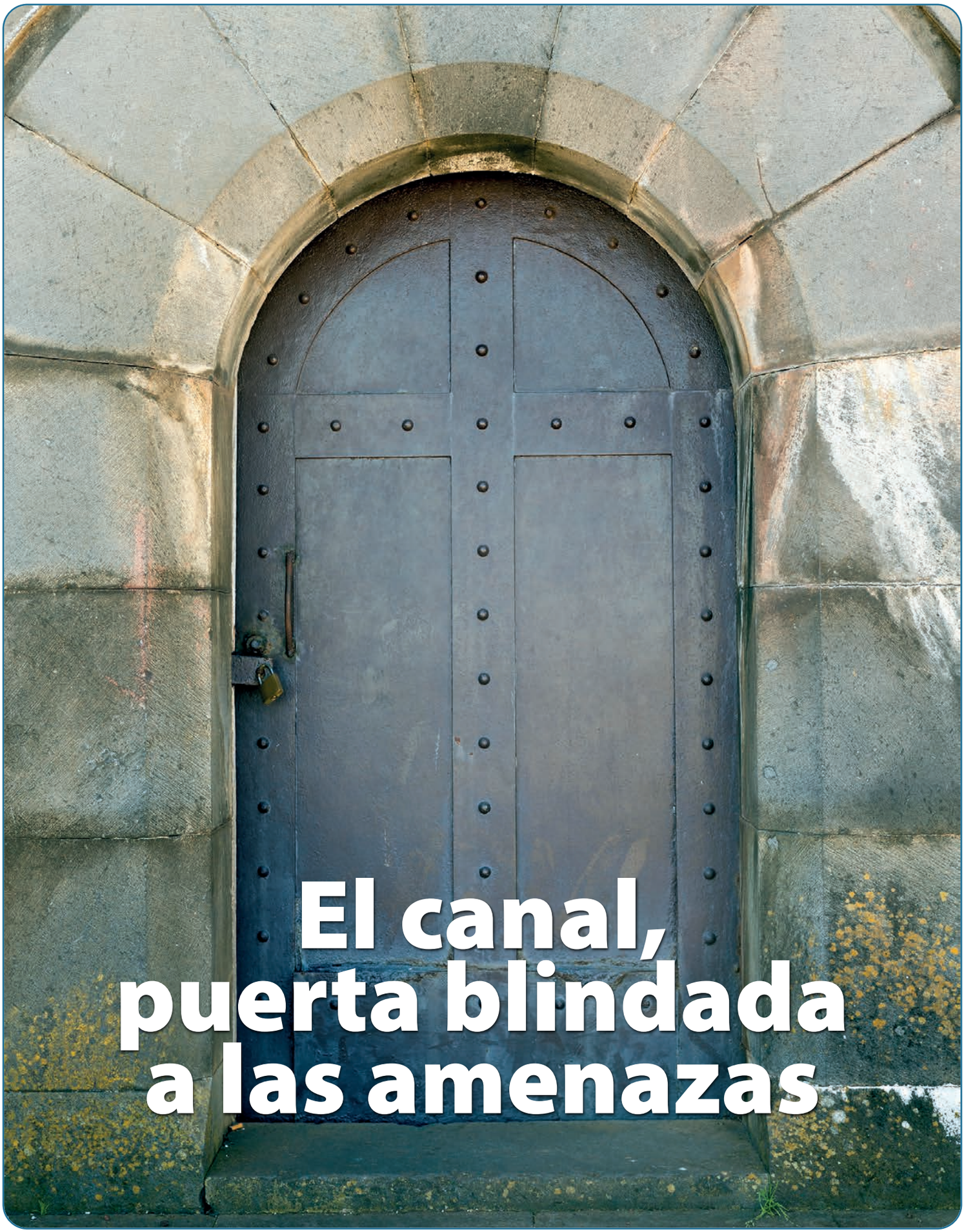


El canal, puerta blindada a las amenazas

Tendencias y oportunidades

del mercado de la ciberseguridad en España en 2024

El mercado de la seguridad en España muestra un crecimiento respecto del año pasado del 12 %, alcanzando los 2.729 millones de euros, y para el año 2027 podría superar la barrera de los 3.891 millones, manteniendo ritmos de crecimiento similares que se acercan al doble dígito (12.6 %). Los segmentos de mayor crecimiento son los relativos a los servicios gestionados de seguridad, los servicios de integración y los servicios de red.

El impacto de los negocios digitales dentro de la operativa de las organizaciones está derivando en la progresiva inversión en iniciativas de negocios digitales por parte de los CEO (un 40 % de ellos incrementará la inversión en 2024), mientras que el 44 % reconoce que están tratando de integrar la transformación digital a largo plazo. Por ello, no sorprende que en 2023 el 64 % de los CEO indique que el rol principal de sus CIO estuviera focalizado en alcanzar la agilidad empresarial, en los resultados empresariales y en impulsar nuevas fuentes de ingresos.

Las organizaciones enfrentan desafíos desde muchas direcciones e incluyen amenazas al negocio que el CISO debe equilibrar con nuevos enfoques en evaluación continua de riesgos, protección de activos digitales y gestión del rápido ritmo de innovación en tecnologías de seguridad. Este incremento de las operaciones digitales, unido a un escenario regulatorio cada vez más exigente (NIS2, DORA), requiere de un mayor y mejor control del riesgo organizacional y la adopción de nuevas estrategias de ciberseguridad.

La protección de los activos de TI, ya sean datos, aplicaciones, redes o dispositivos, es un requisito fundamental, generalmente obligatorio por el departamento de tecnología o legal de una empresa. La falta de protección de estos activos puede resultar en brechas desastrosas y altamente publicitadas que pueden hacer que clientes, socios y partes interesadas pierdan la confianza en una organización, y que una organización pierda ventaja competitiva y beneficios.

Las organizaciones se enfrentan a la necesidad de cambios en las estrategias operativas, que den respuesta a la complejidad en la gestión del marco de seguridad (el 70 % del tiempo de los equipos de seguridad se destina exclusivamente a mantener y operar el conjunto de soluciones y herramientas de seguridad de las organizaciones), y al auge de los datos.

En la actualidad la adopción de seguridad en la nube es una tónica creciente en las organizaciones (38 % de las mismas), ya que los servicios gestionados de seguridad en la nube (MCSS) son una evolución natural de los MSS (Servicios Gestionados de Seguridad). De hecho, los datos de IDC apuntan a que el 43 % de las organizaciones que han trabajado con sus actuales proveedores de servicios gestionados de seguridad (MSSP) han ampliado su contrato de MSS para incluir el alcance *multicloud*. Así mismo, un 39 % de las organizaciones indica la naturaleza "incorporada" de los acuerdos de servicios gestionados de seguridad en la nube, ya que la nube requiere una transformación en la seguridad: velocidad, escala y transparencia.

También en la seguridad irrumpe con fuerza la IA generativa, el aprendizaje automático, los grandes modelos de lenguaje (LLM por sus siglas en inglés), el desarrollo asistido por IA, los copilotos y aplicaciones inteligentes.

La incorporación de la IA Generativa para la mejora de las estrategias de defensa mediante la incorporación de esta en los sistemas de detección automática de las amenazas; especialmente en la parte de robo de identidades y combatir el *"deepfake"* hace que la gestión de identidades represente ya un 14 % del mercado de la ciberseguridad. Por ello, se requiere cada vez más una mayor diversificación de las defensas. Las organizaciones buscan mejorar la seguridad de su infraestructura de red y recibir servicios avanzados de asesoramiento para proteger sus organizaciones.

La búsqueda de la seguridad unificada y ciberresiliencia, principalmente en la nube, se configura como un imperativo. El impulso en las organizaciones de automatizar e integrar o racionalizar el entorno de seguridad, unido a la gestión de identidades y accesos en estos nuevos entornos, evoluciona hacia la adopción de un contexto de seguridad unificada donde se hace clave garantizar la protección y soberanía del dato.

Por último, la necesidad de incorporar ciberresiliencia en las organizaciones llevará a que el 20 % de las empresas en 2026 incorporará plataformas de ciberseguridad proactivas.

José Antonio Cano
Director de análisis de IDC

Excelente inicio de año para la división de ciberseguridad de V-Valley

"Uno más uno han sido más que dos"

Alberto López, administrador delegado, y **David Gasca,** *sales & marketing manager cybersecurity* en **V-Valley**

Ha iniciado el año la división de ciberseguridad de V-Valley con muy buenos números. Tras un mes de diciembre en el que el balance fue espectacular, la buena inercia ha continuado en el primer tramo de este ejercicio; arropada además por la integración del equipo y del negocio de Lidera Network. "Uno más uno han sido más que dos", resume Alberto López, administrador delegado del mayorista. "Ha crecido tanto el negocio procedente de la cartera de V-Valley como el que se genera desde Lidera".

Marilés de Pedro

Estamos en un área de crecimiento, un segmento que evoluciona continuamente, con el panorama, cambiante, que provocan las nuevas amenazas y las necesidades de los clientes". Según la consultora Context, el pasado año la seguridad, con un crecimiento del 17 %, fue el segmento tras el área del centro de datos, que creció un 29 %, que mejor comportamiento tuvo dentro del área del valor en el canal mayorista en España. Una seguridad que, como señala, está cada vez "más enfocada al dato que se debe proteger, a quién lo tiene y a quién puede acceder a él".

Potente oferta

Apenas le han bastado a V-Valley seis años para conformar esta unidad de negocio, potente, que ya cuenta con más de 40 fabricantes. Una oferta, reforzada con la propuesta de Lidera, que le permite al mayorista cubrir todos los segmentos de negocio. "Cubríamos la parte *enterprise* y, ahora, gracias a Lidera se nos ha abierto un abanico de clientes en los segmentos de la pyme. Somos un mayorista mucho más atractivo para los fabricantes ya que podemos acercar su negocio a muchas más áreas".

A su juicio, el equipo humano marca la diferencia. "El valor son las personas; por lo que la inversión en gente cualificada es esencial". López recuerda que han sido capaces de tratar el área de seguridad "como una compañía ágil,

muy cercana tanto a los *partners* como a los clientes finales".

Servicios gestionados

La falta de talento, la complejidad de la ciberseguridad y los presupuestos, ajustados, han permitido que la ciberseguridad como servicio gane, cada día, mayor peso. "Es una oportunidad que el canal no quiere dejar pasar", asegura David Gasca, *sales & marketing manager cybersecurity* en V-Valley.

El mayorista cuenta con un equipo específico para dar soporte a los *partners* que cuenten con un perfil de MSP y ha incorporado a su oferta de soluciones una plataforma de servicios gestionados, Lidera Cloud, procedente del mayorista español. Una plataforma que se ha reforzado con más soluciones, recursos y profesionales. "Ayudamos a todos aquellos *partners* que creen que el servicio gestionado es un mercado de oportunidad a dar el paso hacia él. Nosotros nos encargamos de poner la capa de servicio y de darles el soporte que necesiten".

V-Valley Academy

El pasado año el mayorista puso en marcha V-Valley Academy, un espacio alojado en las oficinas del Grupo Esprinet en Madrid que despliega cursos de formación y certificación, y que cuenta con un centro de demostraciones. "La formación en ciberseguridad es básica", recuerda Gasca. Una formación que abarca no solo la actualización de las soluciones existentes sino todas las tecnologías nuevas que van apareciendo. El mayorista es centro autorizado de formación (ATC) de todas las soluciones que comercializa. "Los fabricantes han observado en V-Vallley Academy un gran potencial y están reforzando la formación en torno a sus soluciones. Algunos, incluso, satisfechos con el trabajo que estamos haciendo en España, nos han pedido si podemos ofrecer cobertura al resto de Europa", asegura.

Una tarea formativa que se complementa con los servicios que ofrecen los equipos de preventa y la oferta de servicios profesionales con la que contaba Lidera Network. Gasca anuncia que han creado un equipo, trasversal a todas las tecnologías, para completar su servicio al canal.

En línea con esta estela formativa, V-Valley está desplegando en los últimos meses un programa para ayudar a sus *partners* a conocer todas las herramientas de IA que tienen a su disposición y cómo sacar el máximo partido a esta tecnología. Gasca recuerda que se trata de una tecnología a la que los *hackers* ya están sacando partido, haciendo uso de la automatización para lanzar ataques más rápidos, eficientes y difíciles de detectar. Un uso que también alcanza al área de los fabricantes que la están utilizando para ser más eficientes. Incluso, explica Gasca, hay fabricantes que están basando toda su tecnología en ella. "Gracias a la automatización que imprimen es posible cubrir la escasez de talento y dar un mejor soporte en los SOC. No se trata de reemplazar a las personas que trabajan en estos centros sino de hacer más eficaz su labor".

> "Somos un mayorista mucho más atractivo para los fabricantes ya que podemos acercar su negocio a muchas más áreas"

Perspectivas

Las perspectivas de negocio son muy positivas. Alberto López desvela que han sido capaces de incrementar su cuota de mercado en aquellos fabricantes con los que no disfrutan de una distribución en exclusividad. "Incrementar nuestra presencia y generar una mayor facturación con los fabricantes amplía el número de oportunidades", valora.

El mayorista sigue apostando por el diseño de soluciones como proa de negocio. Junto a su apuesta por fabricantes más jóvenes o con un menor recorrido en el mercado, sigue desplegando una cartera de soluciones, en proveedores más tradicionales, para mantener una oferta innovadora para que su ecosistema de *partners* se la haga llegar a sus clientes. "Es un sector que mantiene una enorme oportunidad", asegura. Áreas como la protección del dato, la gestión de identidades o el control de accesos tienen un enorme recorrido. "Las amenazas no paran y siempre surgen nuevas necesidades. La ciberseguridad es un área tremendamente interesante, incesante en su actividad, que permite, no solamente vivir el presente, sino preparar el futuro, lo que nos permite tomar las medidas pertinentes en la oferta para cubrir esas necesidades".

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

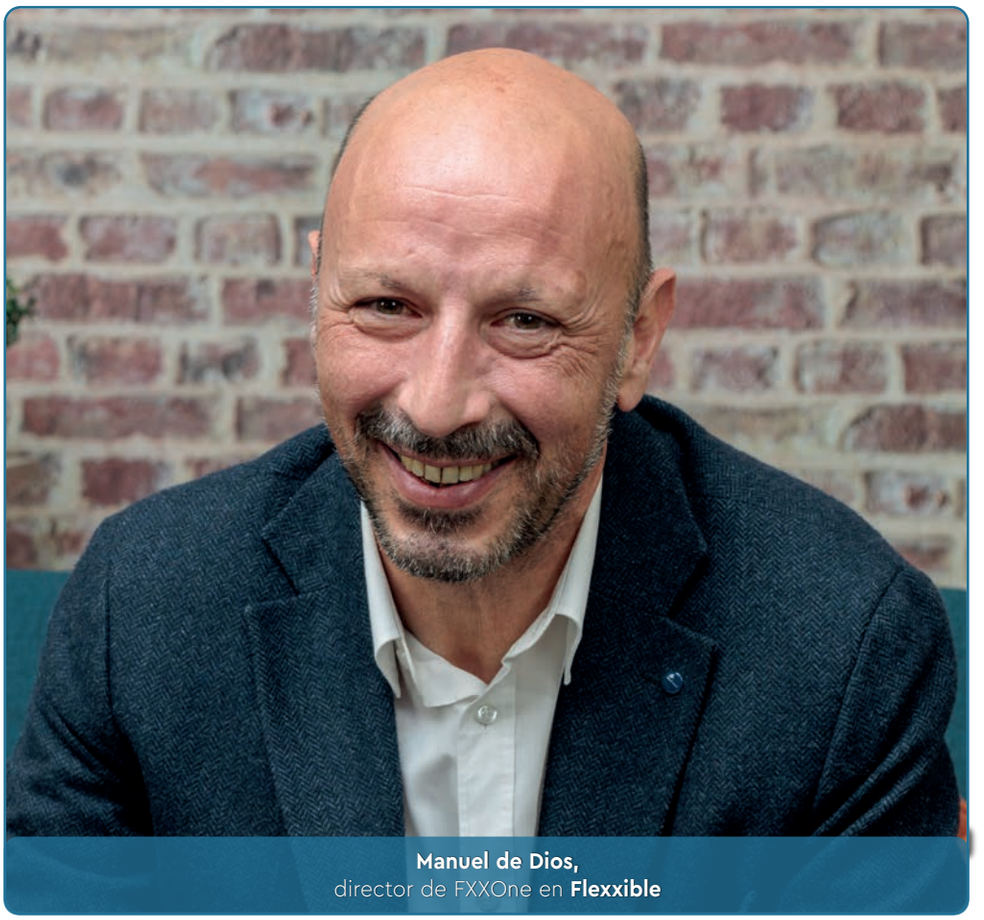
https://newsbook.es/actualidad/uno-mas-uno-han-sido-mas-que-dos-20240430109112.htm

El canal es pieza básica en la comercialización de la solución

FXXOne: protección a la medida de los "héroes" de la pyme

En el área del puesto de trabajo, corazón de negocio de Flexxible, es crítico el despliegue de la seguridad. Una materia en la que la multinacional española, sin ser una especialista, ha desplegado una poderosa estrategia en la que la protección del dispositivo es esencial. Embebida por diseño, la seguridad, por tanto, es materia troncal en el catálogo completo de la multinacional, al que el pasado mes de marzo llegaba FXXOne, su solución específicamente pensada para el entorno de la pyme.

Marilés de Pedro



Manuel de Dios,
director de FXXOne en **Flexxible**

Estrategia de seguridad

Manuel de Dios, director de FXXOne en Flexxible, explica las dos variables en las que reposa la estrategia de seguridad de la multinacional. "Todas nuestras líneas de producto, que cuentan con un *core* tecnológico común, tienen la protección por diseño, con lo cual utilizan los más altos estándares, sellos y certificaciones de seguridad", explica.

Una protección que, en el entorno del puesto de trabajo, se ubica como elemento imprescindible. Flexxible, que no es un proveedor centrado en el despliegue de esta funcionalidad, sí "tiene una relación muy próxima con ella", explica. "Trabajamos muy cerca de las empresas expertas en ciberseguridad. El desarrollo de todos nuestros productos observa una integración con fabricantes específicos de seguridad en el ámbito del EDR, el antivirus, el análisis de intrusión o la seguridad del dato". Flexxible está creando, por tanto, un ecosistema para aprovechar todo el conocimiento de estos fabricantes y concedérselo al puesto de trabajo. "La seguridad es un campo enorme que exige contar con equipos muy especializados", argumenta. En el caso de Flexxible sus profesionales centrados en el desarrollo de su oferta, en torno a 60 ingenieros, centran su labor en dar el máximo valor al entorno del puesto de trabajo.

> "FXXOne abre al canal una vía para la creación de servicios"

Manuel de Dios insiste en la importancia de la formación del usuario. "Hay comportamientos digitales que entrañan mucho riesgo y es necesario formarle en estos aspectos". Reconoce el directivo que es difícil estar a la última en esta área de la seguridad. "El concurso de nuestras alianzas y colaboradores tecnológicos es esencial para incrementar la protección del dispositivo y reducir, al mínimo, los riesgos. El eslabón más débil es, sin duda, la ingeniería social. El usuario se conecta a redes públicas, navega sin protección, etc.".

FXXOne

El pasado mes de marzo el fabricante presentaba FXXOne, una solución centrada en el entorno de la pyme. Se trata de un producto que

da respuesta a las necesidades tecnológicas que exigen los entornos híbridos. "Estas empresas, con muchos menos recursos, tienen que enfrentarse a las mismas situaciones que las grandes compañías. Cuentan con menos nivel de conocimiento, menos capacidad de contratación y menos inversión".

El *core* tecnológico de FXXOne es idéntico a FlexxClient, la solución para los entornos corporativos. "Permite un control y una visión 360 del uso de los dispositivos; tanto virtuales como físicos, lo que permite observar el comportamiento del usuario: dónde y cómo se conecta, qué uso está haciendo de las aplicaciones, el rendimiento de las máquinas, etc. Y, específicamente, en términos de seguridad, concede un factor de protección". Con ello, bien los gestores TI que pueda tener una pyme, bien el distribuidor especialista que se encarga de darle soporte, disfrutan de una gestión completa del dispositivo, con la posibilidad, si hay una incidencia, de responder en tiempo real de manera remota. "La herramienta también les permite anticiparse a los fallos. Automatizamos hasta el 73 % de las actividades de soporte".

El control de la actividad de las aplicaciones es esencial. "La seguridad ha pasado a ser foco para ellas. Ahora, para acceder a cualquier aplicación contamos con un proceso de autenticación mucho más complejo, lo que supone un gran cambio". FXXOne controla dos tipos de aplicaciones. Primero, las instaladas en el PC, con dos variantes: es posible hacer un inventario de las que el usuario tiene instaladas y del uso que hace de las mismas. "Muchas veces la empresa está pagando por licencias que no se usan, lo que es especialmente crítico para empresas que tienen mucho volumen". La solución también controla el rendimiento de las aplicaciones web. Disfruta, entre otras, de integración con Microsoft365 lo que proporciona un mapa de las aplicaciones web, con datos de dónde se conectan, el rendimiento y las latencias que tienen con cada una de sus conexiones; "lo que proporciona una foto muy aproximada de lo que está haciendo bien la máquina y lo que está haciendo mal", explica. Por último, también ofrece visibilidad de aquellas aplicaciones que los usuarios utilizan pero que no forman parte del abanico que ha sido validado por la empresa. "La adquisición y el uso de una aplicación está impulsado por el negocio. En ocasiones, la rigidez de los departamentos de TI no da respuesta a lo que necesita el negocio", alerta.

> El canal mayorista de Flexxible está conformado por Ingram Micro y V-Valley

El canal, vital

En la comercialización de FXXOne el ecosistema de *partners* es vital. Una solución que permite al canal gestionar la seguridad de las pymes y que se convierte en una pieza importante en su oferta de servicios para este tipo de empresas. "Se trata de distribuidores capaces de dar soporte, lo que convierte a nuestra solución en una herramienta que incrementa el valor que le concede a su cliente". FXXOne también abre la vía a la creación de servicios con la base de su tecnología. "Ayudamos a crear un paquete de servicios para que el canal sea mucho más competitivo, no solo en aquellas áreas en las que ya trabajan; también con la creación de un valor o de un servicio incremental".

FXXOne se adapta al modelo de negocio del distribuidor, con diferentes fórmulas de contratación para el consumo y el pago del mismo, lo que concede una enorme flexibilidad.

La estrategia incluye al canal mayorista, en el que cuentan con dos figuras: Ingram Micro y V-Valley. "Ponemos en sus manos la preventa, el soporte técnico y el desarrollo de negocio con los *partners*, no solo la captación del *partner*, también el despliegue conjunto. El distribuidor que se dirige a la pyme tiene una relación muy estrecha con ambos mayoristas; son ellos los que conocen perfectamente cuáles son sus requerimientos", explica. Flexxible ha llevado a cabo una automatización de una gran parte de los procesos transaccionales y de la gestión de las suscripciones, a través de sus *marketplaces*, para ayudarles en el negocio.

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

https://newsbook.es/actualidad/fxxone-proteccion-a-la-medida-de-los-heroes-de-la-pyme-20240430109115.htm

La ciberseguridad sigue abriendo importantes oportunidades al ecosistema del mayorista

"La inversión en seguridad debe formar parte de las estrategias de negocio de las compañías"

Carmen Muñoz,
directora general de **Exclusive Networks** en España y Portugal

Tras los buenos resultados cosechados el año pasado, en el que la multinacional consiguió crecer un 14 % a nivel mundial, con un 16 % en el área de EMEA, zona que es su principal motor de negocio; la filial ibérica de Exclusive Networks ha empezado 2024 con muy buen tono. Carmen Muñoz, directora general del mayorista en España y Portugal, desvela que han superado las expectativas que se habían marcado. "Hemos tenido un muy buen trimestre", asegura. Los proyectos alrededor del puesto de trabajo y la protección del correo electrónico, junto la actualización de las plataformas de red y el despliegue de SASE han marcado la tendencia creciente en este primer tramo.

Marilés de Pedro

La directiva, que señala el retraso que se han producido en algunos proyectos vinculados con la Administración pública, también apunta que se han presentado muchas solicitudes en este entorno, lo que marca, sin duda, un buen año en este apartado público. "Se prevé un crecimiento a lo largo de este año". En las grandes cuentas, indica, "la banca sigue siendo un motor importante de inversión". También el negocio del segmento de las pequeñas y las medianas cuentas "ha empezado fuerte", valora.

La ciberseguridad, inversión de negocio

Insiste Carmen Muñoz que la inversión en seguridad tiene que ser entendida como una inversión de negocio. "Debe formar parte de las estrategias de negocio de las compañías". Consciente de que la protección completa no existe y del crecimiento constante de la sofisticación de los ataques, es un reto mantener esta necesaria inversión. Y, sobre todo, concienciar. "Para estrechar la brecha con los ataques, es vital la concienciación, sobre todo en el mercado de las pymes", alerta. Es un área crítica para las compañías. "Todas las empresas son vulnerables, da igual el tamaño o el sector en el que estén. Y, por tanto, es importante educar a usuarios y empresas en lo importante que es intentar mantenerse al día en las estrategias de seguridad".

"Exclusive Networks es reconocida por traer, lanzar y por posicionar soluciones que no eran conocidas"

De cara a los próximos meses, Carmen Muñoz

ve grandes oportunidades, además de en el despliegue de proyectos en el área pública, en la protección de la nube. "La seguridad de los entornos industriales empieza a ser ya una realidad", enumera. Áreas claves son también la seguridad del puesto de trabajo, la protección de los datos y la gestión de identidades. "La tecnología SASE, con las soluciones en torno a la seguridad de acceso, SD-WAN y la protección de los entornos IoT marcarán las principales áreas de oportunidad", completa.

Pieza clave en el mercado son los servicios gestionados de seguridad. Según un informe de Canalys, el 65 % de los distribuidores del ámbito de EMEA asegura que es su principal vía de crecimiento. "Está creciendo mucho el negocio vinculado con esta fórmula", reconoce. Muchos integradores tradicionales están abordando proyectos de seguridad gestionada. "Es una vía esencial de crecimiento". En un entorno pintado por la falta de talento, de recursos y de insuficiente concienciación, "las empresas necesitan incluir automatización y apostar por la externalización en aquellas áreas en las que no cuentan ni con el conocimiento ni con los recursos necesarios".

Por último, se observan impulsos importantes como, por ejemplo, la Directiva sobre Seguridad de las Redes y los Sistema Informáticos (NIS2), para crear un nivel común de ciberseguridad en todos los estados miembros de la Unión Europea. Muñoz la observa como una oportunidad. "Antes de final de año las empresas tienen que cumplir con este marco regulatorio; lo que hace esencial la labor de consultoría y la capacidad de ofrecer servicios gestionados de los *partners* para ayudar a las empresas a alcanzar los niveles de seguridad que implica esta nueva regulación".

Papel del mayorista

El rol del mayorista en este complejo entorno ha cobrado un mayor valor con los años. "La oferta es enorme, con muchas soluciones y multitud de fabricantes: junto a proveedores que apuestan por el desarrollo de una plataforma, ofreciendo una respuesta integral a todas las necesidades de seguridad; hay proveedores con una apuesta más especializada". Un panorama, complejo, que ofrece al mayorista la oportunidad de ser una pieza esencial. "Es muy complicado que el canal conozca y se especialice en todo. Nuestra labor, por tanto, en el entorno de su educación y su formación es clave; también en apoyarle, con nuestros recursos, para trabajar en su especialización". Precisamente el complicado equilibrio entre los diferentes perfiles de proveedores señala el ADN de Exclusive Networks. "Nuestra filosofía es detectar las mejores soluciones que den respuesta a las necesidades de cada momento. Exclusive Networks es reconocida por traer, lanzar y por posicionar soluciones que no eran conocidas", recuerda. Con una oferta actual en la que conviven fabricantes más consolidados con otros más de nicho, "el reto para el canal es elegir quiénes son sus socios y con quién quiere hacer el camino de negocio", explica. Una vez determinados los socios en el apartado del proveedor, "apoyarse en otras compañías, como Exclusive Networks, en el desarrollo de temas como la formación es muy importante". Muñoz defiende el gusto por la especialización. "Cuando un fabricante se incorpora a nuestra oferta va a disfrutar de un equipo especializado en su tecnología. Contar con el mejor *portfolio* y con las mejores soluciones para que los socios de canal puedan elegir cuáles son sus alianzas es esencial".

La brecha de talento

En el desarrollo del canal, la educación es fundamental. Exclusive Networks cuenta con iniciativas para la captación, formación y retención de nuevo talento cibernético. El reto es enorme porque se calcula que hay en torno a 140.000 vacantes tecnológicas en España que no están cubiertas. Carmen Muñoz recuerda que, a diferencia de otros países, en nuestro país no existen ayudas, ni es obligatorio, por ley, destinar una partida a la formación de los empleados. "No es frecuente que las compañías cuenten con un presupuesto específico para estos fines". Sin embargo, señala que algunas normativas, como NIS2, van a incluir la formación como un tema esencial. "La concienciación y la formación del empleado son fundamentales".

En los últimos años, la mayor difusión de los riesgos asociados a la ciberseguridad se está reflejando en las carreras profesionales por las que los jóvenes están apostando. "Es un área con muy buenas salidas profesionales", recuerda. "Una mayor colaboración de las entidades educativas con el Gobierno y con el mercado corporativo, en general, también ayudaría a cubrir esa brecha de talento".

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

https://newsbook.es/actualidad/la-inversion-en-seguridad-debe-formar-parte-de-las-estrategias-de-negocio-de-las-companias-20240430109150.htm

"Es que queremos seguir yendo al cliente"

Como fabricantes de herramientas de monitorización y gestión remota, esta es una de las frases que escuchamos habitualmente por parte de los profesionales de los *partners* de TI. Es cierto: el contacto con el cliente, sea con la excusa que sea, es bueno. Genera oportunidades, nos aporta información única y estrecha los lazos personales entre el equipo y la fidelización de la cuenta.

Esto se torna mucho más evidente, y se convierte en un valor diferencial en los clientes pequeños y medianos, donde los formatos de reporte y procedimientos de comunicación de incidencias están menos marcados y existe una cultura de transmisión oral. Con FXXOne, que se focaliza en ese mercado, nos hemos encontrado a menudo con esto. Remoto es lo contrario. "Si les ayudamos sin aparecer, no perciben nuestro valor; si intervenimos de forma "transparente" es difícil justificar las horas del técnico". Es una paradoja, lo que podríamos pensar como mejora, trabajar con nuestras herramientas: ahorro de tiempos, costes de desplazamiento, reducción de tiempo de espera del usuario, aumento de la productividad de usuarios y técnicos. Se convertía en una desventaja. ¡Menudo chasco!

Afortunadamente, los partners con los que hemos tenido el lujo de colaborar fueron los que ayudaron a poner en, muy positiva, una barrera que originalmente no habíamos tenido en cuenta. "No dejaremos de ver al cliente. Vamos a orientar las visitas con un cariz de recogida de impresiones y planteamientos de mejora, en lugar de realizar diagnósticos y análisis insitu. Llevaremos el análisis y el diagnóstico hecho (rendimiento, parcheado, seguridad, actividad del parque), los planteamientos de solución e incluso las primeras estimaciones de costes de inversión en los mismos. Mejoraremos la percepción del cliente con un mayor control y anticipación".

"Por supuesto, usaremos las herramientas de remediación y mantenimiento, así como la asistencia remota. ¡Hay que seguir apagando fuegos! Pero en remoto nos permite una mayor flexibilidad y en esos casos la inmediatez de respuesta está muy bien valorada".

"Es más, dado el coste que supone sensorizar los dispositivos y monitorizarlos, que es menor que invitarles a desayunar, vamos a hacerlo en todos aquellos clientes potenciales. Un mes o dos. Y les damos un informe de auditoría sobre el estado de su parque, con recomendaciones y propuestas".

El planteamiento nos ha parecido tan bueno que vamos a apoyarlos directamente. Crearemos informes, de forma gratuita y bajo demanda, para que los *partners* puedan adecuarlos a su tipología de cliente. Aunque ya existe una amplia biblioteca de automatismos, ayudaremos o diseñaremos los *scripts* técnicos necesarios para los casos concretos que se necesiten en cada situación.

Y por supuesto, seguiremos escuchando atentamente cómo mejorar tecnológicamente una herramienta, de la mano de los que la explotan día a día.

Los que trabajamos en tecnología estamos acostumbrados a tener lejos al fabricante. Vamos a aprovechar, en este caso, que tenemos a golpe de teléfono al equipo de ingenieros de diseño y desarrolladores. ¡Además en nuestro idioma! Gracias a todas las empresas que nos ayudan día a día en la mejora continua de FXXOne.

Manuel de Dios
Responsable de FXXOne en **Flexxible**

Planea acudir a numerosos eventos del sector este año para estar más cerca de sus *partners* y clientes

Hornetsecurity, escudo para el correo

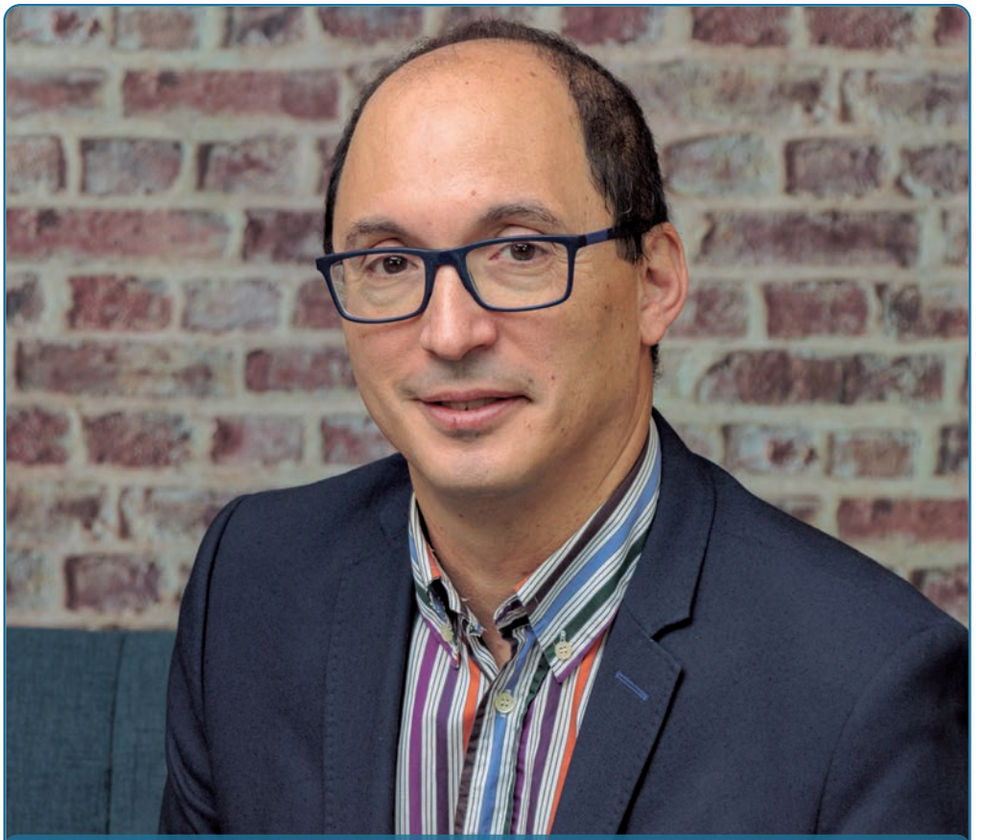
y para las soluciones de Microsoft 365

En el panorama actual de las ciberamenazas, Hornetsecurity cree que el vector principal de ataque sigue siendo el correo electrónico porque el usuario "interactúa con ese correo y es el que cae en las trampas de los ciberdelincuentes", señala Canales.

En este contexto de riesgos y amenazas ha aparecido un elemento que puede ser una herramienta para mejorar la protección o un factor que agudiza el peligro. Se trata de la inteligencia artificial que está siendo utilizada tanto por los ciberdelincuentes como por los especialistas en ciberseguridad. Canales confirma que "la inteligencia artificial ha llegado a todos los ámbitos de la seguridad".

> "La inteligencia artificial hemos de pensarla siempre como algo positivo"

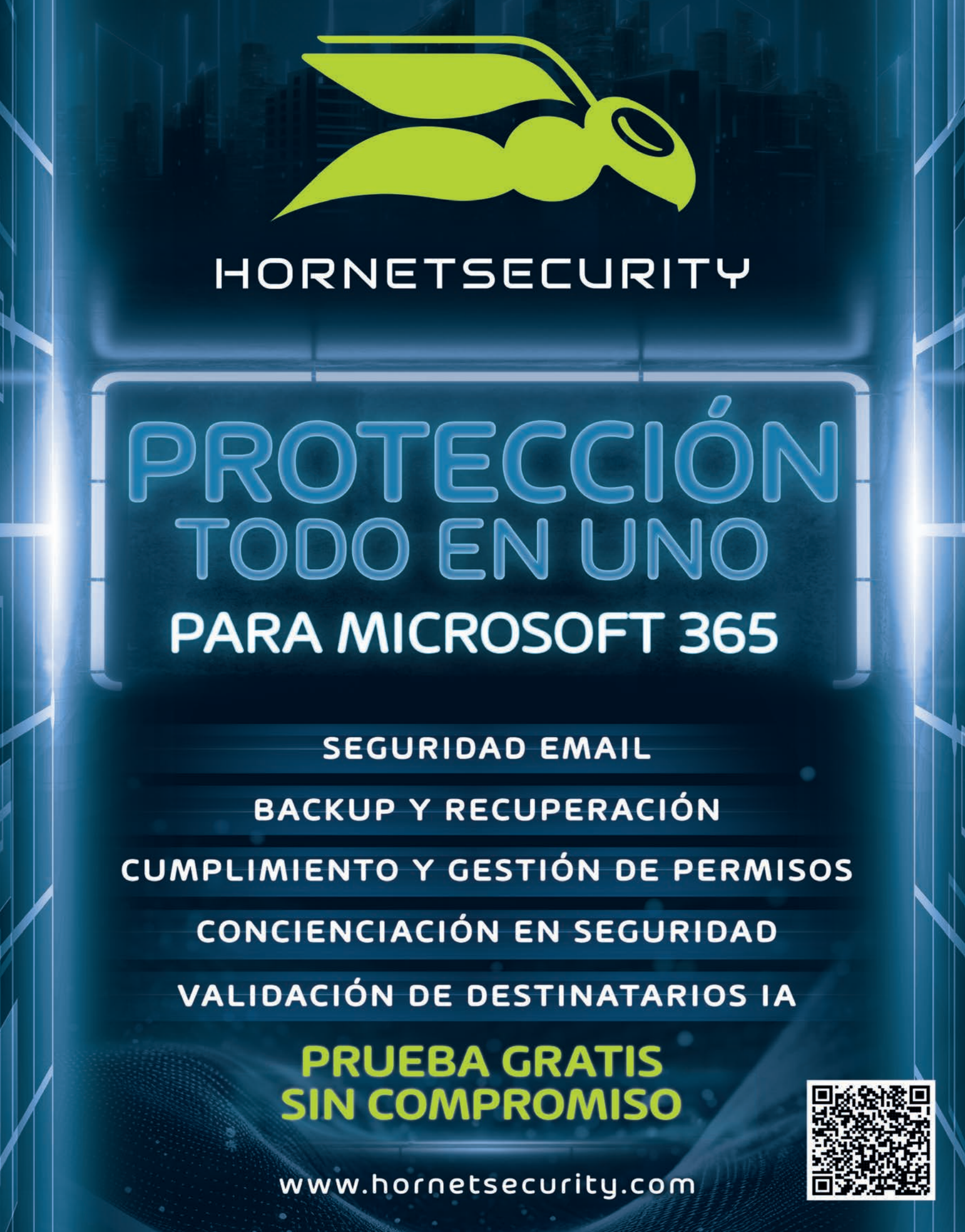
Desde el lado de la ciberdelincuencia, se está utilizando para elaborar ataques más complejos incluyendo los de *phishing*. Hornetsecurity ha detectado que los *emails* maliciosos están mejor hechos, sin errores gramaticales e imitando mejor a los reales. "La inteligencia artificial ayuda de manera muy exacerbada a los ciberdelincuentes a crear ataques más sofisticados y mucho más personalizados", explica el directivo. Sin embargo, la otra cara de la inteligencia artificial es más positiva porque está sirviendo para reconocer los patrones de ataque y mejorar las técnicas de detección. "La inteligencia artificial hemos de pensarla siempre como algo positivo. No podemos pensarla siempre como algo negativo. Nos está ayudando a programar las máquinas que van a detectar esos tipos de ataques con mucha más rapidez y facilidad", añade Canales.



Paul Canales,
director de canal de **Hornetsecurity**

La protección del correo electrónico es una de las prioridades de Hornetsecurity porque es uno de los principales vectores de ataque de los ciberdelincuentes. Al mismo tiempo, está centrando su propuesta en la protección de la tecnología Microsoft 365 que tiene un alto nivel de penetración en la empresa. Y para llevar esta oferta al mercado sigue confiando en su red de distribución, que juega un papel muy importante dentro de su estrategia, según confirma Paul Canales, director de canal de Hornetsecurity.

Rosa Martín


HORNETSECURITY
PROTECCIÓN
TODO EN UNO
PARA MICROSOFT 365
SEGURIDAD EMAIL
BACKUP Y RECUPERACIÓN
CUMPLIMIENTO Y GESTIÓN DE PERMISOS
CONCIENCIACIÓN EN SEGURIDAD
VALIDACIÓN DE DESTINATARIOS IA
PRUEBA GRATIS
SIN COMPROMISO
www.hornetsecurity.com

Estrategia y oferta

Hornetsecurity está desarrollando una estrategia para ayudar a las empresas a combatir las principales amenazas que tiene el puesto de trabajo. Según indica el responsable del canal de la compañía, monitoriza de manera constante el mercado global para identificar las tendencias y como fruto de este trabajo ha elaborado su plan de acción. "Hay una tendencia de las empresas a adoptar la nube de Microsoft 365, por lo que la compañía está focalizando sus esfuerzos en desarrollar el negocio en ese área, sin descuidar la parte de protección del correo".

Compra de Vade

El pasado mes de marzo Hornetsecurity anunció la compra de Vade, una compañía especialista en seguridad del *email* con más de 2.500 millones de mensajes analizados diariamente. Esta compañía, como explica Canales, le permite convertirse "en el líder de ciberseguridad europeo". La combinación de ambas, que comparten una aproximación al mercado similar, ampliará su propuesta tecnológica y las opciones que brinda a las empresas. Inicialmente, la tecnología de Vade se integrará de manera paulatina en las soluciones de Hornetseurity. "Vamos a ir integrando, poco a poco, todo ese conocimiento y la tecnología de Vade Secure en el *portfolio*".

Canal y planes

A la hora de llevar estos planes al mercado cuenta con su red de distribución que está encabezada por los mayoristas Ingram Micro y V-Valley, que tienen un papel estratégico. "Sin hacer ningún cambio, el mercado es suficiente para los dos".

Los dos mayoristas articulan el trabajo con la red de *partners*, que cuenta con un programa a través del que ofrece formación mensual de forma gratuita a estas figuras para que conozcan de manera detallada sus soluciones. La formación se ofrece tanto cuando empiezan a trabajar con la marca como a lo largo de su relación comercial en forma de talleres y píldoras formativas. Además, el trabajo con sus distribuidores se basa en la colaboración constante que empieza con ir juntos a las primeras visitas a los clientes durante la primer etapa de la relación para posteriormente acompañarles en su día a día de manera personalizada.

Esta atención personal se completa con las acciones generales para todos sus *partners*. "En términos generales estamos haciendo *webinars*, pequeños *road shows* y acciones junto con otros fabricantes para ofrecer un valor añadido general al *partner*", señala Canales.

Esta actividad, que se completa con promociones, tendrá continuidad durante los próximos meses. El director de canal de Hornetsecurity resalta que planea "seguir realizando promociones continuas y estar en diferentes ferias del sector".

Dentro de su oferta cuenta con varios planes para proteger el ámbito de Microsoft 365. El último plan, el 4, de 365 Total Protection, ofrece una protección completa que suma a la protección del correo y el *backup*, que se encontraban en los planes anteriores, la gestión de permisos, el cumplimiento normativo y la concienciación en seguridad de los empleados.

Este plan está dirigido a cualquier empresa usuaria de Microsoft 365 con independencia de su tamaño y está disponible para todos los sectores. Este plan no será el último porque, como avanza el directivo, hay un *roadmap* para nuevos planes.

> "La competencia es muy sana entre los dos mayoristas"

ellos no podríamos llegar a todos los *partners* que tenemos en toda España". El trabajo de ambos mayoristas es complementario y, a juicio de Canales, "la competencia es muy sana entre los dos mayoristas". Por tanto, Hornetsecurity no se plantea ampliar su cartera mayorista. "No tenemos que

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

https://newsbook.es/actualidad/videos/hornetsecurity-escudo-para-el-correo-y-las-soluciones-de-microsoft-365-20240430109118.htm