“Cisco Hypershield es la primera solución diseñada de forma nativa para proteger el data center del futuro”

“Cisco Hypershield es la primera solución diseñada de forma nativa para proteger el data center del futuro”

Ángel Ortiz, director de Seguridad en **Cisco**

Hace unas semanas Cisco realizó el que aseguraba que era el anuncio más trascendental en los últimos 40 años de historia de la compañía y que promete inclinar la balanza a favor de los defensores. Hypershield, que es como se ha bautizado a esta nueva propuesta, es una arquitectura de seguridad altamente distribuida que se basa en la tecnología de Isovalent, adquirida por Cisco a finales de 2023. Isovalent está especializa en eBPF (extended Berkeley Packet Filter), una tecnología que ha transformado la forma en que se monitoriza, analiza y optimiza el rendimiento en sistemas Linux; la tecnología, de código abierto, facilita el rastreo de paquetes en una amplia variedad de sistemas basados en Linux, lo que permite a los equipos de seguridad realizar acciones de cumplimiento y monitorización a través del kernel.

Esto significa que los contenedores, las máquinas virtuales, cada puerto de red... se convierte en un punto de aplicación de la seguridad. Y, en medio de la explosión de la Inteligencia Artificial, cada punto puede aprender del comportamiento de cada activo para detectar actividades sospechosas y activar automáticamente cambios en la segmentación de la red, evitar movimientos laterales y eliminar amenazas potenciales.

De todo ello hablamos con Ángel Ortiz, director de Seguridad en Cisco, a quien empezamos preguntando qué es lo que está ocurriendo en el mercado para que Cisco haya lanzado esta solución, ¿qué es lo que viene a solucionar? Asegurando que Hypershield es la primera solución diseñada de forma nativa para proteger el data center del futuro, explica Ángel Ortiz que la arquitectura de los centros de datos actuales es "una arquitectura tremendamente distribuida, donde no podemos aplicar ciberseguridad a escala humana, sino que tenemos que apoyarnos en la inteligencia artificial". Hypershield se concibe como un nuevo modelo de ciberseguridad, una malla tremendamente distribuida "donde tenemos miles, cientos de miles de puntos de aplicación de la seguridad donde, mediante el uso de inteligencia artificial, podemos aplicar políticas de forma centralizada".

Hablando de las características particulares de la nueva propuesta de Cisco, deja claro Ángel Ortiz que, "al llevar el punto de aplicación de la seguridad allá donde lo necesitamos, allá donde esté el servicio, donde está la aplicación, podemos aplicar políticas de seguridad mucho más granulares". A diferencia de lo que tradicionalmente se ha hecho en ciberseguridad, como forzar a que el tráfico pase por un sitio, "llevamos la política allá donde interesa".

> "Con Hypershield llevamos la política allá donde interesa"

> “Para el canal de distribución, Hypershield es una nueva fuente de ingresos”

Esto permite resolver varios casos concretos, explica el directivo de Cisco. Menciona tres: hacer una microsegmentación en los data centers, es decir, controlar cómo se comunican las aplicaciones entre sí; aplicar virtual Patching; y la posibilidad de hacer actualizaciones de software, actualizaciones de políticas, que ya estén probadas previamente gracias a que cada punto de aplicación de la seguridad tiene un doble plano de control, “con lo cual yo puedo aplicar las nuevas políticas de seguridad o la actualización en el plano secundario, ver qué es lo que ocurre y luego actualizar el plano primario”.

Cisco anunció la compra de Splunk el pasado mes de septiembre en un acuerdo valorado en 28.000 millones de dólares en efectivo, la mayor adquisición de la empresa de redes hasta la fecha. Splunk es una compañía reconocida en el mercado de gestión de eventos e información de seguridad, capaz de analizar archivos de registro y otros datos y utilizar inteligencia artificial para ayudar a las empresas a minimizar el riesgo de incidentes de ciberseguridad. ¿Qué papel juega en la nueva propuesta de Cisco?

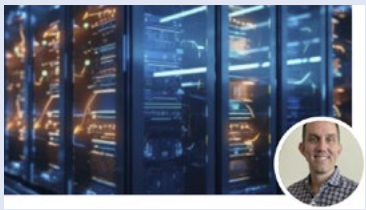
“Teniendo miles de puntos de aplicación de la seguridad y de recolección de telemetría distribuidos, Hypershield es una fuente de telemetría muy potente para Splunk”, responde el directivo, añadiendo que Splunk es una plataforma de analítica de datos muy potente, “que nos va a permitir identificar tendencias para proteger mejor a los clientes”.

Respecto al tipo de cliente que podrá aprovechar todo el potencial de Hypershield, puede ser “cualquier cliente que se esté llevando archivos de computación a la nube y que esté evolucionando su arquitectura de data center va a poder aprovecharse de Hypershield”, explicas Ángel Ortiz.

En opinión del directivo de Cisco, los fabricantes tienen una asignatura pendiente a la hora de hacer más sencilla la seguridad de la nube, la seguridad de los data centers modernos, o en “cómo securizamos no solo el tráfico norte-sur de nuestros data centers, sino el este oeste de cómo se comunican las aplicaciones entre sí”.

Para el canal de distribución, Hypershield es una nueva fuente de ingresos. “Es un nuevo punto de aplicación de la seguridad y una nueva filosofía que también le va a permitir complementar sus servicios”, no solo en seguridad, sino aplicando la microsegmentación como un servicio, o el virtual patching, etcétera. En opinión dl director de seguridad de Cisco, “complementa muy bien lo que son los servicios gestionados de seguridad que están ofreciendo nuestros partners”. CST

ENLACES DESTACADOS



Cisco Hypershield: Reimagining Security

Cisco propone una nueva era de ciberserguridad con Hypershield