Cisco, la seguridad está en la red

Enero 2018

Cisco, la seguridad está en la red

Las amenazas crecen y se hacen más sofisticadas, por eso saber lo que ocurre en tu red es más necesario que nunca. Hablar de visibilidad se ha puesto de moda, pero no es fácil cuando las redes son cada vez más complejas, cuando el número de dispositivos conectados a ellas crece sin parar, cuando el cloud está cada vez más presente, los minutos de vídeo no paran de crecer y el Internet de las Cosas empieza a desbordarse sin ni siquiera haber alcanzado las previsiones.

Estamos en la era del Big Data, de la automatización y el machine learning, en plena evolución hacia un negocio digital y ubicuo que no llega sin riesgos. La conectividad universal tiene un coste, implica una mayor complejidad de la red, que debe ser capaz de generar más eventos y datos para un creciente número de usuarios y aplicaciones. Son cambios que llevan a la necesidad de una nueva arquitectura de red, a Cisco DNA, o Digital Network Architecture, capaz de soportar el centro de datos, el cloud y las infraestructuras de IoT manteniendo la disponibilidad, escalabilidad y rendimiento.

En todo este proceso, la seguridad se ha convertido en el principal freno para la transformación digital de las empresas, que tienen ente seis y 50 soluciones desplegadas, lo que genera entornos complejos de gestionar. La propuesta de Cisco es hacer que las soluciones se integren y compartan contexto e información sobre las amenazas, con el concepto de 'ver una vez y detener en todas partes', y que se aprovechen las inversiones ya realizadas y la infraestructura de red ya desplegada.

Cisco proporciona visibilidad y capacidad de respuesta de última generación para detectar más amenazas y detenerlas más rápidamente

No en vano el negocio de Seguridad de Cisco lleva cuatro trimestres consecutivos de crecimiento a doble dígito, con importantes adquisiciones e inversiones estratégicas. Entre ellas destacan la compra de Sourcefire en 2013 por 2.700 millones de dólares; la de OpenDNS por más de 652 millones; Lancope por 425 millones o la de CloudLock por 293 millones de dólares en 2016. La última ha sido la de Observable Networks el pasado verano, con la que Cisco mejora la monitorización de conductas que permitan a los equipos de TI detectar anomalías que puedan estar relacionadas con brechas de seguridad.

Compartir en RRSS

El objetivo de Cisco es crear una red capaz de 'auto-defenderse' que opere bajo el modelo de 'detectar una vez y proteger en todas partes'.

Seguridad Integrada, sencilla e inteligente

La seguridad está en la red. Es una frase que se viene repitiendo en los últimos años. También se habla mucho de visibilidad, sobre todo asociado a una mejor detección de las amenazas, y para ello nada mejor que unir un gran conocimiento de redes y de seguridad.

Cisco, una de las mayores compañías de seguridad del mundo, con más de 5.000 profesionales dedicados y 22 centros de datos ubicados por todo el mundo que analizan el 35% del tráfico de e-mail mundial, es la única compañía con la capacidad de ver en tiempo real los cambios producidos en terminales, redes y el Cloud, y de comprender y detener los ataques en todas sus etapas (antes, durante y después) con mayor rapidez.

Sólo Cisco incorpora seguridad dentro de la infraestructura de red de una manera que reduce las vulnerabilidades y genera políticas de seguridad coherentes en todas las líneas de productos, lo que permite proteger contra productos falsificados y modificaciones no autorizadas de hardware y software, además de proporcionar verificación de que los dispositivos de red de Cisco están funcionando según lo previsto.

Sólo Cisco permite a las organizaciones utilizar análisis de red para identificar malware y amenazas en el tráfico cifrado, especialmente en puntos de la red donde el descifrado y la inspección de paquetes son un desafío.

Las soluciones y servicios de Cisco se han diseñado para simplificar la ciber-seguridad, proporcionando una defensa integrada frente a amenazas que elimina la complejidad y permite a las organizaciones centrarse en la innovación. Este porfolio se combina con inteligencia frente a amenazas de clase empresarial, servicios líderes y productos integrados para lograr una seguridad más sencilla y efectiva y menos compleja.

Además, Cisco invierte en I+D cerca de 6.300 millones de dólares al año (en torno al 13% de sus ingresos globales). Y tampoco hay que olvidar que cuenta con Talos, el mayor grupo de investigación en ciberseguridad de la industria. Los datos están ahí: Cisco Talos bloquea cada día 19.700 millones de amenazas, una cifra que multiplica por seis el número de búsquedas diarias de Google, o lo que es lo mismo, tres amenazas bloqueadas diariamente por cada habitante del planeta. Y ha conseguido reducir el tiempo de detección de nuevas amenazas a 3,5 horas, frente a los 100 días de media de la industria.

Pero además, Cisco Talos analiza más de 300.000 millones de correos electrónicos y OpenDNS resuelve más de 80.000 millones de peticiones de Internet al día, el 2% de todas las peticiones de internet mundiales, bloqueando 80 millones de peticiones DNS maliciosas diariamente.

Parte del éxito de Talos se basa en la telemetría… o la monitorización y seguimiento de lo que ocurre por la red; y si alguien sabe de redes es Cisco, ya que el 80% del tráfico de Internet ha pasado por equipos de Cisco en los últimos 30 años.

Cisco, la seguridad está en la red

CISCO, LA SEGURIDAD ESTÁ EN LA RED

CLICAR PARA VER EL VÍDEO

La Red Intuitiva de Cisco: hacia la auto-defensa

Con su Red Intuitiva, Cisco reinventa la red creando una plataforma inteligente y segura, capaz de enfrentarse a este mundo multicloud, a extraer todo el poder de los datos y desplegar la seguridad en todas y cada una de las partes de la propia red. La Red Intuitiva de Cisco marca el inicio de una nueva red en la que, además de tenerse en cuenta el contexto, es capaz de hacer frente a las más de un millón de conexiones por hora que se añadirán a Internet en 2020.

La Red Intuitiva de Cisco, el logro más significativo de la compañía en los últimos diez años, está basada en su Digital Network Architecture y se compone de tres partes. Por un lado, DNA-Center, el centro de comando y plataforma de análisis de la red; por otro, su capacidad de analizar el tráfico cifrado; y en tercer lugar una serie de switches programables, la serie Catalyst 900, diseñados desde cero pensando en las necesidades de movilidad, cloud e IoT en la era de la transformación digital.

Y teniendo en cuenta que la seguridad no supone únicamente un mecanismo para proteger el negocio, sino un impulsor; que en España los ciberataques detectados han pasado de 50.000 en 2015 a 115.000 en 2016; que más de un tercio de las organizaciones que sufrieron un ataque de ciberseguridad en 2016 tuvieron pérdidas sustanciales; que sólo el 56% de las alertas de seguridad son investigadas; que el 27% de las aplicaciones cloud de terceros introducidas por los empleados son consideradas como de alto riesgo… lo que propone Cisco es una nueva aproximación a la ciber-seguridad centrada en las amenazas, integrada (que reduce la complejidad generada por múltiples soluciones puntuales), basada en la compartición de contexto y de inteligencia global entre todos los dispositivos y capaz de proteger a lo largo de la red extendida (desde el perímetro hasta el Cloud) antes, durante y

Las recomendaciones de Seguridad de Cisco.

Cisco es una de las mayores empresas de seguridad del mundo, con más de 5.000 profesionales y 22 centros de datos dedicados a detectar y bloquear el malware

Las recomendaciones de Cisco para mantener las empresas a salvo:

- Convertir la seguridad en prioridad de negocio
- Evaluar la estrategia operativa: revisar las prácticas de seguridad, parcheo y control de puntos de acceso a los sistemas de red, aplicaciones, funciones y datos
- Medir la eficacia de seguridad: establecer métricas claras y utilizarlas para validar y mejorar las prácticas de seguridad
- Adoptar una estrategia de defensa integrada: convertir la integración y la automatización en una prioridad para incrementar la visibilidad, mejorar la interoperabilidad y reducir el Tiempo de Detección

después de los ataques mediante una arquitectura sencilla, abierta y automatizada.

El sistema Cisco Stealthwatch y Cisco Identity Services Engine (ISE) son las soluciones de próxima generación que funcionan dentro de Cisco Digital Network Architecture (DNA). Ambas, son capaces de transformar la red en un sistema de seguridad. Lo que hace Cisco ISE es identificar cada dispositivo y usuario que accede a la red, mientras que Cisco Stealthwatch descubre las amenazas en toda la red, incluso si superan las defensas del perímetro.

Lo que ha hecho Cisco es integrar la seguridad en Cisco DNA, proporcionando una arquitectura confiable que permita transformar la red. Se consigue así una red más inteligente, con un control de accesos centralizado, que ofrezca gran visibilidad y que permita simplificar las herramientas y procesos para reducir los riesgos, costes y complejidad. El resultado es una red que puede utilizarse como un sensor de seguridad para obtener visibilidad a través del análisis y la inteligencia en tiempo real. Puede comprender mejor quién y qué hay en la red, identificar y seguir a los usuarios, controlar el rendimiento de la aplicación y comprender dónde se produce la congestión de la red. Con las características recientemente anunciadas, incluso puede detectar amenazas avanzadas en el tráfico cifrado a la vez que mantiene la privacidad.

Al mismo tiempo, y al ser definida por software, la red de Cisco también permite un control más detallado para aplicar políticas en toda la red y capaz de implementar la segmentación más rápidamente, administrarla más fácilmente y restringir el movimiento de amenazas para reducir la exposición de la red al riesgo.

Con más de 5.000 profesionales dedicados, Cisco es una de las mayores compañías de seguridad del mundo

Para crear sistemas confiables, Cisco incorpora la seguridad -desde el diseño y la primera etapa de fabricación- en dispositivos de red como conmutadores, enrutadores y puntos de acceso inalámbrico. Esta base segura y confiable hace que las soluciones de la compañía sean más resistentes a los modernos ciberataques y ayuda a proteger a los clientes y sus redes.

El reto del tráfico cifrado

Datos de Gartner indican que en 2019 el 80% del tráfico web estará cifrado. Detrás de esta pasión por cifrar está la búsqueda de la privacidad. Pero también hay estudios, en este caso de Ponemon Institute, que indican que el 41% de las amenazas aprovechan el tráfico cifrado para evitar su detección.

La identificación de amenazas contenidas en el tráfico de red cifrado plantea un conjunto único de desafíos. Es importante controlar este tráfico

Cisco, la seguridad está en la red

en busca de amenazas y malware, pero hay que hacerlo de forma que se mantenga la integridad del cifrado. Debido a que la técnica de inspección profunda de paquetes (deep-packet-inspection) no puede aplicarse por motivos de privacidad, las técnicas utilizadas hasta ahora se han basado en el análisis de los metadatos obtenidos del flujo de tráfico, como pueden ser las longitudes de paquetes del flujo y los tiempos entre llegadas.

Cisco ha dado un paso más al considerar un enfoque denominado “data omnia” o “todo datos”, para lo que se han desarrollado modelos supervisados de aprendizaje automático basados en un amplio abanico de muestras de malware en entornos de ejecución acotados (sandbox) y diversas características de flujos de datos de red. Entre ellas se incluyen metadatos TLS, flujos DNS contextuales y cabeceras HTTP procedentes de la misma fuente de direcciones IP durante un marco temporal de cinco minutos.

Al correlacionar estos metadatos con tráfico benigno y maligno en millones de flujos, Cisco logra clasificar con precisión los flujos de tráfico maliciosos. Y sin necesidad de descifrar el tráfico en volumen. En experimentos con datos reales, los resultados son asombrosos: una precisión superior al 99% con 0,01% de falsos positivos. Es decir, sólo un falso positivo por cada 10.000 conexiones TLS analizadas. Esto demuestra que la aproximación data omnia realmente funciona.

Por primera vez la red puede identificar y mitigar las comunicaciones de malware ocultas en tráfico cifrado utilizando nuevos modelos de inteligencia artificial que analizan los patrones de tráfico de los metadatos con gran precisión y mediante un procesamiento de alta velocidad que no ralentiza el tráfico. Esta capacidad de Encrypted Traffic Analytics está disponible en los nuevos switches Catalyst 9000 y en la familia Cisco 4000 Series Integrated Services Routers.

Sólo Cisco, mediante inteligencia frente a amenazas líder en la industria y algoritmos de machine learning, puede convertir la red en un sensor y reforzador de políticas de extremo a extremo que detecta, detiene y previene las sofisticadas ciber-amenazas a la par que mantiene la privacidad.

Cisco NetACad, conocer el aspecto técnico de la seguridad ya no es suficiente

Según el Estudio Mundial sobre los Profesionales de Seguridad de la Información (Global Information Security Workforce Study) de (ISC)2 de 2017,

Cisco, la seguridad está en la red

en 2022 habrá un déficit de 1,8 millones de profesionales en ciberseguridad. Esto supone un 20% más que la previsión realizada en 2015. Concretamente, el 66% de las empresas en Europa indica que no hay suficientes profesionales en seguridad de la información. Las organizaciones mencionaron que el motivo principal es la dificultad para encontrar personal cualificado.

Para hacer frente a un reto de hoy nació hace 20 años Cisco Networking Academy, o NetAcad, un programa sin ánimo de lucro que ha formado en tecnologías de redes de última generación a más de 7,8 millones de estudiantes en todo el mundo desde 1997. Y a 155.500 alumnos en España desde 2000. Y que ahora apuesta por la ciberseguridad.

NetAcad ofrece paquetes de formación básicos, medios y avanzados. Diseñados conjuntamente con empresas e instituciones educativas, los currículos responden a las demandas actuales y futuras, incluyendo Internet of Things (IoT), ciber-seguridad, smart grids o redes de nueva generación. Cisco cede gratuitamente los contenidos y todo el programa de formación, proporcionando también equipos para prácticas a precio de coste.

El 70% de los alumnos (71% en España) que completan un curso avanzado consiguen un nuevo trabajo, ascienden de categoría profesional o mejoran sus condiciones salariales. Además, NetAcad utiliza una plataforma Cloud para extender la formación a múltiples colectivos a escala global, incluyendo aquellos en riesgo de exclusión social .

Actualmente, NetAcad se apoya en una red de 10.400 academias (escuelas, colegios y universidades) en 180 países. Con 22.000 formadores y cursos disponibles en 20 idiomas, suma 1,3 millones de estudiantes concurrentes (el 24% mujeres). Es la mayor aula tecnológica del mundo. Y con una importante apuesta por la diversidad y la inclusión de género, fomentando la formación de las mujeres en ciber-seguridad y otras tecnologías.

En España hay 372 academias (universidades, Formación Profesional y otros centros formativos), 737 instructores y 19.000 alumnos activos. El 85% de los centros son instituciones educativas (el 15% restante corresponde a formación para empresas o Administraciones) y el 87% de los alumnos optan por cursos medios o avanzados con una alta empleabilidad, como CCNA. Además, Madrid, Cataluña, La Rioja, Aragón, Valencia y Galicia han integrado el programa en su oferta formativa para desempleados.

Como seguimiento al programa de formación, el servicio Talent Bridge permitirá a los actuales y antiguos alumnos acceder directamente a las ofertas de empleo de Cisco y de su comunidad de partners (más de 1.000 en España). NetAcad también apuesta por la generación de proyectos emprendedores -colaborando con entidades como INLEA- y la inclusión social (mediante programas con diferentes fundaciones como Esplai o Carmen Pardo-Valcarce).

Además de las academias, NetAcad cuenta con el apoyo de partners regionales y locales -públicos y privados- que desde la creación del programa apoyan e impulsan los cursos de formación. Su labor es fundamental para inspirar a los jóvenes y multiplicar el 'efecto NetAcad' para construir la fuerza laboral del futuro.

Para saber más sobre las soluciones de seguridad de Cisco, pincha aquí.