No hay seguridad sin canal

Ciberseguridad *everywhere*: presente y futuro de los servicios gestionados de ciberseguridad

El incremento de las ciberamenazas, el déficit de talento y la fragmentación de los entornos de ciberseguridad son los principales catalizadores del incremento del consumo de la seguridad como servicio en España.

Este año está resultando especialmente interesante desde el punto de vista de la ciberseguridad. Por una parte, motivado por el incremento del número y sofisticación de las amenazas de seguridad y la falta de habilidades de seguridad que obligan a las organizaciones a repensar su estrategia de ciberseguridad, y por otra, la reciente guerra de Rusia y Ucrania, que está multiplicando los ciberataques (especialmente a entidades financieras e infraestructuras críticas), con crecimientos de hasta un 56 % en el número de ciberataques en los últimos dos meses.

Este crecimiento del número y variedad de ciberataques (cada día se producen más de 200.000 ataques de *ramsonware*) hace que se requiera una mayor diversidad de defensas. Por ello, las organizaciones buscan mejorar la seguridad de su infraestructura de red y recibir servicios avanzados de asesoramiento para proteger adecuadamente sus organizaciones. Por otra parte, la escasez de habilidades de seguridad y la dificultad y los gastos de reclutamiento y retención de profesionales de seguridad cualificados de un grupo de mano de obra finito (así como la importancia de evitar el agotamiento de los analistas de seguridad), están llevando a las organizaciones españolas a adoptar nuevos enfoques de seguridad que mejoren la seguridad de su infraestructura de red, así como servicios avanzados de asesoramiento que ayuden a proteger adecuadamente sus organizaciones.

El mercado de la seguridad en España refleja esta transformación de las organizaciones, donde se produce un desplazamiento de la seguridad perimetral hacia la seguridad del dato. En concreto, las prioridades para este año en la empresa española (en materia de ciberseguridad) están estructuradas alrededor de la confianza digital (aspecto clave de las empresas que debe medirse, y parte de ello está relacionado con la seguridad y privacidad de los datos), la resiliencia empresarial (entendida como "empresa mínima viable" o lo que es lo mismo: la infraestructura, el acceso y los datos necesarios para que los procesos críticos de la empresa sigan funcionando en cualquier situación), así como la soberanía de los datos, especialmente importante en Europa con las regulaciones locales y de la UE.

Estas tres prioridades afectan de manera directa a la cartera de seguridad de los proveedores y sus enfoques tienen un impacto material en la evolución comercial y estructural de las plataformas, los productos y los servicios; por ejemplo, la seguridad como servicio.

De esta manera, en un entorno híbrido *multicloud* que es donde confluirá el tráfico de datos, el consumo de los servicios de seguridad se dará a través de servicios gestionados de seguridad y de integración. De manera concreta, con un crecimiento respecto del año pasado del 7,7 %, IDC prevé que el mercado de seguridad en España alcanzará los 1.749,3 millones de euros en 2022 y para el año 2025 podría superar la barrera de los 2.200 millones de euros, manteniendo ritmos de crecimiento similares que se acercan al doble dígito. Los segmentos de mayor crecimiento son los relativos a servicios gestionados de seguridad (11,8 %), servicios de integración (11,8 %) y servicios de red (10,6 %).

El auge del consumo de la seguridad como servicio se dará de manera decidida en las organizaciones como alternativa para abordar la fragmentación de los entornos de seguridad actuales, así como para paliar el aumento de la complejidad de las infraestructuras y el ritmo al que surgen las nuevas tecnologías y amenazas.

José Antonio Cano
Director de análisis de IDC

Los socios apuestan por la certificación en Samsung Knox

La seguridad es una parte esencial en la nueva era móvil y el canal apuesta por una mayor formación en este ámbito. En lo que llevamos de 2022, nuestros socios han realizado un 173 % más de cursos con respecto al año pasado.

Tras dos años de transformación en nuestro tejido empresarial por la pandemia, las empresas han comprobado los beneficios que les aportan las tecnologías móviles. Desde la agilización y control en tiempo real de las operativas hasta la respuesta inmediata al usuario; la movilidad ha dado como resultado una mejora en la toma de decisiones y, por lo tanto, una mayor productividad, eficiencia y competitividad.

La seguridad se ha convertido en un eje fundamental dentro de la digitalización. Todos los procesos de negocio deben desarrollarse con fiabilidad y la información corporativa debe estar protegida ante cualquier tipo de ataque o intromisión por parte de terceros.

En Samsung, la seguridad forma parte intrínseca de nuestro porfolio. Samsung Knox se incluye de fábrica en nuestros dispositivos, que están protegidos desde el chip hasta el software. Por otro lado, sabemos que las amenazas crecen y se transforman muy rápidamente. Nuestro equipo de I+D, formado por un 25 % de la plantilla, analiza las vulnerabilidades más sofisticadas y continúa desarrollando las capacidades de Knox. El mejor ejemplo es Samsung Knox Vault, incluido en la gama S22, que incluye un procesador y una memoria seguros que aíslan por completo los datos sensibles del sistema operativo, como contraseñas, datos biométricos o claves de Blockchain.

Nuestros socios de canal también son muy conscientes de la importancia de la seguridad. Empresas de todo tipo acuden a ellos como los principales referentes en digitalización; y conocen muy de cerca sus necesidades y preocupaciones. El año pasado adquirieron un grado muy elevado de especialización por la demanda de sus clientes y este año la tendencia sigue en crecimiento. En lo que llevamos de este año, España es el segundo país de Europa con más cursos realizados en nuestra plataforma de formación *(Samsung Business Academy)*, un 173 % más con respecto a 2021. Además, somos el tercer país de Europa en conseguir un mayor número de certificaciones.

En definitiva, el canal de distribución sigue formándose en productos y soluciones, no sólo para cumplir con la demanda de la industria, sino también para formar parte de nuestro programa de canal SMVP *(Samsung Mobile Valued Partner Programme)*. El canal sabe que el verdadero valor de una propuesta comercial va más allá de las especificaciones de un dispositivo y se asienta en la seguridad y soluciones que aporta un ecosistema móvil.

Samsung es un socio de confianza para la transformación digital de las empresas, ya que somos uno los principales fabricantes móviles que ofrece una seguridad de vanguardia, a través de Samsung Knox. Colaboramos con INCIBE en España y nuestros dispositivos están certificados por el CCN.

Para nosotros es una satisfacción que nuestros socios puedan apoyarse en nuestras soluciones para cumplir con las necesidades y expectativas de sus clientes. El aumento de las formaciones en seguridad demuestra que quieren ofrecer un servicio de calidad y ser los mentores de todas las empresas que están abordando su transformación digital. Gracias a Samsung Knox pueden ofrecer soluciones de vanguardia a sus clientes y convertirse en una parte esencial de la digitalización de las empresas españolas.

Anna Coll
Responsable de canal en **Samsung Electronics**

SD-WAN, la nube, el desarrollo de la seguridad gestionada y la protección de los entornos industriales, oportunidades para el canal

"Es el mejor momento para ser parte del ecosistema de *partners* de Fortinet"

Guillermo Sato, director de canal de **Fortinet**

Reconoce Guillermo Sato, director de canal de Fortinet, el excelente año fiscal que cerró la compañía el pasado 31 de diciembre. A nivel mundial la compañía facturó 4.180 millones de dólares, lo que supuso un potente ascenso del 35 %. Sin desvelar, como es norma en la casa, cifras locales, el responsable de canal explicó que la estrategia de Fortinet está perfectamente alineada con las tendencias del mercado: el desarrollo de SD-WAN, la protección de los entornos del teletrabajo, la expansión de la seguridad en la nube y la consolidación de los modelos de seguridad gestionada. Áreas que señalan las máximas oportunidades en este 2022.

Marilés de Pedro

Ha sido un año espectacular", insiste. Sato señala la enorme expansión que ha experimentado el área de SD-WAN, donde Fortinet ha conseguido situarse como líder en el apartado que Gartner define como WAN Edge Infrastructure. Un negocio cuyos proyectos se vinculan en muchas ocasiones con el área SD-Branch. "Gracias a la integración nativa de las soluciones de acceso (*switches* y puntos de acceso), es posible ofrecer una conectividad segura de la oficina remota, trasladando las políticas de seguridad a los puntos de acceso", explica. Una convergencia que permite que un proyecto de SD-WAN se multiplique por dos o por tres. "La red, por tanto, ejerce de palanca", explica. "Nuestro canal tradicional, vinculado con la ciberseguridad, ha observado un complemento y una oportunidad de negocio en el área de las redes". De hecho, el acercamiento de Fortinet a estas soluciones lleva el nombre de Network Security, lo que apela, directamente, a la seguridad de red. En España, Fortinet ya cuenta con 16 *partners* que exhiben la especialización en SD-WAN. "Se trata de un negocio que nació unido al ahorro de costes y que está evolucionando hacia el control de los datos y de las aplicaciones", explica. A su juicio, SD-WAN está en la agenda de inversión de los responsables TI de las compañías. Una aseveración refrendada por el hecho de que en la facturación de la multinacional más del 16 % estuvo vinculada con una SD-WAN segura en 2021.

La consolidación de la plataforma Security Fabric, que aúna soluciones perfectamente integradas que llevan la protección hasta el último rincón, también ha sido clave. Una estrategia que, como recuerda Sato, casa a la perfección con el concepto de ciberseguridad Mesh que entona Gartner. "Es una arquitectura que, aplicando la máxima automatiza-

ción, simplifica las tareas de adquisición, operación y soporte".

Los buenos resultados han permitido ampliar el equipo local, con incorporación de profesionales para el negocio en áreas como la seguridad de los entornos industriales o para el desarrollo de la nube. También ha crecido la plantilla destinada a dar soporte al canal.

Repaso al programa de canal

Hace un par de años la marca lanzó su programa de canal, Fortinet Engage, que un año después se actualizó a Engage 2.0. Un programa que reparte a los *partners* en cuatro categorías: Advocate, Select, Advanced y Expert. "Contamos con un amplio canal; con *partners* especializados y perfiles muy diferentes".

En el último año el canal ha incrementado el número de compañías que lo conforman, tanto en el segmento de la pyme como en el área *enterprise*. "Ha crecido la facturación media de los *partners*", asegura. "Todos los *partners* han crecido con Fortinet".

El programa permite a los *partners* adoptar diferentes modelos de negocio: el desarrollo de la seguridad en la nube, la reventa de hardware y la oferta de servicios gestionados. Fortinet les ofrece herramientas y la capacidad para que se diferencien, con el objetivo último de que mejoren su beneficio. "No se trata de que seleccionen entre un modelo u otro, sino de que escojan lo que mejor les encaje", explica.

El negocio MSSP ha tenido un enorme desarrollo. "Está creciendo muchísimo", desvela. El panorama de mercado, valora, es muy propicio. "Más del 40 % de las pymes no tiene ningún tipo de concienciación o especialización en temas de seguridad. Viven ajenas al mundo de la ciberseguridad". Un dato, contundente, que se une al hecho de que más del 65 % de las medianas y las pequeñas cuentas reconocen que han sido atacadas. "Muchas de estas compañías no tiene un responsable de TI. Mucho menos alguien con conocimiento en el área de la seguridad; lo que propicia que sea un segmento en el que encaja a la perfección el modelo de seguridad gestionada".

Prácticamente la totalidad de las soluciones de Fortinet está accesible en un formato de pago por uso. "No se requiere ningún desembolso inicial. Las empresas conocen cuál es el coste y qué beneficio pueden esperar".

Fortinet llevó a cabo una encuesta a principios de año entre sus *partners* de EMEA en la que cerca del 80 % aseguraba que ya tenía en mente o estaba desplegando servicios gestionados de ciberseguridad. En España, aunque el grupo de *partners* que se declaran formalmente MSSP está conformado por una treintena de compañías, Sato asegura que están trabajando, bajo este modelo, con cientos de *partners*. "España está siendo punta de lanza en Europa ya que de esos 30, alrededor de 8 están impulsando soluciones más allá del negocio más tradicional de Fortinet, identificado con el *next generation firewall*, como es el caso del *email*, WAF, DDR o SIEM", desvela.

> "Ha crecido la facturación media de los *partners*"

Explosión del negocio de la nube

El desarrollo del área de la nube es uno de los focos de negocio prioritarios. El año pasado Fortinet simplificó el acceso a este modelo y ha seguido facilitando a los *partners* tradicionales su evolución hacia este mercado. "El canal tradicional volcado en el desarrollo de la seguridad y las redes no tiene absolutamente nada que ver con los *partners* nacidos en la nube. Está focalizado en el despliegue de la seguridad pero no conoce las particularidades de cada uno de los hiperescalares. Y, al contrario, los *partners* especializados en los entornos de la nube nos aportan un enorme valor pero la seguridad no forma parte de su negocio", analiza. El programa de canal de Fortinet ofrece un *go to market* generalizado para todos, con formaciones específicas para cubrir esas carencias. "Ya contamos con una decena de *partners* tradicionales que están evolucionando hacia la seguridad en la nube".

La marca ha simplificado los requisitos para que los *partners* especializados en los hiperescalares consigan las certificaciones que les den acceso a la seguridad. Sato asegura que ya están empezando a trabajar con alguno de los *partners* más relevantes de cada uno de los hiperescalares (Azure, AWS y Google).

Batería de especializaciones

A las tradicionales especializaciones del programa de canal (Adaptive Cloud Security, LAN Edge&SD-Branch, Secure SD-WAN y Data Center), Fortinet unió el año pasado tres más: seguridad en los entornos industriales, Security Operations, para la gestión óptima del SOC; y Zero Trust Access.

Sato reconoce una buena cobertura en SD-WAN y en el área de acceso. "Está en auge la certificación de Zero Trust Access. Ante el auge del teletrabajo y la digitalización del negocio el perímetro ha desaparecido por lo que resulta fundamental controlar a qué datos y aplicativos se accede. El canal está viendo la oportunidad".

También está en plena expansión la especialización de protección de los entornos industriales, un área en la que han reforzado el equipo con profesionales con un alto conocimiento en este apartado. "Ya somos un referente", asegura. "Aunque nuestra madurez en este apartado es menor, contamos con importantes referencias en el despliegue de esta protección; por lo que es clave contar con *partners* especializados para que sean realmente la punta de lanza con la que ir de la mano a proyectos específicos y complejos". Por último, la protección del *cloud* también está creciendo de manera importante.

Fortinet
fortinet.com

Los mayoristas, claves

Con un negocio que transcurre en su totalidad a través del canal, Arrow y Exclusive Networks conforman el dueto mayorista. En este 2022 van a jugar un papel especial en el desarrollo del negocio de la pyme. También en la expansión de los modelos de seguridad gestionada y en la protección de los entornos de la nube.

"Su papel es esencial", reitera. "Su compromiso para extender el número de certificaciones en el canal es muy importante".

WatchGuard quiere incrementar su cobertura de canal

"Cada vez más, nuestro canal está desarrollando una venta cruzada"

Carlos Vieira,
country manager de **WatchGuard** en España y Portugal

WatchGuard quiere crecer a doble dígito este año. Tras dos excelentes ejercicios para el mercado de la seguridad, en este 2022 todo apunta a que siga creciendo y la marca quiere seguir incrementando su negocio y su participación en el mercado. Su canal es pieza fundamental para lograrlo. Tras un 2021 en el que la integración entre los canales de WatchGuard y la "antigua" Panda Security ha continuado, en este 2022 el foco principal va a estar puesto en potenciar la venta cruzada entre las diferentes soluciones del fabricante.

Marilés de Pedro

La estrategia de canal de WatchGuard reposa en su programa WatchGuard ONE. Una iniciativa que ha acogido a los distribuidores de Panda Security y que persigue la completa integración de socios y negocios. Tres son las áreas prioritarias. La primera y principal es la potenciación de la venta cruzada. "Permite al *partner* mantener a su cliente lo más protegido posible", recuerda Carlos Vieira, *country manager* de WatchGuard en España y Portugal. "Hay una tendencia clara hacia los servicios XDR, que permiten contar con una solución de seguridad sincronizada que incluye el perímetro, el puesto de trabajo y el área de la nube".

Durante el pasado 2021 prosiguió la integración de los canales. "Los distribuidores están percibiendo la enorme oportunidad que se les abre con nuestra oferta, ahora mucho más extensa con la incorporación de las soluciones del puesto de trabajo", recuerda.

Muchos *partners* de Panda Security han abierto su negocio a las áreas de autentificación multifactor (MFA), de seguridad de red y de protección inalámbrica de WatchGuard. Y, al contrario. "Hemos obtenido resultados muy interesantes en esta venta cruzada durante 2021", desvela. "Sin embargo, apenas estamos en la primera fase de esta estrategia".

Junto a esta venta, Vieira señala la importancia de aumentar la cobertura del canal. "Tenemos que conseguir que los *partners* incrementen sus operaciones con WatchGuard, comprando más de manera regular. Hay que ganar participación de mercado, bien a la competencia o tratando de ganar nuevos clientes que contaban con una protección insuficiente". Por último, es esencial retener a los *partners*.

Tirón de la autenticación multifactor (MFA)

Junto al desarrollo de las soluciones del puesto de trabajo, que fue una de las áreas que más creció el pasado año, el área de la autenticación multifactor (MFA) señala un apartado con un enorme crecimiento. "Ha crecido de manera exponencial el número de empresas que han percibido el valor de contar con este tipo de soluciones", desvela. Muchas pymes, continúa, ya cuentan con una solución MFA, muy económica de implementar, y que mitiga un gran nú-

mero de problemas en el acceso a los dispositivos, a las aplicaciones corporativas (ya sea en la nube u *onpremise*) o al puesto de trabajo remoto.

WatchGuard ha conseguido casi duplicar la facturación en esta línea de negocio en el primer trimestre de 2022. "Ha sido clave el conjunto de *partners* que vienen del mundo Panda y que, adoptando un modelo de venta cruzada, han comercializado estas soluciones". Vieira prevé que esta tendencia de crecimiento va a continuar. "La facturación todavía es pequeña pero el ascenso es enorme. Cada vez tendrá un mayor peso en nuestras líneas de negocio".

Desarrollo de la seguridad gestionada

El despliegue de la seguridad gestionada es otro área de foco prioritario. "Los *partners* tienen que dar el salto hacia estas fórmulas de negocio", explica. La seguridad es cada vez más compleja, recuerda, y faltan recursos especializados en el mercado. "Las empresas pequeñas, sobre todo, no tienen capacidad para contar con profesionales en sus plantillas dedicados a la protección de sus sistemas".

A su juicio, los modelos de venta tradicionales, en los que el canal hacía la instalación y "desaparecía" del entorno del cliente, van a disminuir. "La creciente complejidad que va ganando la seguridad requiere que los *partners* cuenten con SOC, más o menos grandes, que les permitan ofrecer a sus clientes estos modelos".

Ahora bien, no todos los clientes van a optar por fórmulas gestionadas. "Habrá espacio para todos", prevé. En WatchGuard, sin embargo, continúan evangelizando para que los *partners* abracen estas fórmulas. "Quien no las dé, va a tener más complicado el negocio en los próximos años".

Dentro de la amplia oferta de la marca para estos servicios,

> "Los distribuidores están percibiendo la enorme oportunidad que se les abre con nuestra oferta, ahora mucho más extensa con la incorporación de las soluciones del puesto de trabajo"

Vieira señala que son las áreas del puesto de trabajo y de la seguridad perimetral las que presentan más facilidades para que un *partner* se inicie en estos modelos. "No tiene sentido ofrecer un servicio gestionado en el puesto de trabajo que no se despliegue también en el perímetro, en los entornos del *cloud* o de SD-WAN", razona. WatchGuard ha realizado una gran inversión para permitir la integración con herramientas de SIEM, de monitorización o provisión de servicios, por ejemplo.

WatchGuard
watchguard.es

Acceda al vídeo desde el siguiente **código QR**

"Cada vez más, nuestro canal está desarrollando una venta cruzada"

Panorama de amenazas

WatchGuard evaluó el panorama de amenazas que marcó el último trimestre de 2021 con un informe en el que el equipo de investigación de la marca encontró un número récord de detecciones de *malware* evasivo. Las amenazas avanzadas aumentaron en un 33 %, lo que indica un nivel de amenazas *zero-day* más alto que nunca.

Las detecciones de red también continuaron con una trayectoria ascendente, lo que pone de manifiesto la complejidad de la seguridad en este entorno. Los especialistas de WatchGuard señalan que se siguen atacando viejas vulnerabilidades. Además, al crecer las redes de las organizaciones, a medida que se conectan nuevos dispositivos, las viejas vulnerabilidades quedan sin parchear, por lo que la seguridad de la red se vuelve más compleja.

WatchGuard señala que las amenazas de *malware* se detectaron en EMEA a un ritmo mucho mayor que en otras regiones del mundo. De hecho, en esta zona se detectó *malware* por los Firebox (49 %) a un ritmo casi o superior al doble de otras regiones del mundo (América 23 % y APAC 29 %).

Otra de las conclusiones es que el 78 % del *malware* enviado a través de conexiones cifradas es evasivo. En general, el 67 % de las detecciones de *malware* llegó a través de una conexión cifrada, y dentro de esas detecciones de *malware*, el 78 % era amenazas *zero-day* evasivas que eluden las detecciones básicas. Esto continúa la tendencia observada en trimestres anteriores. Estas amenazas a menudo pueden detenerse en el perímetro configurando los *firewalls* para descifrar y analizar el tráfico entrante, un paso que, por desgracia, muchas organizaciones no dan. "Durante dos años hemos abandonado la seguridad en la red ya que nos hemos enfocado en el puesto trabajo", analiza Carlos Vieira. "Seguimos viendo clientes que no tienen una solución de UTM, ni una solución de *firewall*, ni de servicios en el perímetro de *antimalware* avanzado o de servicios para mitigar el *phishing*. De ahí este aumento de amenazas en la red".

España es el segundo país de Europa con más cursos de seguridad dirigidos al canal

"La ciberseguridad es el eje fundamental de la transformación digital"

El canal percibe la enorme oportunidad que hay en torno al mercado de la seguridad. Como bien recuerda la responsable de canal, los procesos de transformación digital que se han acelerado en los dos últimos años, no solo implican la adquisición de terminales, sino otros aspectos básicos como la formación en herramientas digitales o la protección. "La ciberseguridad es el eje fundamental de esta transformación digital".

España es el tercer país de Europa con más *partners* certificados

Seguridad y canal

Samsung Knox es el pilar de la estrategia de seguridad de Samsung. Una plataforma disponible en todos los dispositivos de la marca, desde la gama de entrada hasta los equipos *prémium*; protegiendo desde el chip, a nivel de hardware, hasta el software del dispositivo. Samsung cuenta con Business Academy, un portal donde los *partners* tienen acceso a sesiones de formación de las soluciones y a la certificación en la plataforma Knox, para acceder a su comercialización y gestión.

La marca cuenta con tres certificaciones en seguridad. Associated, una certificación que dura unos 45 minutos, y que explica qué es Knox y qué usos ofrece en el ámbito empresarial. "Cuando un *partner* está comercializando

Anna Coll,
B2B Channel Sales manager de **Samsung**

En Samsung la seguridad, que lleva el nombre de su plataforma Samsung Knox, va unida inexorablemente a la movilidad. Desde hace años ha sido obsesión de la multinacional incorporar a su canal "móvil" a este negocio, lo que le ha llevado a desplegar una exhaustiva formación a través de su Business Academy. Una labor que se ha visto recompensada por el nutrido grupo de *partners* que contaban, a final de 2021, con alguna de las certificaciones en Knox. Un número que situó a España en cabeza de Europa. Anna Coll, *B2B Channel Sales manager* de la multinacional, asegura que la seguridad ya está integrada en el discurso de negocio del canal.

Marilés de Pedro

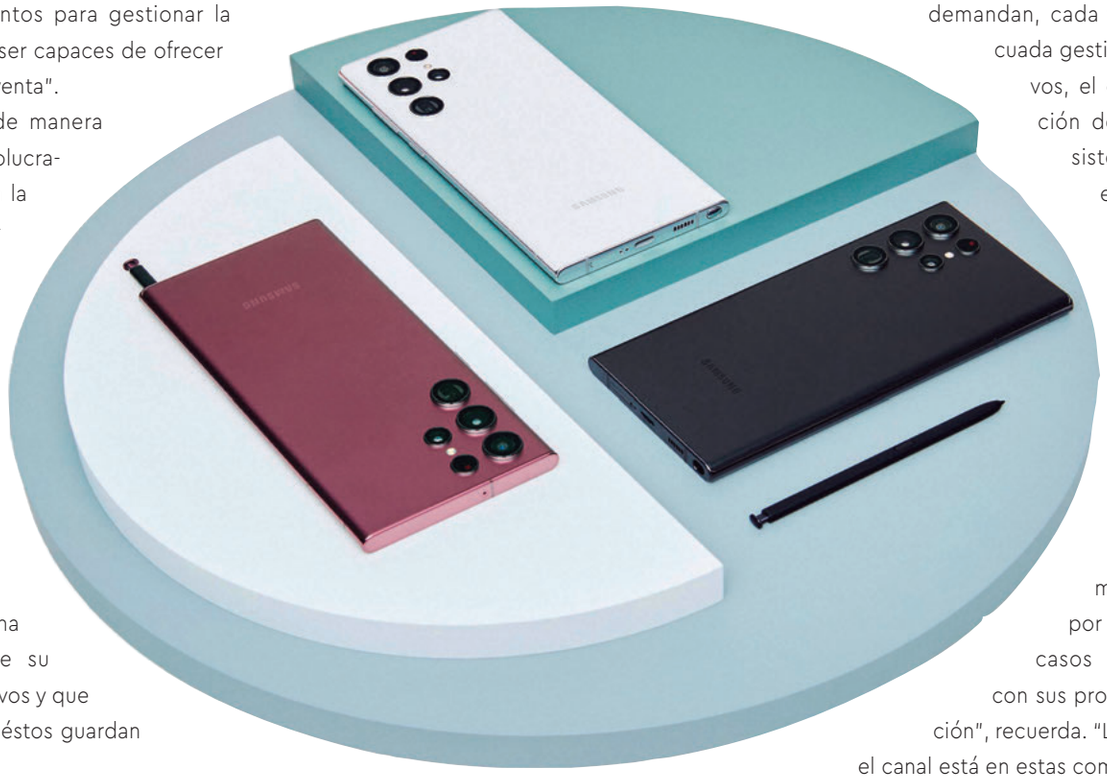
nuestros dispositivos, no solo debe referirse a las especificaciones de los mismos, sino ser capaz de apelar al concepto de solución. La certificación les pueda ayudar en esta labor". Knox Professional, con una duración de unas dos horas, está más enfocada a profesionales comerciales con perfiles con un cierto grado técnico. La más completa es Knox Expert, que se alarga durante dos días, y que se imparte en inglés desde el centro de Samsung de I+D en Polonia. Está absolutamente destinada a los equipos técnicos, que deben aprobar un examen posterior, y es obligatoria para todos aquellos *partners* que quieran comercializar licencias Knox. "Deben tener suficientes conocimientos para gestionar la consola de Knox y ser capaces de ofrecer un servicio de posventa".

Anna Coll valora de manera muy positiva la involucración del canal con la seguridad. El pasado año España se situó como el país de Europa con más socios certificados. "Los *partners* están viendo que sus clientes, en sus procesos de digitalización, exigen una segura gestión de su parque de dispositivos y que la información que éstos guardan esté protegida".

En el primer tramo de este 2022, España se ha situado como el segundo país de Europa con más cursos realizados (más de 500), lo que supone un 170 % de crecimiento respecto al mismo periodo del año pasado. En cuanto al número de certificaciones, es el tercer país con más *partners* certificados. "Hay que seguir impulsando que los *partners* se certifiquen en este tipo de herramientas", insiste.

Coll puntualiza, consciente del alto compromiso y conocimiento, que no es obsesión del equipo de canal que los *partners* obtengan su certificación en Expert. "Pero sí les empujamos a que consigan la Associated o la Profesional", puntualiza. "Y les incentivamos a ello desde nuestro programa de canal". Para establecerse en alguna de las categorías del mismo (Platinum, Gold, Silver y Registered), es indispensable contar con alguna certificación y haber cursado formación en la academia.

> "Es muy importante conseguir que los *partners* que cuenten con alguna certificación en Samsung Knox la renueven cada año"



Coll recuerda que la seguridad exige una formación continua. Hay que mantenerse al día, más en materia de protección, con un panorama cada vez más complejo y en el que las amenazas siguen creciendo. Aunque las certificaciones tienen una validez de dos años, Samsung pide a su canal que las renueve cada año. "Tenemos que mantener, como mínimo, el mismo número de certificaciones que conseguimos el pasado año", desvela. "Es muy importante conseguir que los *partners* que estén certificados las renueven, lo que demostraría su grado de satisfacción con Samsung". Junto a ello, el objetivo de incrementar, en la mayor medida posible, el número de *partners* nuevos que se sumen a este negocio. "Espero que acabemos el año como el primer país de Europa en número de *partners* certificados", sonríe.

Grandes oportunidades

Coll no ve barreras a la expansión de la seguridad en el canal. "Está viendo que sus clientes demandan, cada vez más, una adecuada gestión de sus dispositivos, el control y actualización de las versiones de sistemas operativos, etc.". Unos *partners* que despliegan su cobertura desde el autónomo hasta la gran cuenta, con "parada" en la pyme, el segmento, a juicio de la responsable de canal, que más recorrido tiene por cubrir. "En muchos casos están arrancando con sus procesos de digitalización", recuerda. "La oportunidad para el canal está en estas compañías".

Samsung
samsung.com

Acceda al vídeo desde el siguiente **código QR**

"La ciberseguridad es el eje fundamental de la transformación digital"

El desarrollo del canal es básico en el despliegue de la seguridad

"La seguridad ya es parte del ADN de VMware"

Ya nadie duda del decidido foco de VMware en el segmento de la seguridad. Con la enorme ventaja que le permite su privilegiada, y cada vez más extensa posición en los sistemas tecnológicos de las empresas, la marca ha reivindicado su particular filosofía en el entorno de la seguridad que lleva el apellido de intrínseca. Su canal, como ha sucedido en cada uno de los "nuevos" mercados hacia los que ha extendido su primigenia oferta, es pieza básica en este seguro despliegue.

Marilés de Pedro

La seguridad que defiende VMware se engarza 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. Francisco Verdugo, *senior partner solution engineer* de VMware, explica que la seguridad intrínseca responde a un enfoque apoyado en varios pilares. "El objetivo es incluir la seguridad en todas y cada una de las soluciones que tenemos en nuestro portfolio, que es enorme". No se trata, especifica, de incluirla como una capa superpuesta. "La seguridad forma parte del ADN de VMware".

Una seguridad basada en el contexto y que busca la máxima simplicidad. "No tanto en las firmas, la seguridad debe estar basada en el contexto, en el análisis del dispositivo que se utiliza, los procesos del sistema, los usuarios, la red que se utiliza, etc.". Un contexto que permite una toma de decisiones mucho más inteligente y eficiente, interceptando, incluso, ataques y amenazas no conocidas. "Incluso en la capa del hipervisor es mucho más fácil disfrutar de visibilidad en un entorno virtualizado o *cloud* que tenga nuestro *stack*", determina.

Pilar fundamental es permitir la interconexión entre distintos silos. "Hay que hacer cómplices a los profesionales que desarrollan su labor en el entorno de la infraestructura y de las redes", explica. El análisis del contexto permite detectar las vulnerabilidades sin consumir recursos, ni llevar a cabo un análisis de red. "Los procesos se simplifican y se rompe con los silos".

> "No tanto en las firmas, la seguridad debe estar basada en el contexto"

Engarzada también 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.

Foco en el canal

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. "Necesitamos que los *partners* se habiliten tanto a nivel comercial como técnico", reconoce Verdugo.

La marca quiere ampliar su capilaridad, alcanzando a todo tipo de *partners*. Una labor que

tiene en el canal mayorista un aliado fundamental. "Son nuestro brazo extendido para detectar y formar a nuevos *partners*".

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 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 %.

Francisco Verdugo,
senior partner solution engineer de **VMware**

"Necesitamos que los *partners* se habiliten tanto a nivel comercial como técnico"

Oportunidad en seguridad

Aunque la proa principal del crecimiento de VMware señala al desarrollo del área de las aplicaciones emergentes y, por supuesto, la implantación de los modelos *multicloud*, la seguridad es una enorme área de oportunidad. "Año a año seguimos creciendo tanto en facturación como en el número de *partners* que conocen nuestras soluciones de seguridad", señala. "Siempre hay muchas oportunidades para crecer ya que la seguridad está vinculada a todas las áreas de negocio: acompaña a todos los casos de uso y a todas y cada una de las soluciones que ayudan a nuestros clientes en su día a día".

VMware
vmware.es

Acceda al vídeo desde el siguiente **código QR**

"La seguridad es parte del ADN de VMware"

Enorme oportunidad

El negocio de la ciberseguridad es uno de los más boyantes del universo tecnológico en los últimos años. A finales del pasado año, IDC hacía sus previsiones para este 2022 y preveía que el negocio en torno a la seguridad en España se incrementaría un 7,7 %, con un 8 % de ascenso hasta 2024. "La ciberseguridad, no solamente en nuestro país sino a nivel mundial, es cada vez más importante. En el caso de España, además, es más relevante ya que se parte de un modelo en el cual se ve a la seguridad como un gasto, no como una inversión". Sin embargo, Francisco Verdugo reconoce que las empresas españolas, sobre todo las pymes, se han dado cuenta de que cada vez es más importante tener una estrategia de seguridad.

Verdugo pronostica un enorme crecimiento para este apartado ya que se ha extendido a todos los ámbitos. "Incluso los desarrolladores empiezan a tener en cuenta la seguridad desde la fase de diseño de sus programas y sus aplicaciones",

Ya hay tecnologías en las cuales el modelo de seguridad está incluido como diseño. "Se está abriendo cada vez más espectro, la seguridad se incluye dentro de la propia *cloud* o cómo se protegen los servicios o las aplicaciones".

¿Por qué incluir el *threat hunting* en su *portfolio*?

Crece el interés por el *threat hunting*. Según Pulse, el 32 % de los responsables de TI afirma que sus organizaciones planea reforzar su postura de seguridad de los *endpoints* añadiendo un programa de *threat hunting* a su estrategia global de seguridad.

Y no es de extrañar ya que es una potente herramienta para defender a sus clientes aportando a sus servicios valor añadido, pues permite descubrir e interrumpir a tiempo las amenazas internas y externas que han eludido los controles basados en la tecnología antes de una infracción; aumenta las tecnologías de seguridad con la experiencia humana para reducir el tiempo de permanencia; dota a los equipos de seguridad de los conocimientos necesarios para desbaratar a los adversarios a gran escala; o alimenta el esfuerzo continuo por reducir la superficie de ataque y mejorar las capacidades de detección automatizada.

¿Está preparado para llevar sus servicios de seguridad al siguiente nivel?

Los MSPs que estén considerando aprovechar la oportunidad y poner en marcha un servicio de hunting deberían evaluar lo siguiente:

1 - **Toda organización es un objetivo, independientemente de su tamaño, sector o ubicación.**

2 - **Las amenazas se mueven más rápido que nunca**. Recuerde la velocidad a la que operan y evolucionan las amenazas.

3 - **Por tanto, el *threat hunting* es ahora una necesidad para todas las organizaciones. Ya no es un *"nice-to-have"*.** La oportunidad de proporcionar el servicio de valor añadido del *threat hunting* es relevante.

4 - **La velocidad, la escala y la coherencia son fundamentales.** El *hunting* debe poder realizarse con rapidez y a gran escala. Esto requiere procesos estructurados y repetibles, tecnologías maduras, visibilidad a largo plazo y *hunters* de amenazas respaldados por una amplia gama de productos, con una profunda experiencia, conocimiento e inteligencia sobre amenazas.

5 - **Estructure sus acciones de *hunting* utilizando el marco MITRE ATT&CK.** Las soluciones de WatchGuard vienen reforzadas con muchas técnicas ATT&CK identificadas, permitiendo así al equipo de seguridad centrar sus esfuerzos en hacer frente a las amenazas de seguridad aprovechando la información bien definida que proporciona el marco y que nuestro equipo de ciberseguridad ha ampliado.

6 - **Aproveche la oportunidad.** Siempre es más fácil vender a los clientes existentes, y los servicios de seguridad para *endpoints* no son una excepción. Los *partners* que ya ofrecen servicios de seguridad encontrarán en WatchGuard EDR, WatchGuard EPDR y el servicio de *threat hunting* una extensión natural de su actual oferta de servicios.

7 - **Si no puede hacerlo internamente, considere nuestro servicio de *threat hunting*.** Por último, si no puede hacerlo internamente, asegúrese de asociarse con un proveedor que pueda hacerlo. Elegir el adecuado puede simplificar la prestación de servicios básicos y nuevos servicios de seguridad gestionados a lo largo del tiempo.

Nuestro servicio de *threat hunting*, incluido en WatchGuard EDR y WatchGuard EPDR, es una potente herramienta que permite a los MSP añadir un servicio de *hunting* como parte de su oferta. Permite detectar las amenazas antes de que se produzca el daño y mejora las defensas contra futuros ataques a sus clientes.

Aprenda cómo puede ampliar sus soluciones añadiendo este servicio leyendo nuestro último eBook *Your threat hunting service program simplified with WatchGuard* e inicie el camino del servicio de *threat hunting* con WatchGuard Advanced Endpoint security.

Iratxe Vázquez
Senior product marketing manager de
WatchGuard Technologies

¿Cómo pueden ayudar los *partners* a abordar los pilares de la seguridad de los clientes?

Si hay dos grandes aspectos por los que las empresas deberían preocuparse son, en primer lugar, la capacidad de ofrecer experiencias excepcionales a los usuarios. La segunda es asegurar lo que se ha convertido en algo cada vez más fragmentado: las aplicaciones, los dispositivos y la infraestructura que forman la base sobre la que se construyen estas experiencias.

Pero las empresas luchan por cubrir ambos frentes y necesitan la ayuda de sus *partners* para superar la percepción actual de que la seguridad sigue siendo un obstáculo, lo cual es especialmente cierto cuando se trata de realizar cambios: el 61 % de los equipos de TI y el 52 % de los desarrolladores afirman que las políticas de seguridad asfixian su propia innovación. No es difícil entender por qué: llevamos años ajustando nuevas soluciones y productos para protegernos de las nuevas amenazas y defender una superficie cada vez mayor, una tendencia que se ha acelerado con el incremento del trabajo híbrido.

El resultado es que el parque informático de muchas organizaciones se ha convertido en una maraña compleja de plataformas, sistemas y soluciones que los enfoques de seguridad tradicionales no pueden proteger.

Ahora hemos llegado a un punto en el que, para poner orden en el caos, las empresas necesitan la ayuda de socios capacitados que puedan convertir un gran abanico de soluciones (y perspectivas) de seguridad en una defensa intrínseca que no sólo proteja contra amenazas sofisticadas, sino que permita a las empresas impulsar experiencias de usuario innovadoras.

La capacidad de los socios de analizar el entorno informático de una empresa de forma integral, junto con las necesidades del negocio, es lo que les sitúa en la mejor de las posiciones para ayudarles a desarrollar un plan que logre este equilibrio tan importante.

Los socios deben saber que la "seguridad" se divide en tres categorías: usuarios, cargas de trabajo y operaciones. Los usuarios tienen que poder trabajar, utilizar las aplicaciones, los datos y los servicios que deseen, de la manera que quieran, en el lugar que elijan. Las cargas de trabajo, las aplicaciones y los datos deben

ser totalmente seguros, pero igual de dinámicos; es decir, deben poder moverse y compartirse cuando sea necesario. En cuanto a las operaciones, la implementación real de la seguridad tiene que ofrecer una protección total sin restricciones que sea capaz de proporcionar una detección, protección y respuesta adecuada. Además de estas diferentes perspectivas está la confianza cero. Con el fin de ofrecer una seguridad dinámica en la empresa actual, cada vez son más las empresas que buscan adoptar este enfoque de la seguridad.

La oportunidad de los *partners*: ser polivalente

Todo esto supone una complejidad y un reto importantes. Sin embargo, también es una oportunidad para los socios, que consiste en ser esa luz en la oscuridad, ese orden en el caos. Ayudar a hacer operativa la verdadera confianza cero, a consolidar proveedores y soluciones para que todos los productos de seguridad se comporten como tienen que hacerlo y garantizar que no haya solapamientos ni lagunas.

En todo este proceso resulta imprescindible la labor de conectar todas las partes de la empresa que luchan por conectarse entre sí. Los equipos de TI y los desarrolladores, a los que se les confía la innovación, se sienten asfixiados por la seguridad. Para ser innovadores y ofrecer experiencias de usuario excepcionales es necesario que los diferentes equipos trabajen en colaboración. Parte del problema es que los desarrolladores, los informáticos y los equipos de seguridad hablan idiomas diferentes. Sin embargo, los *partners* pueden interactuar con ellos haciéndose entender y transmitiéndoles las prioridades y necesidades de otros departamentos. En eso consiste ser polivalentes, utilizar su visión informada pero distante y su función de soporte para ayudar a resolver los problemas de la empresa.

Con la ayuda de los socios, las empresas pueden convertir el caos en orden y la complejidad en innovación sin comprometer la seguridad. Aunque ésta se ha considerado siempre un obstáculo para el cambio, ahora debería verse como todo lo contrario, una de las herramientas vitales para realinear el negocio y ofrecer la primera gran línea roja de la empresa moderna: experiencias de usuario excelentes.