

El canal se apunta a los



servicios gestionados de seguridad

Hacia el consumo de la seguridad como servicio: presente y futuro de los servicios gestionados de seguridad

Esta nueva década ya ha dado muchas lecciones. Una es que el mantra "Nunca dejes que una buena crisis se desperdicie" podría haber sido escrito para la fraternidad cibercriminal. Otra es que el progresivo desplazamiento de los modelos de TI de las organizaciones al entorno *cloud* y el consumo, cada vez, de más servicios en diferentes nubes está motivando el desarrollo de productos, servicios y experiencias de usuario que están basadas en los datos.

El mercado de la seguridad no ha sido ajeno a este movimiento y, sumado a la transformación del puesto de trabajo y la movilidad del empleado, está asistiendo a un cambio en la forma en la que se consumen los servicios de seguridad en las organizaciones. Según datos de IDC, alcanzará los 1.324 millones de euros en 2021 y tendrá un crecimiento del 8,1 % en el periodo comprendido entre el año 2021 y el 2024, donde los segmentos que más crecerán serán los relativos a los servicios gestionados de seguridad (30 %), la seguridad de red (22 %) y los servicios de integración (13 %).

La adopción de nube como modelo de TI predominante en la actualidad en las organizaciones (el 90 % de las empresas españolas opera en un entorno de *cloud* híbrido según datos de IDC) entrega la resiliencia necesaria para dotar de continuidad de negocio, permitiendo la agilidad necesaria en la organización para hacer frente a las condiciones cambiantes del mercado, pero a su vez complicando la gestión de la seguridad, puesto que las fronteras de seguridad se difuminan y se requiere proteger un dato que circula en un entorno *multicloud*. En este contexto, el acceso y el consumo de servicios y aplicaciones, así como la relación con el ecosistema de



José Antonio Cano,
director de análisis de IDC España

proveedores requiere ser gestionado y orquestado, requieren de una aproximación global de gestión de la seguridad, que si no se realiza partiendo de la nube, no es posible abordarlo.


“La automatización de los procesos de detección automática de amenazas imbuidos de capacidades de inteligencia artificial permite a las organizaciones incrementar la seguridad”

En este contexto, la automatización de los procesos de detección automática de amenazas imbuidos de capacidades de inteligencia artificial permite a las organizaciones no sólo anali-

zar el cada vez mayor volumen de tráfico cifrado que circula por las organizaciones, sino incrementar la seguridad. Por ello, en este nuevo escenario digital actual, disponer de una plataforma integral de ciberseguridad (inteligente) donde la empresa consume esa inteligencia a través de servicios gestionados de seguridad y servicios de integración, permite vislumbrar cómo es el destino al que las organizaciones deben dirigirse para disponer de este marco de confianza necesario que permita generar y comunicar la "confianza digital" que se requiere en esta nueva década.

Los servicios en la nube pueden ayudar a alcanzar los objetivos de negocio creando, desplegando y gestionando las cargas de trabajo en un

entorno *multicloud* integrado con la infraestructura tradicional. A medida que las infraestructuras estrechamente integradas se sustituyen por servicios gestionados y modulares en un entorno de nube híbrida privada y/o pública, las cargas de trabajo deben migrarse, optimizarse y habilitarse para obtener ventajas competitivas de las aplicaciones en la nube. Es en este escenario

donde garantizar la seguridad del dato se vuelve cada vez más complejo y necesario. 

José Antonio Cano,
director de análisis de IDC España

Tome medidas contra las ciberamenazas.



MTR

Sophos Managed Threat Response

Nuestro equipo de expertos ofrece un servicio totalmente gestionado con funciones de búsqueda, detección y respuesta ante amenazas las 24 horas.

Más allá de la simple notificación de ataques o comportamientos sospechosos, Sophos adopta medidas específicas en su nombre para neutralizar incluso las amenazas más sofisticadas y complejas.

www.sophos.com/es

SOPHOS
Cybersecurity evolved.

El desarrollo del modelo de seguridad gestionada, área destacada de crecimiento para Fortinet en 2021

“Quiero que el canal de **Fortinet** entienda el enorme **beneficio** que abre el modelo **MSSP**”

Un año después de lanzar Fortinet Engage, la compañía ha renovado su programa de canal con Engage 2.0, escribiendo un ambicioso propósito: ayudar a su canal a diferenciarse. Una iniciativa que ha vuelto a impulsar el desarrollo de los servicios gestionados como una de las máximas oportunidades para el canal.

Marilés de Pedro

Fortinet Engage ofrecía cuatro especializaciones a su canal: Dynamic cloud (que ha cambiado su denominación a Adaptive Cloud Security), LAN Edge&SD-Branch, Secure SD-WAN y Data Center. Con Engage 2.0 se han añadido tres más: seguridad en los entornos industriales, Security Operations, para la gestión óptima del SOC; y Zero Trust Access. Junto a estas especializaciones, la marca mantiene los modelos a los que el *partner* puede anclar su negocio: revendedores, MSSP o desarrollo de la nube.

Guillermo Sato, director de canal de Fortinet, explica que han flexibilizado el modelo MSSP, incluyendo distintas ventajas que incrementan el beneficio de los socios. “Cuando lanzamos Fortinet Engage nos focalizamos en aquellos con un mayor compromiso con la marca, pero ahora estamos trabajando para que todo el canal acceda a las ventajas de este modelo”. Sato incide en que es clave que se den cuenta de que se trata de un negocio con un enorme recorrido, “no para que lo aprovechen de manera puntual”.

En Engage 2.0 Fortinet ha incluido descuentos en el área del software y de las licencias de

consumo en formato SaaS para impulsar este área de los servicios. Además, la marca pone en manos del canal una enorme batería de herramientas gratuitas para complementar cada una de las soluciones que conforman su oferta. “Son herramientas de gestión, de despliegue y de operación para facilitar el negocio; lo que repercute en un ahorro de costes y en una mejora de sus beneficios”. No olvida in-

“El canal tiene que ofrecer, a través de estos modelos de seguridad gestionada, protección a las pymes”

sistir en la capacitación y la formación que “aseguran que el lanzamiento de sus servicios gestionados se lleve a cabo de la manera más rápida y eficiente posible”.



Guillermo Sato,
director de canal de Fortinet

Potenciación de su oferta

Este foco en el desarrollo del modelo MSSP conlleva una potenciación de su oferta. En este apartado el fabricante ya contaba con sus soluciones de correo electrónico y de SIEM bajo este modelo de pago por uso; y ahora ha incluido la solución avanzada para el *endpoint* (EDR) y un modelo de consumo flexible de las licencias virtuales del *firewall*. Sato recuerda que, aunque la punta de lanza sigue siendo el *next generation firewall*, el socio tiene plena li-

bertad para escoger las soluciones que mejor encajen en su negocio. "Nuestro canal debe aprovechar la ventaja que le ofrece Security Fabric, la piedra angular en la que reposa toda nuestra oferta", recuerda. "Todas nuestras soluciones están perfectamente integradas lo que permite al *partner* empezar por una solución concreta y posteriormente, complementarla de una forma muy rápida y ágil, con más opciones; gracias a una integración nativa y automatizada".

Sato reconoce que este modelo MSSP supone un cambio de paradigma importante para el canal. "Está acostumbrado, al igual que sucedía con las marcas, a un modelo tradicional, basado en la venta de licencias *onpremise*, y ahora debe modificar sus sistemas tradicionales para ofrecer un pago por uso adaptado a lo que sus clientes necesitan consumir". No es sencillo, reconoce. "Debe transformar el negocio hacia el servicio, con un pago dividido en mensualidades, controlando el consumo de las soluciones, bajo un modelo sencillo".

Un modelo completo de seguridad gestionada incluye no solo la oferta de soluciones en un formato "de servicio" sino también los servicios propios que cada *partner* les acople para complementarlas. Sato asegura que el canal de Fortinet cuenta con una oferta propia de servicios identificada con auditorías de seguridad, tareas de *testing* para identificar las vulnerabilidades de los clientes o la visibilidad de lo que ocurre en torno a la solución. "A medida que vamos extendiendo el porfolio, el canal también amplía sus servicios".

El dueto mayorista de Fortinet, compuesto por Arrow y Exclusive Networks, participa activa-



mente en este modelo de negocio. "Ambos ofrecen soporte para su desarrollo, capacitación e incluso servicios que permiten al canal esta evolución, facilitando tanto su llegada al mercado como su formación".

Objetivos en 2021

Sato, mucho más que por el número de los socios que se sumen a este modelo de negocio, está interesado en asegurar la calidad de los mismos. "Mi objetivo es que el canal entienda realmente su beneficio y cómo funcionan cada una de las soluciones que ofrecemos bajo este modelo de negocio".

El mercado español, recuerda, está compuesto principalmente por pymes,

lo que abre una enorme oportunidad a este modelo. "Son empresas que no cuentan, en su inmensa mayoría, con un responsable de TI y sufren los ciberataques con similar virulencia que las grandes empresas. El canal tiene que ofrecer, a través de estos modelos, seguridad a este tipo de empresas. La oportunidad es enorme".

Fortinet

Tel.: 91 790 11 16

Acceda al vídeo desde el siguiente código QR



"Quiero que el canal de Fortinet entienda el enorme beneficio que abre el modelo MSSP"



Buenas perspectivas para 2021

El negocio de la ciberseguridad ha sido uno de los negocios que mejor se ha comportado en los últimos meses. Este año, según IDC, el mercado de la ciberseguridad crecerá un 8,1 %, sobrepasando los 1.324 millones de euros en España. Una previsión con la que está de acuerdo Sato. "El negocio de cibersegu-

ridad ha salido muy fortalecido y mantiene su auge", reconoce. "Crecen especialmente las áreas vinculadas con la gestión de identidades y la protección de los entornos 100 % digitales". En el caso particular de Fortinet, Sato destaca el crecimiento que están experimentando las áreas SD-WAN en una

doble vertiente: la protección de estos entornos vinculada con las demandas de optimización de costes o de control de estas redes; y los proyectos en los que se vincula con SD-Branch, gracias a la integración nativa de las soluciones de acceso (*switches* y puntos de acceso), ofreciendo la conectivi-

dad de la oficina remota de forma segura, trasladando las políticas de seguridad a los puntos de acceso. Sato también apunta el negocio en torno a los NOC y a los SOC, con modelos de seguridad operada como un servicio; un área en la que Fortinet ha potenciado su oferta.

La zona ibérica presenta el crecimiento más alto en la contratación del servicio de gestión de respuesta frente a amenazas (MTR)

"Queremos que el canal de **Sophos** fortalezca su presencia en los modelos de negocio **MSP**"



Carlos Galdón,
director de canal de **Sophos**

El desarrollo del modelo de seguridad gestionada es uno de los focos de negocio prioritarios para Sophos. Un área que ha crecido en España un 64 % en su último año fiscal, concluido el pasado mes de marzo, con un ascenso del 84 % en el trimestre que lo cerraba. Carlos Galdón, director de canal de la marca, es un convencido de que es un modelo que encaja, a la perfección, en un tejido empresarial como el español, cosido en su mayoría por pymes. "Es un modelo bárbaro para ellas, por la cobertura de protección que les brinda y el modelo financiero, flexible, gracias al pago por uso".

 Marilés de Pedro

Sophos concluyó su año fiscal el pasado 31 de marzo con un crecimiento del 23 % en la zona ibérica y un 32 % en los productos que la marca engloba como "next generation". Un resultado que, como reconoce Galdón, que rige los destinos de la red de distribución de Sophos desde el pasado verano, impacta directamente en el canal. "Al ser una compañía que se rige por una estrategia 100 % indirecta, si crecemos, también lo hace de manera similar nuestra red de distribución". Galdón recuerda que la marca es una de las compañías que mejor retribuye al canal y que está empeñada en que cuente con una poderosa base de conocimiento.

Clave el desarrollo del modelo MSP

Desde hace tiempo Sophos ha puesto especial atención en el reclutamiento de MSP, compañías capaces de ofrecer la seguridad en un formato de servicio. "Uno de nuestros objetivos es que el canal acceda al mundo de los servicios y que fortalezca su presencia en los modelos de negocio MSP". El pasado año 30 nuevas compañías se incorporaron a esta modalidad, lo que ha permitido sumar 90 empresa que son capaces de ofrecer a las empresas las soluciones de Sophos bajo un formato de servicio. Galdón cree que el modelo tecnológico que exhibe la marca ayuda a implementar un modelo MSP. "Trabajamos en un modelo de nube, soportado por un portal único que permite que el despliegue de estos modelos MSP sea mucho más fácil". Las dos principales barreras que obstaculizan el acceso de los distribuidores a esta fórmula de negocio apelan a la dificultad y la complejidad en el uso de los portales y en el despliegue de las operaciones. "Sophos es una compañía obsesionada con hacer las cosas

Seguridad y amenazas

Tras el crecimiento del 8 % experimentado por el mercado de la seguridad el pasado año en España, según cálculos de IDC, en 2021 seguirá creciendo en guarismos parecidos. Carlos Galdón complementa que, incluso, otras consultoras aventuran crecimientos del 10 o 11 %. "La tendencia es al alza, sin duda, para este 2021".

La protección del teletrabajo va a seguir siendo clave. Galdón prevé que, instalados en un modelo híbrido, en la inversión, centrada el pasado año en torno a los accesos remotos y VPN, tendrá mayor protagonismo el Zero Trust.

"Las empresas van a invertir en las estrategias que defiendan la seguridad integral que, en el caso de Sophos, apuesta por el modelo de seguridad sincronizada para contar con una protección integral frente a todos los ataques: *ransomware*, *phishing*, etc."



fáciles", recuerda. "Queremos que las operaciones se lleven a cabo de una manera sencilla y que el uso del portal que permite a los distribuidores la gestión de los sistemas de seguridad de sus clientes no entrañe ninguna dificultad". Una obsesión por la sencillez que Galdón cree que es la razón principal del crecimiento que exhiben en este modelo MSP.

Servicio de gestión de respuesta frente a amenazas (MTR)

Además de la consola, Sophos Central, dentro de esta estrategia MSP es clave Sophos MTR, un servicio que fue lanzado en octubre de 2019, para fortalecer la oferta en torno al puesto de trabajo.

Un servicio totalmente gestionado con funciones de búsqueda, detección y respuesta ante amenazas que fusiona el *machine learning* con el análisis humano, lo que permite a Sophos exhibir un enfoque evolucionado de la protección de seguridad proactiva. Galdón asegura que MTR está teniendo una aceptación bárbara en la zona ibérica. "Somos la región que más está creciendo en Sophos". Un éxito que se explica por el peso, inmenso, que tiene la pyme en el tejido empresarial español. "Se trata de empresas que no tienen ni el tiempo ni el conocimiento para ocuparse de su seguridad, lo que las obliga, si quieren contar con un buen sistema de protección, a contratar este tipo de servicios", recuerda. "Vamos a ver más empre-

sas empleando y contratando servicios de ciberseguridad a través de nuestros canales de distribución".

Los servicios MTR abren la puerta a que los distribuidores ofrezcan a sus clientes una protección complementaria, y necesaria, con las soluciones EDR (*Endpoint Detection and Response*) que les permite analizar todo lo que ocurre en sus sistemas. "Gracias a los servicios MTR disfrutan de un servicio de protección completo, las 24 horas, los 7 días de la semana, gracias al control que mantienen nuestros Sophos Labs, lo que nos permite neutralizar las amenazas más sofisticadas y complejas". Es posible personalizar Sophos MTR para adaptarse a empresas de todos los tamaños y ni-

"Vamos a ver más empresas empleando y contratando servicios de ciberseguridad a través de nuestros canales de distribución"

veles de madurez. A diferencia de otros servicios de MDR que se centran en la supervisión y la notificación de las amenazas, Sophos MTR escala rápidamente el problema y toma medidas contra las amenazas basándose en las preferencias que tenga la empresa.

Los mayoristas, claves

La red de mayoristas de Sophos participa, en un 100 %, en la activación de este modelo. Sophos no puede dar un alta a un distribuidor en un servicio gestionado si éste no lo ha hecho a través

de un mayorista que, por supuesto, tiene que estar habilitado para poder venderlo. Con este mecanismo se eliminan las barreras de entrada para cualquier distribuidor. "Incluso los más pequeños, al estar amparados por un mayorista, pueden desarrollar este negocio", explica. El socio cuenta con el soporte del mayorista que le ayuda a vender el servicio y le ofrece todo su conocimiento para que la implementación esté bien hecha. "Ésta es otra de las claves que explica nuestro crecimiento en este modelo".

Objetivos

Además de mantener el alto crecimiento cosechado en el último ejercicio fiscal, Galdón insiste en fortalecer el papel clave que tiene los mayoristas en el desarrollo del modelo. "Es fundamental". Junto a esta labor, Sophos está estableciendo alianzas con compañías de mayor tamaño y con proveedores de servicio para que incorporen la oferta de Sophos. "Queremos cubrir todo el espectro de empresas".

Sophos
Tel.: 91 375 67 56

Acceda al vídeo desde el siguiente código QR



"Queremos que el canal de Sophos fortalezca su presencia en los modelos de negocio MSP"



El crecimiento del negocio de servicios gestionados creció un 32 % el pasado año

“Los servicios gestionados permiten incrementar la independencia de los socios de Trend Micro”

Los servicios gestionados señalan un área clave en el desarrollo del negocio del canal en Trend Micro. Un apartado que creció un 32 % el pasado año. Umaima Ben Bouker, *MSP channel account manager* de Trend Micro, recuerda que el objetivo de la multinacional es crear en este apartado una red de socios, fuerte e independiente. “El desarrollo de este apartado de negocio permite incrementar la independencia de nuestros socios”, explica. “Conocen los productos y, conforme van incrementando su negocio y explorando nuevas capas de seguridad en sus clientes, más independientes se hacen”.

Marilés de Pedro

Recuerda Ben Bouker que esta fórmula de negocio permite que el canal afiance su presencia en sus clientes gracias a su completa oferta de protección. “El foco es la independencia”, insiste. Un objetivo que reposa en la formación, extensible también al resto de áreas de negocio del fabricante. “Apostamos por una formación extensa y una certificación en nuestros productos. Queremos ayudar a los distribuidores a que adquieran competencias en nuevas áreas y encuentren nuevas oportunidades de negocio”.

El sí del canal

La responsable del negocio de seguridad gestionada reconoce que el número de socios que han dicho sí a este modelo aún no es suficiente. “En número, España está por detrás del desarrollo de otros mercados, incluso Portugal está un poco por delante”. Umaima Ben Bouker explica que la razón principal no es la falta de interés sino que se ha empezado más tarde. Trend Micro cuenta con un departamento interno que se encarga del reclutamiento. “Los socios que antes han abrazado este mo-



Umaima Ben Bouker,
MSP channel account manager
de Trend Micro

delo son aquellos que tienen una base de negocio en el mercado de la pyme”, explica. Han sido más receptivos a este tipo de modelo porque no tienen los recursos necesarios para dar soporte a todos sus clientes. Trend Micro basa su modelo MSP en una oferta de protección, conectada y sincronizada, que cuenta con una eficaz consola multiinquilino para orquestrarla. “Gracias a ella, el distribuidor puede gestionar, de manera centralizada y sencilla, la seguridad de todos sus clientes. Disfruta de una visibilidad completa de todo el sistema: puesto de trabajo, servidores, correo, etc.”. Asegura la responsable que los distribuidores se han percatado de que este tipo de negocio marca el futuro. “El distribuidor debe cumplir con ciertos requisitos de seguridad que le habiliten para ofrecer un adecuado nivel de servicio; lo que exige que cuenten con un equipo de expertos en la plantilla para gestionar el centro de operaciones”.

La mayoría de los distribuidores de Trend Micro exhibe un perfil híbrido. “Una parte de su negocio, identificada con los entornos corporativos, suele gestionarse bajo un modelo de negocio tradicional”, explica. La

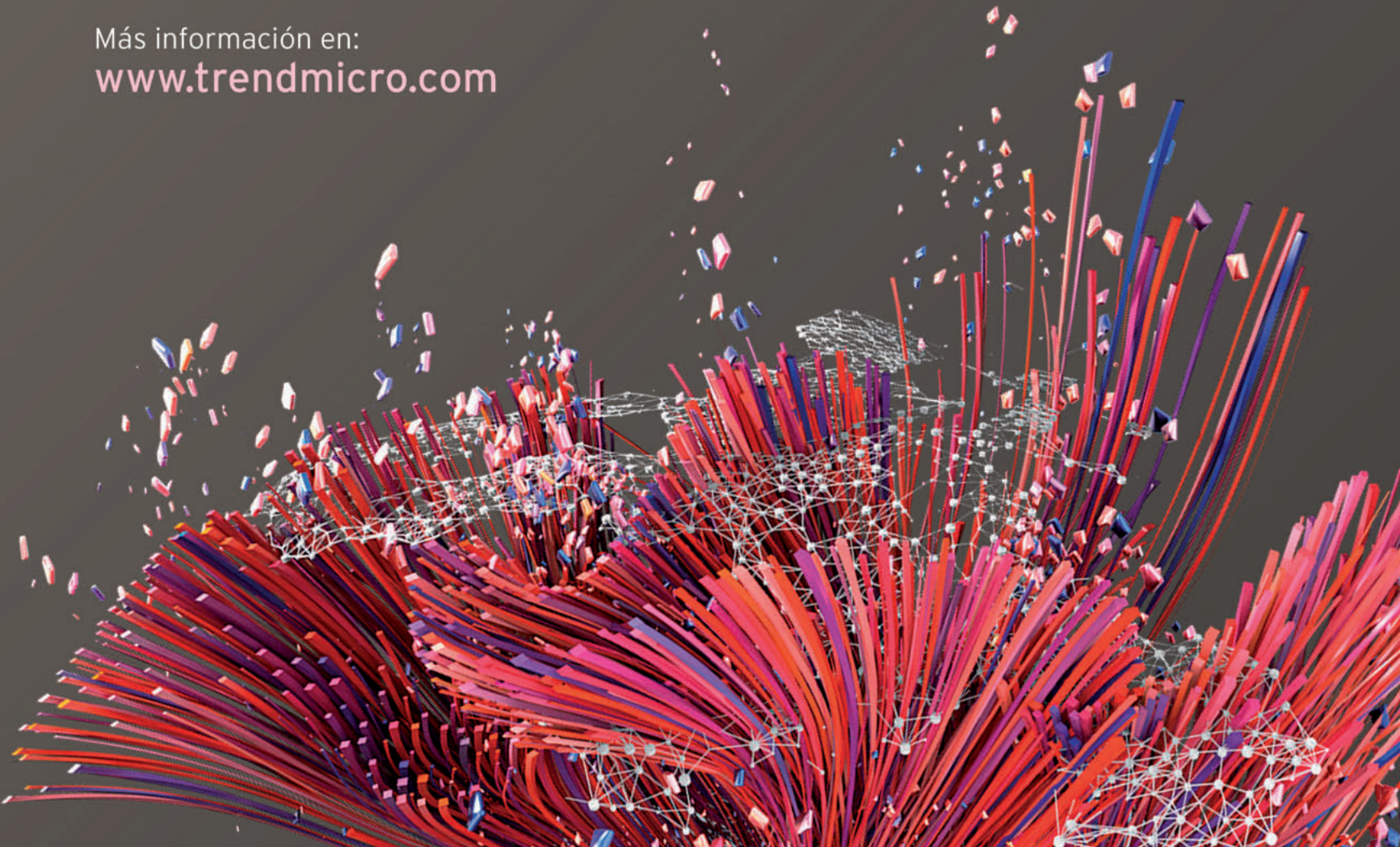
“Queremos ayudar a los distribuidores a que adquieran competencias en nuevas áreas y encuentren nuevas oportunidades de negocio”

Trend Micro Vision One™

Mayor visibilidad para una respuesta más rápida

Una plataforma especialmente diseñada para la
defensa contra amenazas que va más allá que
otras soluciones XDR

Más información en:
www.trendmicro.com





Los mayoristas, Arrow y GTI, juegan un papel importante para ofrecer soporte y formación a los distribuidores a los que, por tamaño y capacidad de capilaridad, no llega Trend Micro

gestión del mercado de la pyme, por su parte, prefieren canalizarla con una fórmula gestionada. "Ambos modelos convivirán ya que una gran parte del mercado sigue prefiriendo el modelo de seguridad más tradicional".

Los mayoristas, Arrow y GTI, juegan un papel importante para ofrecer soporte y formación a los distribuidores a los que, por tamaño y capacidad de capilaridad, no llega Trend Micro. "Ofrecen cercanía a una gran masa de distribución a la que no accedemos". Ambos dis-


ponen de un departamento específico para divulgar y desarrollar esta fórmula entre sus clientes, agrupando a todos los fabricantes que ya tienen su oferta bajo este modelo de pago por uso.

Objetivos para 2021

Tras el crecimiento del 32 % que experimentó este área de la seguridad gestionada el pasado año, Ben Bouker persigue alcanzar un ascenso entre el


35 y el 40 %. "Nuestro objetivo es llegar a todos los *partners*", insiste. "Una gran parte del negocio de los distribuidores se identifica con los servicios". Un canal al que también se han sumado, en el área de las telecomunicaciones, las grandes *telcos* que han visto una enorme oportunidad para acceder, con una oferta más completa, a su base de clientes del mercado de la pyme.

Oportunidad de mercado

Tras ser uno de los mercados que más creció en 2020, el área de la seguridad sigue presentando numerosas oportunidades. "Claramente se mantiene al alza". A juicio de Umaira Ben Bouker la seguridad en torno a las redes es uno de los apartados con mayores perspectivas de inversión. "Algunos proyectos que se quedaron estancados durante el periodo de confinamiento provocado por la expansión de la covid-19, se están reanudando". Junto a ella, la protección en torno al correo electrónico va a ser otro segmento prioritario hacia el que se dirigirá la inversión de las compañías. "Es clave proteger las conexiones de los usuarios y los servicios que las empresas tienen alojados en la nube", insiste. "Tampoco podemos olvidarnos del análisis de vulnerabilidades y del comportamiento de los usuarios". 

Trend Micro

Tel.: 91 369 70 30

Acceda al vídeo desde el siguiente código QR 

"Los servicios gestionados permiten incrementar la independencia de los socios de Trend Micro"



Mejoras en Vision One

Recientemente la marca ha incluido mejoras en Vision One, su plataforma de detección y respuesta extendidas (XDR), que proporciona una visibilidad centralizada de los riesgos y prioriza las alertas para una detección y respuesta más rápi-

das. Se trata de una evolución de esta solución que se lanzó en 2019.

Esta plataforma de defensa contra amenazas permite a las empresas detectar ataques complejos y puntos concretos de riesgo para la seguridad que

las soluciones aisladas pasan por alto. Permite ajustar las políticas de seguridad y dirigir las acciones de respuesta en todas las capas de seguridad desde una única consola. Incluye sensores diseñados específicamente para facilitar in-

tegraciones nativas con el *stack* de seguridad de Trend Micro en las capas de seguridad más importantes y también dispone de API para usar con las soluciones de terceros que ya se utilizan para complementar los flujos de trabajo.

Cómo la consolidación de la seguridad puede impulsar el crecimiento de los MSSP

Cada año, los proveedores de soluciones de TI se enfrentan a nuevos retos y buscan la manera de superarlos mientras aumentan la rentabilidad y hacen crecer sus negocios. 2021 puede estar resultando más difícil que los anteriores, ya que la pandemia sigue trastocando las operaciones empresariales, las TI y la seguridad de organizaciones de todo tipo y tamaño. Las necesidades de los clientes han cambiado y ahora están condicionadas por las realidades de una fuerza de trabajo cada vez más remota, la incertidumbre económica y mucho más.

Una de las formas más efectivas para que los MSSP puedan aumentar su rentabilidad y su crecimiento es a través de la consolidación de la seguridad. Cada vez es más importante trabajar con proveedores que ayuden no solo a mantener y aumentar las listas de clientes, sino también a ahorrar costes y incrementar los márgenes. Es más, asociarse con proveedores que permiten la consolidación puede impulsar la diferenciación competitiva y aportar ahorro de costes al simplificar los requisitos de personal, formación y certificación, así como de administración de servicios.



para cada categoría de servicios de seguridad es la mejor manera de garantizar que sus escasos recursos técnicos sean productivos. Con menos compromisos con los proveedores, las cargas de trabajo de formación, las tareas de gestión y los criterios del programa de *partners* son más fáciles de gestionar, mientras que los beneficios e incentivos son mucho más sencillos de conseguir.


2. Experiencia coherente. La compra y venta de productos y servicios de seguridad también puede ser complicada. Hay que navegar por un mar de proveedores y distribuidores que compiten entre sí, con distintos enfoques en cuanto a licencias, facturación, gestión de renovaciones y atención al cliente. La consolidación de proveedores permite racionalizarlo y simplificarlo.

3. Gestión racionalizada de la plataforma. Los MSSP más rentables no se limitan a consolidar proveedores, sino que se alinean con aquellos que proporcionan soluciones para

más de una oferta en su pila de seguridad, con una gestión centralizada. Antes de elegir un proveedor, hay que comprobar que su plataforma de gestión y sus planes para agilizar las tareas de administración y elaboración de informes son adecuados.

4. Visión unificada. La ampliación de la cartera de productos de seguridad puede contribuir a la captación de clientes y al aumento de la rentabilidad. Cuantos más proveedores trabajen con usted, más difícil será alinear las necesidades de los clientes finales y los requisitos de la cartera asociada.

Los MSSP de WatchGuard pueden ofrecer seguridad de red y servicios avanzados de protección desde una única consola de gestión en la nube. Esto permite eliminar, al menos, otras tres contrataciones de proveedores de la ecuación, al tiempo que agiliza los procesos.

La consolidación de la seguridad garantiza la contratación de *partners* que comprendan sus necesidades, reduzcan costes y generen nuevas oportunidades de negocio. Es el mejor enfoque para establecer el nivel de precios flexibles, servicios de seguridad sofisticados, experiencia en profundidad y eficiencia. Dé el primer paso en su camino hacia la consolidación, evaluando las relaciones con los proveedores existentes e identificando las carencias que podrían frenar su negocio en 2021 y en adelante. 

Javier Montes
area sales manager de
WatchGuard Technologies Spain

Cuatro aspectos claves de la consolidación de la seguridad

1. Asociaciones simplificadas. Las relaciones con los proveedores pueden ser complejas y requerir mucho tiempo de gestión. Cada uno tiene un nivel de certificaciones basado en la formación, lo que exige un mayor presión sobre sus valiosos recursos técnicos. Estos acaban atascados con una acumulación de trabajo administrativo para mantener los conocimientos que exigen los distintos proveedores. Además, deben mantener múltiples entornos de prueba. El resultado final es que se dedica más tiempo a la formación y a la administración para mantener las alianzas con los proveedores, y menos a la expansión del negocio. Establecer una única oferta de proveedores

"Queremos que el **distribuidor**, además de un proveedor de servicios, se convierta en **asesor del negocio** de sus clientes"

La estrategia de canal de WatchGuard reposa en su programa WatchGuard ONE. Un programa al que ya se han incorporado los *partners* de Panda Security que, de la misma forma que a los distribuidores que ya conformaban la estructura de canal de WatchGuard, se les abren enormes oportunidades: la solución de protección del puesto de trabajo de la compañía española se suma a la tradicional oferta de WatchGuard en torno a la protección de los entornos inalámbricos, la red (UTM) y la autenticación multifactor. Javier Montes, *area sales manager* de WatchGuard, desvela que la integración se ha desarrollado muy bien, con un periodo de transición, en el que los distribuidores de Panda Security han recibido la formación requerida para conocer las soluciones de la marca.

Partners MSSP

Dentro de este programa es clave el desarrollo de los servicios gestionados (MSSP) a través del canal. Montes apela a la flexibilidad que aporta este modelo. "No está enfocado a la oferta de soluciones, sino a ayudar a nuestros socios a que ofrezcan servicios". Para ello, reconoce, se impone un cambio de mentalidad. "Son los servicios los que permiten a los distribuidores profundizar en la relación con el cliente".

A pesar de que el desarrollo de los servicios gestionados señala el horizonte de futuro, Montes defiende la existencia de un modelo de negocio mixto en el que se conjugue esta oferta de servicios con una venta tradicional. "La Administración Pública, dinamizadora clave de la situación económica en España, aún mantiene el modelo tradicional basado en un licenciamiento a uno, tres o cinco años", recuerda. En



Javier Montes,
area sales manager de WatchGuard

Desde el pasado mes de junio, Panda Security forma parte de WatchGuard. Con ello, el fabricante norteamericano ha incorporado a su oferta su potente solución en el entorno del *endpoint*, lo que le permite exhibir una completa propuesta en el mercado de la seguridad. Una integración que abre al canal de ambas compañías, ya unificado, una enorme oportunidad de negocio, en la que el desarrollo de los servicios de seguridad gestionados se torna en pieza clave.

 Marilés de Pedro

el área privada, que también mantiene en una gran parte esta fórmula tradicional, el desarrollo de los servicios gestionados exhibe un enorme crecimiento. Buena culpa de ello, recuerda Montes, la tiene su flexibilidad. "Esta fórmula MSSP encaja a la perfección con la

complicada situación económica que vivimos", recuerda. "Permite flexibilizar el pago, crítico ahora, y ayuda a que cualquier cliente, sea del sector que sea o con las circunstancias económicas que presente, pueda acceder a una solución de seguridad a un coste razonable".

Repaso al mercado

El área de la seguridad presenta numerosas oportunidades a fabricantes, y al canal, en este 2021. Montes recuerda que la protección del segmento de las pequeñas y medianas empresas es un segmento de enorme recorrido. "Hay que seguir promoviendo que incrementen suficientes medidas de seguridad para cerrar las ventanas que dejan abiertas a los ataques", insiste. "Es clave educar, formar, a todo este tejido empresarial que es el más golpeado por la crisis económica".

La protección de los entornos del trabajo en remoto señala otro área de oportunidad. Un asunto que compete especialmente a las pymes. "Las empresas se han visto abocadas a extender las medidas de seguridad que tenían implementadas en las oficinas, a los entornos de los domicilios, que no estaban preparados". Montes reconoce que en las grandes y medianas cuentas se llevó a cabo un enorme esfuerzo que ha fructificado en que los empleados hayan podido desempeñar su la-

bor en remoto, con productividad y seguridad. "Sin embargo, hay que seguir implementando una mayor protección porque, sin lugar a dudas, el teletrabajo es una fórmula laboral que va a quedarse".

Otro sector que apunta una enorme oportunidad es la protección de los entornos inalámbricos. Montes reconoce que muchas empresas han desplegado soluciones de protección en el entorno del puesto de trabajo y en el perímetro, con opciones de autenticación multifactor. "Sin embargo, observamos una mayor ventana de riesgo en los entornos inalámbricos". Con la pyme, una vez más, como el es-

labón empresarial más débil. "Es una forma muy fácil y silenciosa de atacar a este tipo de empresas".

También insiste en la formación de los usuarios. "No solo es fundamental el conocimiento de los especialistas y del canal que despliegan la seguridad, sino de los empleados de las empresas y de los usuarios, para operar, de forma óptima, con las nuevas herramientas y aplicar buenas prácticas en materia de seguridad".



Valor ante el cliente

Junto a la flexibilidad del pago que abre este programa, los distribuidores pueden habilitar o deshabilitar servicios de seguridad, con facilidad y de manera inmediata, para adaptarse a las necesidades de sus clientes. La lista de servicios es enorme y alcanza, entre otros, la prevención de intrusiones (IPS), el control de aplicaciones, el filtrado de contenido (*Webb blocker*), el filtrado de correo no deseado (*spamblocker*), *gateway antivirus* (GAV), Reputation Enabled Defense (RED), Network Discovery APT Blocker, Data Loss Prevention (DLP) o la detección y respuesta ante amenazas (TDR), entre otros.

Los socios pueden acceder a un portal, desde donde pueden administrar las suscripciones de estos servicios, mantenerse actualizados con información, descargar materiales personalizables de marketing o acceder a documentación técnica.

Montes destaca el enorme valor de la plataforma de inteligencia de amenazas, Watch-

"Son los servicios los que permiten a los distribuidores profundizar en la relación con el cliente"

Guard Dimension, que permite a los distribuidores disfrutar de funcionalidades de control de red, para que puedan traducir la visibilidad de la misma en acciones para mejorar los sistemas de protección de sus clientes. Se trata de una plataforma que agrega datos de todos los dispositivos de WatchGuard a través de la red del cliente y transforma esos datos en información. "Los *partners* que están en un modelo de pago por uso

pueden desplegar servicios de seguridad, que no solo permiten saber qué está pasando y qué incidencias está teniendo el cliente, sino evaluar el nivel de eficiencia y de productividad de los empleados", apunta Montes.

El objetivo último es que, con esta fórmula de servicios y el porfolio de las soluciones integradas dentro del programa de MSSP, el distribuidor no solamente adquiera un perfil de "proveedor de servicios, sino que se convierta en el asesor del negocio de sus clientes", relata. "Con ello el distribuidor logra fidelizarlos".

WatchGuard

Tel.: 91 793 25 31

Acceda al vídeo desde el siguiente código QR



"Queremos que el distribuidor, además de un proveedor de servicios, se convierta en asesor del negocio de sus clientes"

