VMware: la seguridad hasta el rincón

Seguridad intrínseca. Bajo este término se "esconde" la estrategia de seguridad que despliega VMware. Una protección engarzada en el diseño. En un mercado en el que la tecnología ha extendido sus dominios hasta los últimos rincones, la seguridad debe alcanzarlos también. Roto definitivamente el perímetro, los sistemas de protección se han acoplado a un entorno híbrido y *multicloud* para abarcar dispositivos, aplicaciones y redes. Una estrategia de la que participa activamente su ecosistema de *partners*, en el que Arrow desempeña una función esencial.

Marilés de Pedro

"La seguridad tiene que estar dentro de todo lo que hacemos. Debemos ser capaces de aplicarla en todas y cada una de las áreas en las que operamos", explica Ignacio Arrieta, *solutions engineering director* en VMware Iberia. Una protección por diseño, embebida en todas las soluciones y que alcanza cualquier entorno. "En un mundo *cross cloud*, la seguridad va mucho más allá del perímetro. Se trata de una protección basada en la información que se extrae de todo lo que está pasando en los dispositivos, en las aplicaciones y en las redes", explica. "La clave está en utilizar la misma postura de seguridad".

Seguridad "diferente"

Aunque la seguridad llevaba mucho tiempo formando parte del discurso de VMware, la compra de Carbon Black marcó un antes y un después en su estrategia. Posteriormente la multinacional compró Octarine, una compañía centrada en la protección de los entornos de contenedores y *kubernetes*; y Lastline, con foco en la lucha contra el *malware*. Una inteligente estrategia de compras que ha desembocado en la conformación de una oferta, potente, que abarca todas las áreas de negocio.

"Tenemos una posición privilegiada para observar lo que pasa en las aplicaciones y en las redes de nuestros clientes", señala Arrieta. La seguridad, recuerda, supone la combinación de varias tecnologías. "Es necesario contar con múltiples capas para detectar y detener los ataques. VMware ofrece a las empresas un contexto ampliado, con una información completa, lo que les permite tomar decisiones de seguridad con una mayor profundidad".

Arrieta destaca la capacidad de visibilizar lo que sucede en las redes. Una funcionalidad que con las adquisiciones de Carbon Black y de Lastline, se extendió hasta la propia carga y el entorno del puesto de trabajo. Con la actual expansión del teletrabajo, que ha provocado el uso exhaustivo de los dispositivos, la seguridad tiene que ampliar aún más estas capacidades de visualización. "Además de la red, debemos ser capaces de entender qué es lo que está pasando en las aplicacio-

nes, independientemente de que vivan en máquinas virtuales o en un centro de datos local; en los contenedores y en los *kubernetes*; analizando de forma efectiva, para aplicar los mecanismos necesarios de remediación, los test positivos".

La oferta, hasta el último rincón

La marca, por tanto, practica una seguridad, constante, que alcanza a todos los entornos y que se administra, de manera unificada, desde un único punto. "Contamos con productos *ad hoc* para todas y cada una de las casuísticas; pero sin olvidar que la estrategia está sustentada bajo un paraguas global", insiste.

VMware cuenta con funcionalidades de seguridad en todo el *stack*: desde las capacidades de cifrado que integra vSAN, en el sector de la virtualización del almacenamiento, hasta la creación de reglas de *firewall* distribuido y de puerta de enlace en NSX. Sin enarbolar una personalidad de proveedor de nicho en el mercado de la seguridad, "somos

> "Tenemos una posición privilegiada para observar lo que pasa en las aplicaciones y en las redes de nuestros clientes"

capaces de aportar mucho valor". Incluso, puntualiza, hay entornos, como es el caso de SASE, en el que VMware está ubicado en el cuadrante de líderes de Gartner.

Arrieta cree que a medida que se incremente el consumo de infraestructuras en los entornos *cloud*, con la automatización y los modelos definidos por software ganando peso en los centros de datos más tradicionales, "crecerá la visibilidad de VMware como un proveedor de seguridad global en el mercado". Lo más importante, insiste, es entender el momento *multicloud* en el que vive el cliente. "Más del 75 % de las empresas a las que proveemos de tecnología tiene sus cargas repartidas en dos o más nubes", recuerda. "Lo que exige que los mismos atributos de seguridad que se aplican en el centro de datos tradicional se extiendan a la nube".

Esta mayor visibilidad en el mercado de la seguridad exige una tarea de evangelización en la que, puntualiza, hay que enarbolar la bandera de la automatización en los procesos. "La seguridad es un campo en el que la inteligencia artificial va a ser crítica". Casi todos los ataques tienen un modelo heurístico que, en cierta manera, se puede modelizar. "Si somos capaces de recoger todos los datos que se generan y utilizar la inteligencia artificial para detectar las anomalías y tomar acciones preventivas, estoy convencido de que se va a catapultar nuestra percepción de seguridad en los clientes".

Las aplicaciones, fundamentales

Las aplicaciones son los activos más valiosos que tienen las organizaciones. Hay que pro-

Panorama de amenazas

A mediados del pasado año VMware presentaba su informe Global Security Insights en el que interrogaba a CTO, CIO o CISO de diferentes países, entre ellos 250 españoles, que arrojó una demoledora conclusión: el 92 % de los responsables patrios reconoció que había sufrido alguna brecha de seguridad en los últimos 12 meses. A lo que se sumó la gravedad: 9 de cada 10 de estos agujeros, reconocieron, han sido graves.

Un panorama en el que el *ransomware* seguía siendo el rey. El 75 % de los encuestados afirmaba que el volumen de los ataques se había incrementado, con el 61,5 % puntualizando que el teletrabajo era la causa principal del incremento. Detrás quedaban contar con una solución de seguridad obsoleta (18 %) y la debilidad de los procesos para prevenir ataques (16,5 %).

En el informe, sin embargo, se destacaba que el 98 % de los interrogados desvelaba que tenía pensado aplicar una estrategia de seguridad basada en la nube. Al menos, el 40 % era consciente de que debía desarrollar un enfoque diferente para dar respuesta al complicado panorama.

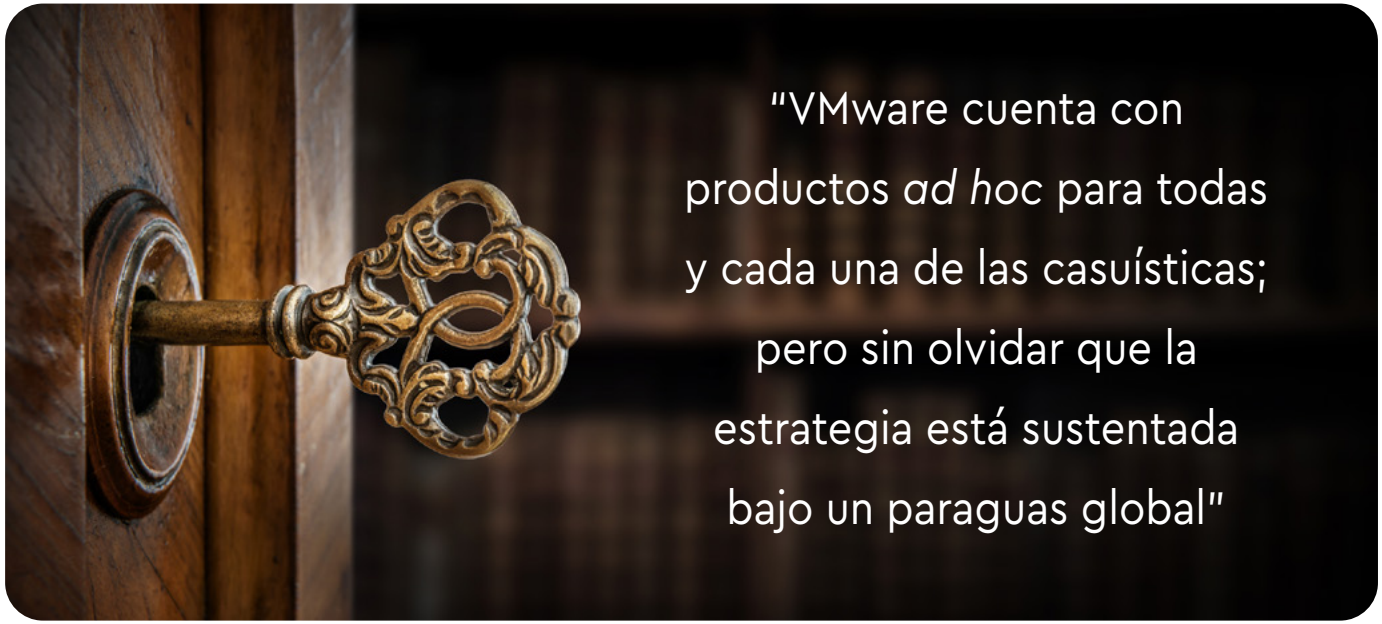
Aplicaciones y cargas de trabajo eran las principales preocupaciones de los CISO: la velocidad a la que se desarrollan y se aplican las aplicaciones era un riesgo. Los CIO reconocían que necesitan disfrutar de una mayor visibilidad sobre los datos y las aplicaciones para prevenir los ataques.

"La seguridad informática puede costar el puesto de trabajo", recuerda Ignacio Arrieta. "No al CISO, sino al CEO", puntualiza. "Estos ya son conscientes, no sólo de los estragos que puede tener el éxito de un ataque en la reputación de una empresa, sino de todas las consecuencias legales que puede acarrear".

¿Soluciones? Además de la obligada formación a los usuarios, siempre "el eslabón más débil", en pos de una mayor concienciación; Arrieta apuesta por la activación, revisión y prueba de los planes de contingencia. Hay que mejorar su aplicación. Y esto se consigue con la automatización y el entrenamiento. "¿Por qué los soldados, los bomberos o los policías repiten, una y otra vez, sus actuaciones, hasta que no tienen que pensar cuando tienen que llevarlas a cabo de manera real; y esto no se hace en las empresas con sus políticas de seguridad?", compara con gran tino. Los planes de contingencia, por suerte, después de la pandemia se han revisado en profundidad, pero no contemplan todos los escenarios. "Hay que simular los ataques; aplicar la ingeniería del caos a los planes de contingencia para conseguir su máxima efectividad".

tegerlas y, precisamente, uno de los grandes retos de la transformación digital que deben afrontar las organizaciones tiene que ver con la seguridad de las mismas. Consultoras como, por ejemplo, Gartner, han señalado este sector como uno de los que más inversión va a mover. Se calcula que el 43 % de los ataques tiene como objetivo a las aplicaciones. En muchos casos son ataques dirigidos aunque también pueden ser ataques de *bots*. Un panorama inseguro que se complica con el desorbitado crecimiento que se observa en este mercado: hasta el año 2019 se crearon 400 millones de aplicaciones en el mundo y la previsión es que entre aquel ejercicio y el año 2023 se creen otros 400 millones de aplicaciones, es decir, todas las que se habían creado en toda la historia de la informática.

Ignacio Arrieta alerta, además, de la básica protección en los procesos de diseño. "Entre los objetivos de los *hackers* se encuentran las cadenas de suministro del software", señala. "En el desarrollo de las aplicaciones hay una tendencia muy acusada a utilizar, de nuevo, piezas de software *open source*; y los ciberdelincuentes se aprovechan de las vulnerabilidades que existen en la cadena de suministro y en el proceso de desarrollo de las aplicaciones corporativas". Una vez más, la receta es el modelo de seguridad como diseño. "Debe estar intrínseca en este proceso".



Modelos de suscripción

Engarzada en el objetivo de VMware de hacer de los modelos de suscripción una de sus vías principales de negocio, la oferta de seguridad ya puede ser ofrecida bajo estas fórmulas. Incluso ya se ha integrado en la oferta de los proveedores de servicio con los que colabora VMware, lo que les permitirá comercializar la seguridad embebida en sus proyectos.

"Los clientes nos están demandando esta manera de consumir la tecnología", recuerda. "De manera muy sencilla y recortando las dependencias de la infraestructura, podemos desplegar un modelo SaaS, aplicando una mayor inteligencia, lo que nos permite disfrutar de un mayor contexto y evolucionar de una manera muy rápida, incluyendo nuevas firmas, monitorizando de manera más efectiva la cadena de suministro del software de seguridad o gestionando cientos de usuarios a la vez... Las ventajas son enormes". Se trata, en definitiva, de defender una seguridad homogénea; lo que permite "tomar mejores decisiones de seguridad".

El canal, brazo armado de VMware

Embajadores digitales. Ignacio Arrieta apela a esta denominación para definir al perfil actual de los *partners*. "Deben ser compañías que acompañen a sus clientes en el despliegue de sus proyectos digitales, desde la primigenia adopción hasta la mejora de las infraestructuras, la calidad del servicio y el *time to market*".

Compañía 100 % canal, VMware también requiere del ecosistema de *partners* para desplegar su oferta de seguridad. Una propuesta que exige a los distribuidores aplicar idéntica filosofía estratégica que la que tiene la marca. Al concebirse la seguridad como una pieza embebida en todas las áreas tecnológicas, los *partners* deben apostar por su integración en todos sus proyectos. Los integradores que quieran dar una solución integral a sus clientes tienen que trabajar de una forma totalmente holística desde la periferia hasta la máquina virtual, con la seguridad como pieza imprescindible.

Ignacio Arrieta valora de manera positiva la adopción de la seguridad por parte del canal más tradicional de VMware, vinculado con el

"La seguridad es un campo en el que la inteligencia artificial va a ser crítica"

entorno del centro de datos. "Han visto la oportunidad de integrar la seguridad en sus proyectos, percibiendo que hay una enorme propuesta de valor".

Competencias y servicios

Dentro del programa de canal de VMware, Partner Connect, hay dos competencias específicas para el mercado de la seguridad (EndPoint Protection y Network Security), a las que próximamente se unirá SASE. Para conseguirlas, primero, el *partner* deberá estar registrado en PartnerConnect, el portal mundial para el canal. Cada *partner* necesita contar en su plantilla con dos profesionales, con un perfil comercial, que hayan completado los VSP (VMware Sales Professional); y otras dos personas con un perfil preventa que hayan superado los cursos VTSP (VMware Technical Sales Professional). En ambos casos se trata de cursos gratuitos *online*. Por ultimo, tienen que contar con un profesional, con perfil técnico, que debe superar un curso de especialización (*postsale*). En este último caso, supone un coste.

Especialmente importante para VMware es la promoción de sus competencias máster en servicios, que permiten al canal desplegar su oferta propia en los clientes. Las tres competencias específicas en el área de la seguridad incluyen una parte técnica apta para servicios. Dependiendo de la competencia existen varios cursos a elegir con su examen correspondiente.

VMware incentiva al *partner* en todo el ciclo de venta. En el área de la preventa, la marca está subvencionando pruebas de concepto y consultorías de preventa. En el proceso de venta, se blinda la oportunidad al *partner* que la ha abierto y que la ha registrado, con descuentos desde un 5 % hasta un 30 %, dependiendo de la tecnología. También cuenta con incentivos una vez cerrado el proyecto. Especialmente incentivado es el modo de suscripción con *rebates* que pueden alcanzar hasta un 22 %.

Papel de Arrow

Arrow cumple un papel esencial en el ecosistema de canal de VMware. Con recursos dedicados a la marca, el mayorista gestiona, de manera directa, a un número importante de *partners*. "Arrow nos asegura una gran cobertura".

En el mercado de la seguridad, VMware está poniendo recursos para conseguir que la seguridad se incluya en el discurso de negocio, reclutando *partners* que quieran trabajar de esa forma.

Arrow despliega también un perfil agregador a través del programa VCPP (VMware

Cloud Provider Program). La integración de las soluciones de seguridad en esta iniciativa permite ofrecerlas bajo un modelo de suscripción. "Con esta fórmula *partners* de todos los tamaños pueden ofrecer, de manera muy sencilla, a sus clientes una seguridad embebida en sus sistemas", insiste Arrieta. "Hay una apuesta muy firme de la compañía de que sea un buen año para el mercado de la seguridad, del que nos podamos aprovechar todos. Sin duda, debe ser un éxito compartido".

¿Qué estamos viendo en este 2022?

A finales del pasado año, VMware presentaba las predicciones que sus expertos hacían en materia de ciberseguridad para este 2022. Todas ellas se están cumpliendo.

Los ataques a sectores críticos, como el energético o el sanitario, y a la cadena de suministro, han seguido creciendo. También están aumentando las amenazas internas y los cibercriminales han puesto su foco en los sistemas operativos Linux.

Analizando el panorama de los sectores críticas, James Alliband, *senior security strategist* en VMware, recordaba, entre otros, los ataques a Colonial Pipeline, que provocó una escasez de combustible en la costa este de Estados Unidos o al sistema sanitario de Irlanda, que cerró los hospitales de todo el país. "Habrá nuevos intentos de ataques a industrias críticas como la energía, la sanidad y las finanzas con la intención de causar pánico mientras se cobra un rescate", preveía. Los expertos mostraban su preocupación por la evolución de los ataques para aprovechar las credenciales de confianza y moverse por la red sin obstáculos.

Linux, por la proliferación de su uso en la transformación digital de las empresas, está siendo diana de los *hackers*. "Muchas organizaciones centran su atención en el *malware* basado en Windows y podrían no darse cuenta de esta amenaza emergente hasta que sea demasiado tarde", alertaba Giovanni Vigna, *senior director of Threat Intelligence* de VMware.

El incremento de los entornos *multicloud* ha conducido a una mayor proliferación de puertos y protocolos comunes, que los ciberdelincuentes utilizan para acceder a los datos de la red. En este contexto, los expertos de VMware consideraban que "tener una buena visibilidad para identificarles será más esencial que nunca a la hora de defender estos entornos".