Cisco Umbrella

INFORME DE SOLUCIONES

Cisco Umbrella para los servicios de salud.
La manera más sencilla de anticiparse a los ataques.

Mejore los resultados de la atención médica mientras reduce costos

El panorama de TI en el sector de la salud ha pasado por una enorme cantidad de cambios. Actualmente se están adoptando o planeando numerosas tecnologías innovadoras, entre las que se incluyen expedientes médicos electrónicos, portales para pacientes, salud móvil (mHealth), medicina a distancia, dispositivos médicos IoT (Internet de las Cosas) y servicios de nube que cumplen con la ley HIPAA (como Office 365 y Google Apps). Los médicos y el personal conectan sus dispositivos móviles y de IoT no gestionados a la red, con lo que pueden acceder a los datos de los pacientes –como la información médica protegida (PHI, por sus siglas en inglés) o la información de identificación personal (PII). De igual modo, los pacientes se conectan a la red inalámbrica abierta con dispositivos que usualmente están infectados, lo que puede ser un inconveniente. Y eso está sucediendo en todas partes –de decenas a cientos de clínicas y consultorios. El potencial es enorme, ¿cierto? ¡Y los criminales también lo creen así!

El Problema: exceso de complejidad, costos y cumplimiento

La contratación de personal (26%) y el mantenimiento (23%) que se le da a la tecnología de protección implementada localmente consume la mitad de los presupuestos de seguridad en el mercado de la salud[1]. Es muy probable que el resto se utilice para cumplir con los requerimientos de HIPAA/HITECH. La mayoría de las soluciones de seguridad integran firewalls para defender las conexiones a la red, antivirus para proteger los endpoints administrados, proxies para aplicar políticas web y SIEM (sistema de información de seguridad y gestión de eventos) para cumplir con las regulaciones. Algunos equipos implementan medios más avanzados como un sandbox (aislamiento de procesos), pero con frecuencia descubren que no cuentan con los recursos suficientes para cubrir cada conexión de la red o responder a todas las alertas. Usted sabe que hoy estas capas no son suficientes, pero para cuando implemente otro producto o agente que cubra una brecha de seguridad, habrán surgido diez más de ellas.

La Necesidad: cerrar las brechas de seguridad en los servicios de salud

Proteja todos los dispositivos
incluso los que no soportan agentes

El Requerimiento: una primera línea de defensa que sea...

Sencilla	▪ Cubra las brechas sin necesidad de instalar hardware o actualizar el software manualmente ▪ Proteja dispositivos y puertos sin cambiar la configuración o la latencia
Abierta	▪ Amplíe la protección con la que cuenta hoy –así como los datos para la respuesta ante incidentes – a través de integraciones ▪ Proteja dispositivos y puertos sin cambiar la configuración o la latencia
Automática	▪ Anticípese a las amenazas al saber dónde se preparan los ataques ▪ Bloquee los dominios e IPs maliciosos antes de que se establezca una conexión
Efectiva	▪ Detenga las amenazas antes de que lleguen a su red y endpoints ▪ Identifique con mayor rapidez los dispositivos infectados y evite la exfiltración de datos

Por qué el uso de Cisco Umbrella puede proteger la PHI

Los callbacks de comando y control (C2) usan cualquier puerto:

- **15%** de los C2 evitan los puertos web 80 y 443[2]
- **91%** de ellos se inician mediante solicitudes DNS[3]

La industria atacada #1 en 2015

Los servicios de salud se han convertido en el objetivo más lucrativo para los criminales porque los expedientes médicos valen 10 veces más que las tarjetas de crédito, por eso la superficie de ataque se está ampliando rápidamente. Además, los atacantes saben que usted desembolsará el dinero rápidamente con tal de liberar los expedientes de sus pacientes en caso de que un ataque de ransomware ponga sus vidas en riesgo verdadero.

Por qué usar Cisco Umbrella en lugar de ISPs

- **65M+** Usuarios activos cada día
- **100%** Disponibilidad del sistema desde 2006[4]
- **#1** La menor latencia de DNS de Norteamérica[5]
- Conozca 10 razones más en cs.co/PointDNS

Fuentes:
[1] cs.co/forrester-healthcare
[2] cs.co/lancope-c2-stat
[3] cs.co/dns-c2-stat
[4] cs.co/umbrellasystems
[5] cs.co/dns-latency

La Solución: Cisco Umbrella se convierte en su primera línea de defensa

Cisco Umbrella es una plataforma de seguridad radicada en la nube que le ofrece la primera línea de defensa contra las amenazas. Gracias a que está fundamentada sobre la base del internet, Umbrella le brinda una visibilidad completa de la actividad que se realiza en todos los lugares de la red, así como dispositivos y usuarios. Además, detiene las amenazas en cada puerto o protocolo antes de que lleguen a su red o endpoints, brindándole una mejor protección contra violaciones a la PHI y PII.

Al hacer un análisis y aprender de los patrones de actividad en internet, Umbrella descubre automáticamente la infraestructura que los atacantes están preparando para lanzar sus amenazas y detiene proactivamente las solicitudes a los destinos maliciosos antes de que se establezca siquiera una conexión.

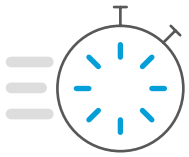
Con Umbrella, usted puede detener de inmediato las infecciones de phishing y malware, identificar más rápidamente los dispositivos que ya están infectados y prevenir la exfiltración de datos. Es la manera más rápida y sencilla de proteger a todos sus usuarios en minutos.

¿Los empleados desconectan sus laptops de la red?

Si usted utiliza Cisco AnyConnect para Windows o Mac, simplemente habilite el módulo de seguridad móvil. Como alternativa, nuestro agente ligero para Windows y Mac aplica la seguridad junto a su agente VPN actual. Consulte más información en cs.co/roaming-client.

Por qué las organizaciones de salud eligen Umbrella para mejorar la seguridad

La seguridad más sencilla y veloz que usted implementará.



- Sin necesidad de agentes, evite que el malware se instale en los dispositivos BYOD, IoT (como bombas de infusión o monitores cardiacos) o en los sistemas corporativos. Además, impida que los callbacks C2 exfiltren o encripten sus datos.
- Sólo dirija las solicitudes de internet desde sus servidores DNS internos, ruteadores o Wi-Fi APs y todos los dispositivos estarán protegidos sin importar quién sea su propietario o cuál sea su sistema operativo.

La reducción más grande del ruido de seguridad y del trabajo reactivo.

- El ruido que producen las alertas de su sistema de seguridad puede ocultarle los ataques más perjudiciales a su equipo de respuesta a incidentes.
- Prevenga las amenazas comunes y avanzadas antes de que se intente siquiera hacer una conexión o que un archivo se descargue, de modo que haya mucho menos alertas para hacer el triaje y priorizar.
- En pocas palabras: firewalls, proxies, antivirus y SIEM no son suficientes.

La mejor forma de ampliar la protección a todas partes.

- Convierta su detección local de amenazas en prevención global de amenazas aprovechando nuestro servicio de nube basado en API.
- Está disponible una gran variedad de integraciones llave en mano –visite cs.co/fireeyeintegration para consultar más información sobre las más populares.
- Al utilizar nuestra API, usted puede ampliar fácilmente y bloquear inmediatamente los dominios maliciosos detectados por su infraestructura de seguridad existente.

Si está interesado en saber más, contacte a **Cisco**

Tel: **001-855-381-3649**

Únase a la conversación

Visite nuestro sitio