

# VMware: lo "intrínseco" como filosofía segura



Su poderosa y extensa posición en los sistemas TIC de las empresas concede a VMware una enorme ventaja para reivindicar su particular filosofía en el entorno de la seguridad. Con una inteligente estrategia de compras y con el punto de inflexión que supuso la adquisición de Carbon Black, VMware exhibe ahora una poderosa estrategia en este atestado mercado de la seguridad que apela a una filosofía intrínseca. Su canal, como ha sucedido en cada una de las batallas que ha emprendido a lo largo de su historia, es pieza básica en el despliegue de esta seguridad intrínseca. Arrow, con quien mantiene una potente alianza desde el año 2012, ya está trabajando el negocio con el proveedor de manera segura.

## ¿A qué responde esta seguridad intrínseca?

La manera en la que VMware observa la seguridad no sabe de silos ni se trata de una capa que se "añade" a cada entorno (infraestructura, puestos de trabajo, nube, *kubernetes*, etc.). La marca practica una seguridad, constante, que alcanza a todos los entornos y que se administra, de manera unificada, desde un único punto. De manera tradicional, la seguridad estaba separada en silos, dependiendo de las prioridades de protección de las empresas. "VMware rompe con esta concepción de la seguridad", explica Eduardo Rodríguez, *presales* de VMware en Arrow. "Con un único producto es posible proteger todos los entornos, lo que alcanza tanto al centro de datos tradicional, en el que las empresas tienen una gran parte de sus cargas, hasta los entornos híbridos como en la nube pública". Se trata de una protección embebida en el propio producto. "Es una seguridad intrínseca", insiste. "Las empresas no deben incorporar ninguna solución adicional ya que los productos de VMware cuentan con esa funcionalidad integrada". Una seguridad basada, sin perder de vista vulnerabilidades y ataques, en el análisis de los patrones de comportamiento, tanto de las aplica-



ciones como de los usuarios. "Se trata de una seguridad basada en el contexto, o sea, en lo que acontece al aplicativo, al centro de datos o a la nube en sí. En cuanto el sistema detecta un comportamiento anómalo, el dato o la aplicación se aíslan, lo que evita la propagación".

## Inteligente estrategia de compras

Aunque la seguridad llevaba mucho tiempo formando parte del discurso de VMware, la compra de Carbon Black marca un antes y un después en su estrategia, provocando el nacimiento de una unidad especializada únicamente en el área de la seguridad en VMware.

Carbon Black contaba con una de las propuestas más solventes en el mercado EDR (*Endpoint Detection and Response*), una tecnología de obligada adopción si las empresas quieren proteger de manera adecuada el puesto de trabajo. Con ella, VMware añadía ese concepto intrínseco a todos y cada uno de los entornos en los que operaba, fortaleciendo por tanto aquellas áreas más desguarnecidas.

Una compra que sin embargo va más allá de la protección del entorno del puesto de trabajo en el que estaba volcado su negocio ya que se reforzaba la estrategia de seguridad de VMware

basada en el patrón de comportamientos. La tecnología de Carbon Black se ha integrado armónicamente en toda la cartera de VMware: las soluciones orientadas al mundo del centro de datos, las aplicaciones, los contenedores o la nube, permitiendo el análisis del comportamiento. Una integración que alcanza también a las soluciones de red, NSX, y que permite automatizar la comprobación de seguridad.

El siguiente paso en esta estrategia de compras se produjo el pasado mes de mayo, con la compra de Octarine, una compañía centrada en la protección de los entornos de contenedores y *kubernetes*. La marca ha explicado que la operación tiene por objetivo simplificar DevSecOps y asegurar que los entornos nativos de la nube estén intrínsecamente seguros desde el desarrollo de las aplicaciones hasta el tiempo de su ejecución. Con ello, VMware va a proporcionar a las empresas una visibilidad completa de los entornos nativos de la nube e incluye el análisis de riesgos en el ciclo de vida de DevOps, por lo que los problemas se

## Estructura "compartida" en Arrow

**Arrow cuenta con una potente división de seguridad y redes, en la que están incluidas 25 marcas; con profesionales enfocados en el desarrollo de cada una. Junto a ella, la división de infraestructura reúne a los principales fabricantes en el desarrollo del centro de datos. Ambas divisiones disponen de profesionales de preventa, muy especializados en cada uno de los fabricantes que forman parte de la oferta del mayorista.**

**VMware está integrado dentro de la oferta de Arrow en el área de infraestructura aunque el negocio de seguridad va a ser promovido, de manera especial, por los preventas que forman parte de la potente división de seguridad y redes. "Desde la división de infraestructura vamos a incidir en que los *partners* perciban el enorme valor que tiene acudir a sus clientes con este mensaje de seguridad intrínseca de VMware", explica el preventa. "Si necesitan profundizar en algún aspecto concreto, a nivel técnico, pueden acudir a los profesionales expertos en seguridad que forman parte de la división de seguridad y redes". Unos profesionales que atesoran un profundo conocimiento de este proveedor ya que Carbon Black, antes de ser adquirida por VMware, formaba parte de la oferta de Arrow. "El *partner* puede aprovechar nuestro conocimiento, tanto en el área de la infraestructura como en el campo de las redes y la seguridad para ofrecer una oferta potente y completa a sus clientes".**

La compra de Carbon Black marca un antes y un después en la estrategia de seguridad de VMware



detectan antes de que las aplicaciones se implementen en producción. La compra de Octarine refleja el compromiso, notorio, de VMware por el desarrollo de los entornos de *kubernetes*. Eduardo Rodríguez recuerda que se integrará con Carbon Black Cloud, "permitiendo hacer *backup* de los entornos de *kubernetes*". La tecnología, combinada con integraciones nativas con Tanzu, vSphere, NSX y VMware Cloud Foundation, "permitirá la protección intrínseca de las cargas de trabajo". La última compra, acontecida el pasado mes de junio, ha tenido como protagonista a Lastline, que ha centrado sus esfuerzos de negocio en la lucha contra el *malware*. Cuenta con una plataforma de protección

contra él para detectar y detener amenazas avanzadas y persistentes, *exploits* de día cero y *malware* evasivo. Sus soluciones protegen la red, el correo electrónico, la nube y las infraestructuras web. VMware ha anunciado que éstas se integrarán en su arquitectura NSX y que incrementarán las capacidades de VMware Carbon Black Threat Analysis Unit (TAU) con análisis de conducta e investigación de amenazas centradas en la red.

### La seguridad de VMware, integrada en Arrow

Este foco claro en el desarrollo del mercado seguridad tiene su reflejo en el programa de canal de VMware. La marca ha diferenciado las certificaciones y competencias por verticales, con la seguridad como una unidad perfectamente diferenciada del resto (centro de datos, NSX, *workspace*, etc.). Con ello, los socios que quieran centrarse únicamente en su desarrollo, podrán hacerlo, con una formación específica para ello. Además ya no será necesario tener la certificación en vSphere como certificación obligatoria para vender cualquier producto. "Queda claro el foco de VMware por la seguridad", ratifica Rodríguez.

La marca ya ha puesto a disposición del canal sus tradicionales certificaciones y acreditaciones VSP (VMware Sales Professional) y VTSP (VMware Technical Sales Professional), aplicadas al área de la seguridad. "Vamos de la mano con VMware para que el canal perciba que va a ser un jugador muy importante en el mercado de la seguridad". No observa,

*"Se trata de una seguridad basada en el contexto, o sea, en lo que acontece al aplicativo, al centro de datos o a la nube en sí"*

sin embargo, un camino complicado. "Los distribuidores que forman parte del canal de VMware ya están empezando a mostrar mucho interés por este mercado", asegura. Se trata, explica, de sumar una fortaleza más a su propuesta. "Por ejemplo, hay una gran parte del canal, como es el caso de los distribuidores que comercializan las soluciones de VMware en torno al puesto de trabajo (Workspace One), que ya habían integrado la potente apuesta de seguridad, al ser el área prioritaria en el que se movía Carbon Black".

#### La seguridad, eterna oportunidad

La potencia del discurso de la seguridad en torno al puesto de trabajo señala una de las grandes oportunidades que se abren para el canal en los próximos meses, ante la explosión que se ha producido en torno al teletrabajo. Rodríguez alerta de los riesgos que se pueden producir en torno a la seguridad en estos entornos domésticos. "La seguridad es más vulnerable ya que es el usuario el que se sitúa como administrador o gestor principal de los datos y aplicaciones que la empresa tiene", recuerda. Con un perímetro completamente "disperso" y en el que los datos reposan en muchos entornos, el reto de la protección es mayor.



Rodríguez recuerda que la protección que exhibe Carbon Black alcanza cualquier perímetro y se administra desde un único punto. "Al usuario hay que dotarle de una movilidad completa lo que exige una completa seguridad de todos los dispositivos que utiliza en su entorno de trabajo". VMware ha lanzado un paquete, *Working from home*, que integra VeloCloud (SD-WAN), lo que habilita también la conexión, tan importante en el puesto de trabajo. "Se trata de que el usuario acceda a sus aplicaciones pero además lo haga de manera segura".

## La decidida apuesta por *kubernetes*

El uso de *kubernetes* para permitir el despliegue de las aplicaciones y soluciones de negocio en las empresas señala uno de los focos prioritarios de VMware. La compra de Pivotal, primero; y la reciente de Octarine, no han hecho sino reforzar la apuesta.

Durante el último VMworld Europe, celebrado en Barcelona a finales de 2019, la marca dejó claro su compromiso a través de su catálogo Tanzu que, como señalaron los principales responsables de la compañía, pretende "cambiar la forma en que la que se crea, gestiona y ejecuta software en *kubernetes*".

Una oferta que incluye VMware Tanzu Mission Control, que se presenta como un punto de control único desde el que los clientes gestionarán todos sus clús-



teres de *kubernetes*, independientemente de dónde se ejecuten; y Project Pacific, que persigue transformar el producto estrella de VMware, vSphere, en una plataforma nativa de *kubernetes*.

Una cartera que también incluye VMware Tanzu Kubernetes Grid, que se presenta como un nuevo *runtime* de *kubernetes* con el que los clientes pueden instalar y ejecutar un entorno *multicluster* de *kubernetes* en la infraestructura que elijan. Está diseñado para ejecutar

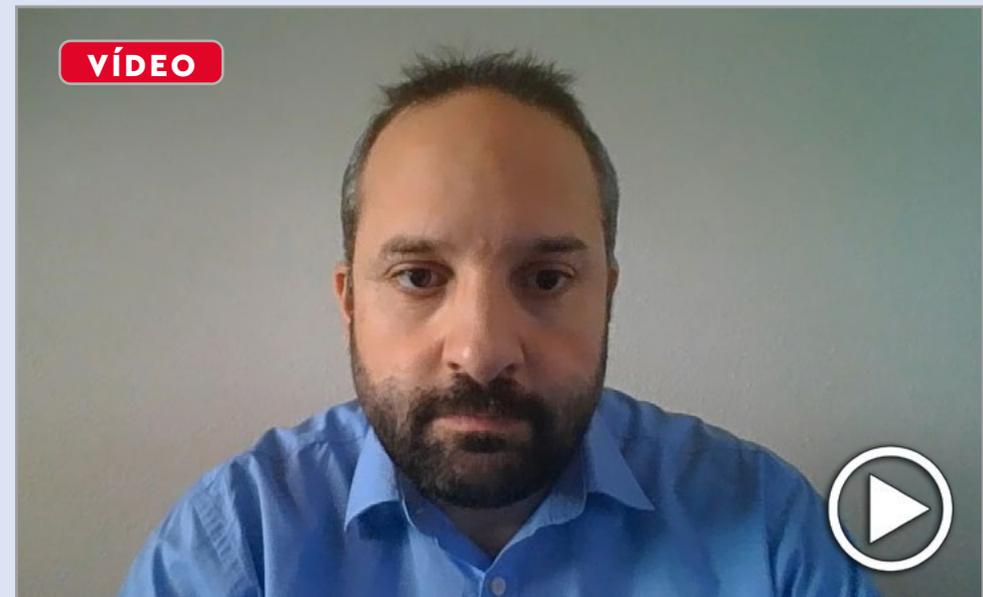
*kubernetes* de forma uniforme en cualquier entorno: centros de datos, hiperescaladores, proveedores de servicios y en el extremo.

Como analiza Eduardo Rodríguez, la apuesta de VMware por *kubernetes* se explica por la demanda, creciente, de los clientes. "Permiten, de forma muy rápida, disponer de los aplicativos, probarlos en pequeños *sites* y desarrollarlos de manera segura, observando cuál es su funcionamiento".

## "La seguridad intrínseca de VMware abre una oportunidad al canal"

Apostar por la seguridad intrínseca de VMware incrementa el valor de los proyectos que el canal de esta marca desarrolla en sus clientes. Eduardo Rodríguez, preventa de VMware en Arrow, insiste en el atractivo de la propuesta de la marca que alcanza, de manera integral y completa, todos los productos que forman parte de la oferta de VMware. "En la solución ya va integrada la seguridad; por lo que no hay que añadir nada a la infraestructura con la que cuentan las empresas".

Rodríguez, que cree que VMware ya es un jugador destacado en el campo de la seguridad, anima al canal a formar parte de este mensaje.



Eduardo Rodríguez, preventa de VMware en Arrow

## La seguridad de VMware, una nueva manera de entender la protección

Seguridad intrínseca en el propio producto, un entorno seguro unificado bajo un mismo producto y administrado desde un único punto y una política basada en el análisis del contexto configuran el terceto en el que reposa la manera en la que VMware entiende la seguridad. Eduardo Rodríguez, preventa de VMware en Arrow, explica que la manera en la que la marca entiende la protección rompe con los silos. "Su seguridad, intrínseca en todos y cada uno de sus productos, permite a las empresas proteger todos los entornos, lo que incluye el centro de datos tradicional, los entornos híbridos o la nube".



Eduardo Rodríguez, preventa de VMware en Arrow