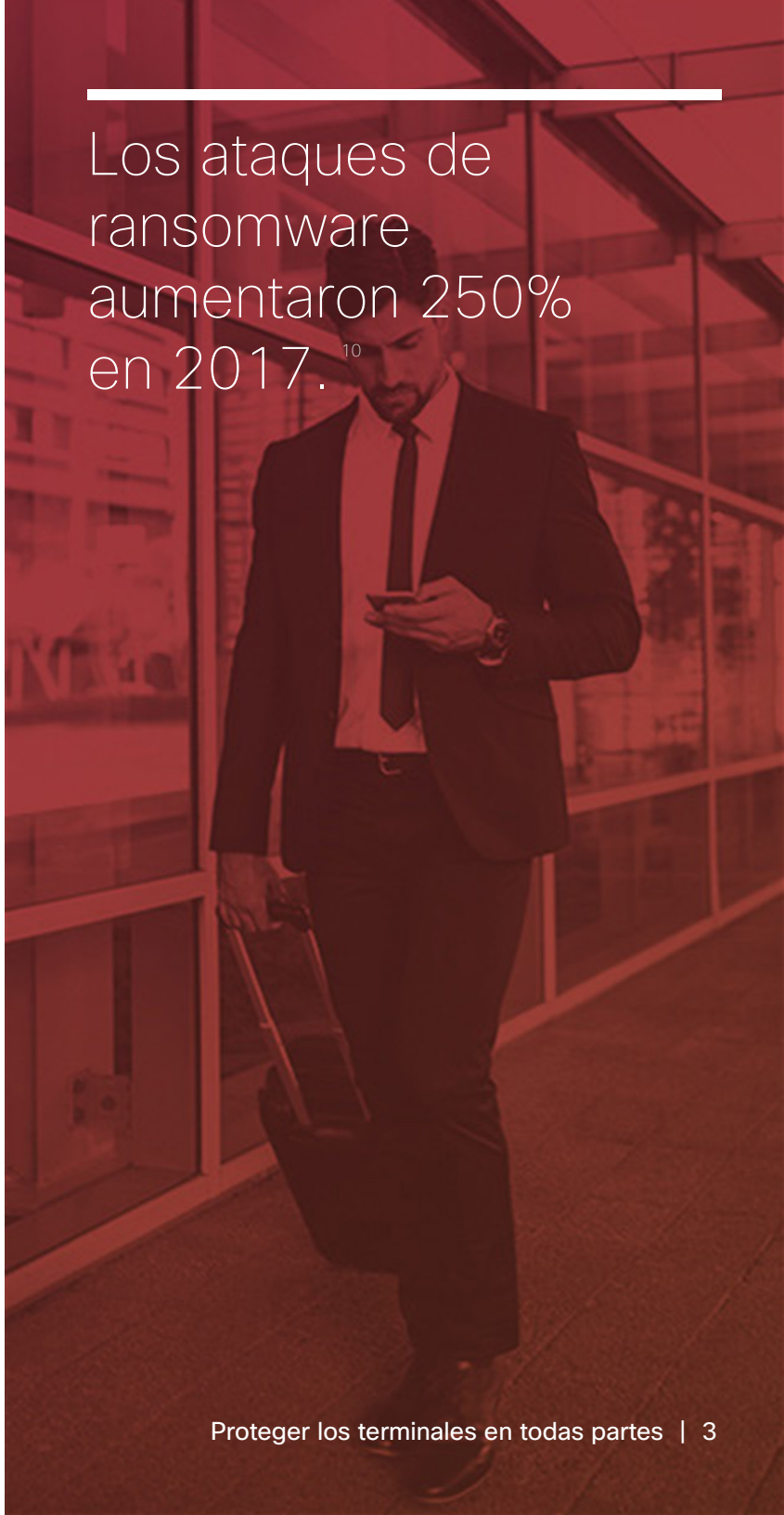
- **Falta de visibilidad.** Las organizaciones tienen una visibilidad limitada de la actividad del usuario y del terminal, y carecen de contexto para ver el malware (de dónde provino, dónde estuvo y qué está haciendo) una vez que llega a un terminal. No se puede detectar lo que no se ve.

  55% de las empresas no pueden determinar la causa de una violación.[7]

  100 días es el promedio del sector para el tiempo de detección.[8]

- **Error del usuario.** Un atacante envía un correo electrónico fraudulento con un archivo adjunto o enlace malicioso. A pesar de la capacitación o las innumerables advertencias, los usuarios hacen clic inevitablemente en cosas que no deberían.

  48% de los atacantes eluden las defensas de los terminales debido a un error del usuario.[9]



Los ataques de ransomware aumentaron 250% en 2017.[10]

Visibilidad, contexto y control para usuarios, archivos e Internet.

Es momento de que la seguridad efectiva sea simple, abierta y automatizada.

Los atacantes son cada vez más inteligentes, más rápidos y más difícil de atrapar. El ransomware en particular se convirtió en una industria de miles de millones de dólares a medida que los ataques dirigidos se vuelven más frecuentes. Y de acuerdo con Gartner, hasta 2020, más del 50% del ransomware se enfocará en la interrupción del negocio en lugar del cifrado de datos.[11]

La evolución de cómo trabajamos y la evolución de las amenazas de Internet se suman a una nueva realidad para TI. Usted ya no puede depender únicamente de las protecciones de nivel de red para mantener sus datos seguros. La seguridad tradicional no puede extender la protección a los usuarios móviles o manejar el aumento exponencial del tráfico de Internet. Los gateways seguros, firewalls y sandboxing son herramientas importantes, pero brindan ayuda solo después de que se produce un ataque.

En la actualidad, usted necesita mayor visibilidad de lo que los usuarios están haciendo en sus terminales, qué sucede con los archivos que se encuentran allí y dónde intenta conectarse ese terminal en Internet. Y necesita control para detener el comportamiento malicioso apenas se detecta. Afortunadamente, la seguridad evolucionó para enfrentar estos desafíos con soluciones simples, abiertas, automatizadas y efectivas.

Proteger cada terminal, en todas partes.

Cisco Umbrella

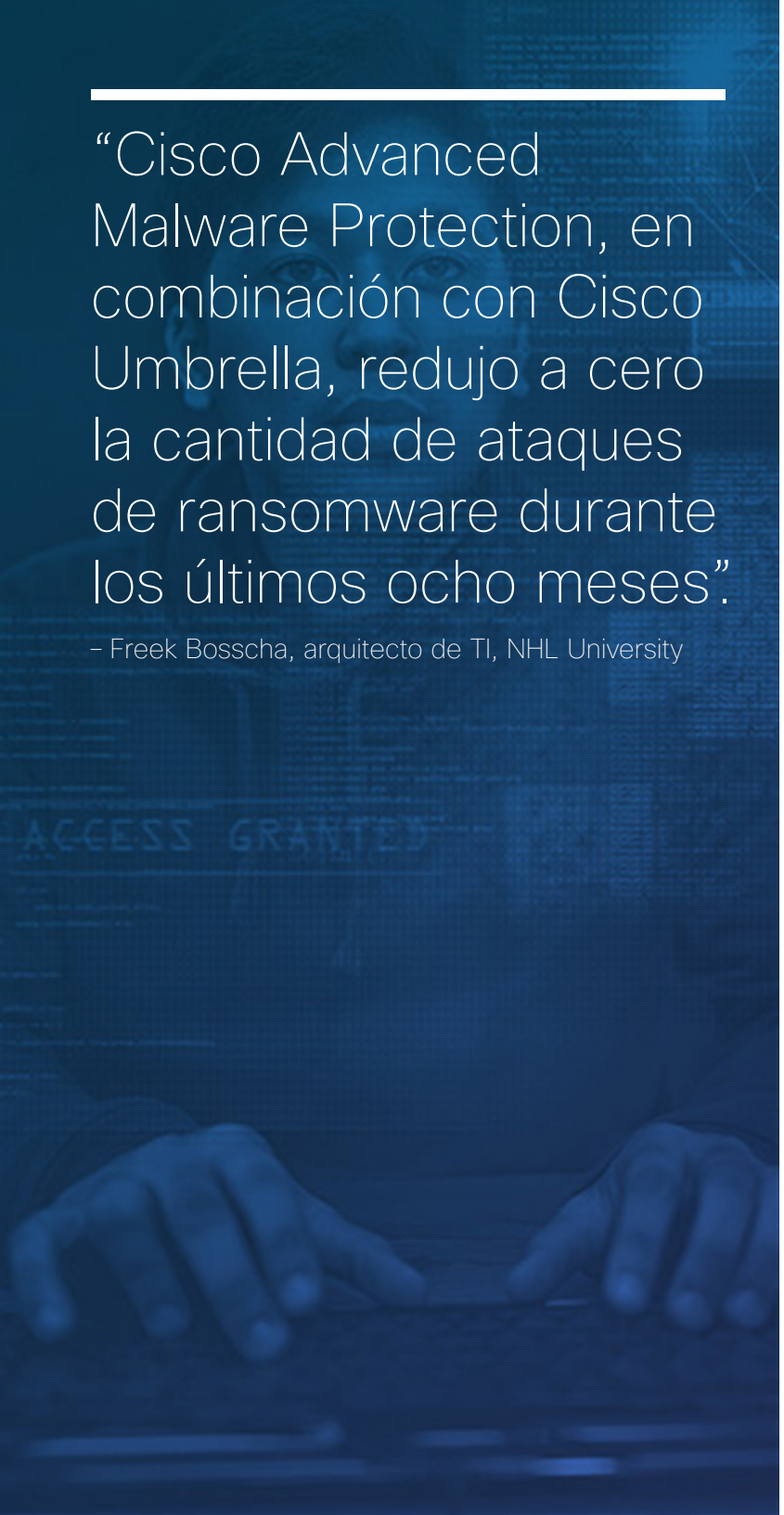
Umbrella es una plataforma de seguridad en la nube que proporciona su primera línea de defensa contra las amenazas alojadas en Internet, independientemente de si los usuarios están conectados o no conectados a la red corporativa. Umbrella le da visibilidad completa de la actividad de Internet en todas las ubicaciones y terminales. Además, supervisa y analiza la infraestructura del atacante para identificar y bloquear proactivamente las solicitudes maliciosas antes de que se establezca siquiera una conexión. Con una red global masiva de DNS y un proxy inteligente, Umbrella lo ayuda a detener los ataques con anticipación, identifica los dispositivos ya infectados más rápidamente y evita la filtración de datos.

Cisco AMP para terminales

AMP for Endpoints es seguridad de próxima generación para terminales administrados en la nube que analiza los archivos desconocidos y bloquea automáticamente el malware para tratar de ejecutar los terminales. Supervisa y registra continuamente toda la actividad de archivos en los terminales, independientemente de la disposición del archivo, para detectar rápidamente el comportamiento malicioso. A continuación, AMP muestra el historial completo del comportamiento del malware en el tiempo (de dónde provino el malware, dónde estuvo y qué está haciendo), lo que le permite detectar y remediar de forma retrospectiva las amenazas que antes se consideraban benignas.

"Confiamos mucho más en la seguridad de nuestros terminales con Cisco Umbrella combinado con Cisco AMP. Tuvimos cero infecciones de malware desde que lo implementamos hace tres años".

– Ingeniero, empresa mediana de servicios financieros



"Cisco Advanced Malware Protection, en combinación con Cisco Umbrella, redujo a cero la cantidad de ataques de ransomware durante los últimos ocho meses".

– Freek Bosscha, arquitecto de TI, NHL University

Un doble golpe contra el malware.

Cisco AMP for Endpoints y Cisco Umbrella son dos soluciones de seguridad que funcionan en armonía para proporcionar la visibilidad, el contexto y el control necesarios para prevenir, detectar y responder a los ataques dirigidos a los terminales, antes de que se pueda producir el daño.

Juntos, Umbrella y AMP for Endpoints ofrecen la primera y última línea de defensa para las amenazas actuales, en cualquier sitio que los usuarios visiten.

Prevenir

Umbrella

Bloquea solicitudes maliciosas de Internet (dominio, URL e IP), independientemente del mecanismo de entrega (correo electrónico, web, descargas ocultas, etc.)

AMP para terminales

Bloquea el malware conocido en la inspección inicial

Utiliza sandbox para analizar archivos desconocidos

Detectar

Umbrella

Impide las autenticaciones de comando y control (C2) a los servidores del atacante para detener la exfiltración de datos y la ejecución de la encriptación de ransomware

AMP para terminales

Analiza constantemente la actividad de todos los archivos en los terminales para detectar rápidamente un comportamiento malintencionado y alertar a los equipos de seguridad

Responder

Umbrella Investigate

Proporciona datos actualizados de amenazas y contexto histórico sobre dominios, direcciones IP y hash de archivo para una investigación más rápida

AMP para terminales

Muestra el historial completo y el contexto de una violación de seguridad para informar sobre decisiones de seguridad que se tomaron

Puede detener ataques a través de las capacidades de control de ataques y archivos en cuarentena

Evite las secuelas con una estrategia anticipada.

Para protegerse contra las amenazas en constante evolución a través de una superficie de ataque cada vez mayor, necesita más de una línea de defensa. Cisco Umbrella y Cisco AMP for Endpoints, respaldados por la investigación de amenazas de Talos, líder de la industria, le brindan una protección ininterrumpida desde la capa de DNS hasta el terminal. Juntos, proporcionan la visibilidad y el control que necesita para proteger a los usuarios contra el malware, la suplantación de identidad y las autenticaciones de comando y control, dondequiera que vayan y cualquiera que sea el dispositivo que utilicen.

¿Está preparado para agregar un doble golpe a su cartera de seguridad?

Comience con Cisco AMP for Endpoints.

PRUÉBELO HOY MISMO

O dele una oportunidad a Cisco Umbrella. Es gratuito durante 14 días.

COMIENCE A PROBARLO

Fuentes:

1. "Datos y aplicaciones portátiles seguros", SANS, 2015
2. Pulso de mercado de IDG Research Services: "IDG Research Services Market Pulse" (La necesidad de seguridad fuera de la red), mayo de 2016
3. "Keeping SaaS Secure" (Mantener el SaaS seguro), Gartner, 2016
4. Índice global de la nube de Cisco: "Forecast and Methodology" (Pronóstico y metodología), 2015-2020
5. "Secure Direct-to-Internet Branch Offices: Cloud-Based Security Offers Flexibility and Control" (Sucursales seguras de acceso directo a Internet: la seguridad basada en la nube ofrece flexibilidad y control), Forrester, 2015
6. "Effective Incident Detection and Investigation Saves Money" (La detección e investigación efectiva de incidentes ahorra dinero), IDC, 2016
7. "A Year of Mega Breaches" (Un año de grandes infracciones a la seguridad), Ponemon Institute, 2015
8. Informe de seguridad anual de Cisco , Cisco, 2016
9. "Exploits at the Endpoint: SANS 2016 Threat Landscape Survey" (Ataques al terminal: Encuesta sobre el panorama de amenazas de SANS 2016)
10. "Ransomware Attacks Rise 250 Percent in 2017, Hitting U.S. Hardest" (Los ataques de ransomware aumentan 250 por ciento en 2017, afectando duramente a los EE. UU.), Newsweek, 23 de mayo de 2017
11. "Simple Lessons You Must Learn from WannaCry" (Lecciones sencillas que debe aprender de WannaCry), Ian McShane, Gartner, 29 de junio de 2017