AÑO XXXI Nº346 0.01 Euros

tai price book®

Junio 2024

NP comunicaciones

Fortinet Security Fabric

BROAD INTEGRATED AUTOMATED

Cybersecurity, everywhere you need it.

tai price book®

Junio 2024

NP comunicaciones

Mesa de debate: la ciberseguridad en 2024

Entrevista a Moisés Camarero (Compusof): «Quizás hoy sea mucho pedir llegar al 25% de crecimiento»

Subin George (ManageEngine): «Nuestra soluciones SaaS experimentó un impresionante 72% de crecimiento»

Los sistemas IoT deben abandonar el 2G y 3G en 2025

Hornetsecurity reúne a sus partners clave

Sumario

N.P. Comunicaciones, S.L.
C/ Ramón Gómez de la Serna 10, 3ºB
28035 Madrid
Tfno: +34 91 739 04 11
info@taipricebook.es

Javier Renovell
Director de Publicaciones
javier.renovell@taipricebook.es

Eduardo Navarro
Director de Marketing y Ventas
eduardo@taipricebook.es

Rosa Palacios
Directora Financiera
rosa.palacios@taipricebook.es

Silvia Hernández
Directora de Eventos
silvia@taipricebook.es

Distribución:
Mk Directo
Avda. Real de Pinto 91, Nave A05
28021 Madrid
Tfno: 91 723 25 22

DL - M-21246-1994

Días de cuchillos largos y noches de escopetas recortadas

Se prometen grandes emociones ahora que se venden televisores extremos que obligan a la reconfiguración del salón: lo que han perdido en peso lo ganan en tamaño, pero la nueva escala de certificación energética dejará confundido a más de un activista ecológico. Por nuestra parte, volvemos a la carga envidiando la periodicidad olímpica bisiesta de otros, aunque también se la juegan ante audiencias de centenares de millones de televidentes. Nosotros nos conformamos con dos o tres menos en esta mesa de debate sobre ciberseguridad que hemos preparado como plato fuerte con destacados expertos de Barracuda, ESET, Fortinet y Bitdefender.

Sin perder el aliento, un aperitivo de eventos para partners de la mano de OVHcloud y Hornetsecurity, que como no ocultan su nombre, afrontan dos aspectos vitales de las nuevas tecnologías, la nube y la ciberseguridad. MCR también nos enseña su nuevo espacio para demostraciones a clientes. Y para los que prefieren tomárselo con calma, pero no mucha, Wireless Logic comienza a avisar que algún día llegará el fin del servicio 2G/3G, todavía muy usado en ciertos entornos IoT.

Y para terminar en todo lo alto en amena sobremesa, traemos las palabras de Moisés Camarero (Compusof), que nos habla de algunas curiosidades de la IA, y Subin George (ManageEngine) que nos explica que la administración de sistemas no tiene por qué ser un suplicio. Y todavía nos queda de postre las tribunas de Nacho López Monje (Arrow) y Álvaro Ausín (MaxHub) sobre videocolaboración.

Hoguera de vanidades y sardinas espetadas

¿Se acuerdan ustedes de cuando en el cole se votaba al delegado de clase y siempre salía el más tonto solo para echarnos unas risas? Pues se nos está yendo de las manos. Parecería que la consigna del voto del cabreo fuese esa… o no, porque se ha demostrado con harto desparpajo que lo que se llama establishment no hacen más que reírsenos a la cara y tratarnos como cándidos seres de humillantes tragaderas prometiendo lo contrario y asumiendo la libertad de cambiar de principios estatuytuytutarios por exigencias de la tozuda realidad.

Pero qué grandes rimas se fabrican y qué sofocos se agarran unos y otros, y si no fuera por lo caro que sale este circo, ojalá se obligase a dar las piruetas desde el trapecio sin red, y a meter la cabeza en las fauces de un león a dieta blanda, o que los payasos salieran apretándoles los zapatones y la cara sin pintar. Nostalgia de teatro chino de Manolita Chen, cuando las agitadas sicalípticas de revista dieron paso a un cuplé cuyas transparencias se deshacían en jirones saltando las costuras de la censura impuesta y los dos rombos, pero los cicutas tacañones de entonces por más que sacaban la cinta de medir el tiro de la minifalta al suelo pasando por la rodilla de las azafatas gafotas o asomarse a los vertiginosos escotes de alguna folclórica eran incapaces de presentir lo que se avecinaba. Lo del dedo y la luna.

Pues ya volvió con aquellas clamorosas tardes sudorosas de pañuelos al aire y vueltas al ruedo recogiendo castas ristras de choricillos oreados hasta que la moda lo trocó por las impúdicas prendas íntimas destilando luminol que recogía aquel pseudotototorero de Ubrique que democratizó la imposición de encornaduras en los platós de televisión aderezando zafios cotilleadores pringados de salsa cocktail para mojar su miga.

Y no ha dejado de irse ese torito enamorado de la luna, porque ni los tuits ni los stories, ni los followers ni los trolls, ni los influencers ni los tertulianos han dejado de estar ahí para rellenar el espacio de tiempo perdido, y el ring de fango adiposo, que ralentiza los movimientos y llaves dejando exhaustas a las mentes más argumentadoras sucumbiendo bajo las pegajosas consignas de los más vociferantes. Solo falta el rito del paso firme sobre las ascuas con la prenda a cuestas y la fe inquebrantable de no quemarse las plantas de los pies. Como los que buscan las mieles del paraíso por la vía rápida.

MCR estrena nuevo Espacio Showroom

El mayorista MCR estrena su nuevo Espacio Showroom, concretamente en la planta superior de una nave de 8.000 m2 de almacenamiento, aledaña al centro logístico de su sede central, ambos situados en Getafe (Madrid). Un innovador lugar de encuentro en el que la compañía española muestra las tecnologías que comercializa por verticales con el fin de brindar a sus integradores y fabricantes un marco de trabajo para dar a conocer las soluciones más punteras a sus clientes y mostrar todas sus posibilidades en acción para el desarrollo de los proyectos.

El espacio, de 876 metros cuadrados de exposición, ha sido diseñado por el equipo de técnicos e ingenieros de MCR y está segmentado en función de las tecnologías que integran las diferentes líneas de negocio profesional como AV Pro, Digital Signage, Seguridad Electrónica e Infraestructura de Red. Del mismo modo, está dividido en diferentes verticales: Educación, Gaming, Centro de control CCTV, Retail, Corporate, Horeca y Residencial.

El showroom cuenta además con un auditorio que dará cabida a formaciones, charlas, presentaciones... con posibilidad de hacerlas presenciales o vía streaming, así como un completo plató de TV. En palabras de Pedro Quiroga, CEO de MCR, "nuestro showroom es un espacio dinámico y personalizado. No queremos que el producto se quede obsoleto. Queremos que las novedades puedan incluirse en este espacio para hacerlo vivo y que esté a la altura de las necesidades de los integradores y del mercado".

Espacio dinámico y personalizado

La filosofía del showroom de MCR es ser un espacio dinámico que pueda adaptarse en cada momento a las necesidades de los clientes, a la evolución tecnológica y que por tanto, sea capaz de personalizarse a medida e ir mostrando novedades según vayan surgiendo.

Como explica Enrique Hernández, director de B2B de MCR, "este showroom significa mucho para MCR y con el que damos un paso más hacia la calidad en un negocio en el que entendemos que el valor, tiene que ser seña de identidad. Este espacio nos va a permitir estar al lado del partner que va a poder ver las soluciones de diferentes fabricantes y contar con un lugar que podrá adaptarse en cada momento a las necesidades de los clientes. Vamos a trabajar mucho en la línea de poder estar muy cerca de cada proyecto y por tanto, muy pendientes de cada necesidad técnica que tengan".

Una sala de demostraciones y un centro de experiencia pensado "por y para los integradores" y donde tienen cabida los diferentes fabricantes que han contribuido a la puesta en marcha de este espacio innovador y práctico, un universo habitado por 4.000 figuras dentro del mundo audiovisual (1.700), seguridad electrónica (800) y telecomunicaciones (1.500). Todo lo que está expuesto en el showroom es producto distribuido por MCR, con lo cual, la capacidad de llegar a cada proyecto es real. "Esto puede beneficiar especialmente al integrador mediano, que es el que menos recursos tiene", apunta Hernández.

En todo momento, el showroom estará atendido por el equipo de especialistas de MCR para ofrecer un asesoramiento completo a los integradores que acudan con sus clientes, dando acceso al equipo de preventa de ingeniería de cada una de las líneas de negocio de MRC. Para ello, solo será necesario reservar el espacio (a través de una app) por media jornada o jornada completa, estando la privacidad de los usuarios garantizada. No tiene ningún coste, salvo el de los servicios asociados a su uso (catering, azafatas, etc.).

"MCR quiere que sus fabricantes y partners B2B puedan generar más negocio. De hecho, se trata de una apuesta por el cross-selling, dado que creemos firmemente en esta estrategia. Está pensado por y para el negocio, y esta es la prueba de dicha apuesta", concluye el directivo de MCR Pro.

OVHcloud premia al ecosistema de partners en su evento “Backstage”

El grupo OVHcloud ha reunido a más de una centena de partners y colaboradores con el objetivo de celebrar el crecimiento de su programa para partners en España y premiar a los miembros más destacados del año. En el encuentro celebrado en Madrid, la compañía ha compartido sus novedades tecnológicas y su visión sobre las ventajas de una colaboración cercana, así como los beneficios que el OVHcloud Partner Program ofrece al canal, con un modelo transparente, accesible y previsible en precios.

En una clara apuesta por la especialización del ecosistema y las soluciones PaaS y de IA, el OVHcloud Partner Program está orientado a facilitar que los partners de todo el mundo puedan sacar el mayor partido a la infraestructura del grupo, dotándoles de las herramientas necesarias para crecer y crear soluciones y servicios de gran valor añadido para sus clientes. OVHcloud sigue fortaleciendo su programa de canal y apostando por los partners para su aceleración, incluyendo nuevos beneficios financieros y de co-marketing, laboratorios técnicos y de ventas dedicados para generar nuevas oportunidades comerciales, y acceso prioritario a las versiones beta de nuevos productos y tecnología cloud sin costes.

El OVHcloud Partner Program ha experimentado un gran crecimiento en España hasta alcanzar más de 110 partners a nivel nacional, de los cuales cerca de 50 se han unido al programa en el último año. “Los partners son clave dentro de la estrategia de crecimiento de OVHcloud, nuestra intención es aprovechar las sinergias en un marco de estrecha colaboración, aportándoles la mejor experiencia posible. Creemos que es una fórmula exitosa: el canal aporta sus conocimientos y su atención especializada y nosotros un amplio portfolio de infraestructuras y plataformas cloud soberanas. Nuestros 111 partners en España son una prueba de que el canal valora nuestra propuesta”, ha señalado Cristina Ortiz, Partner Program Manager de OVHcloud en España.

La gestión del dato como nueva oportunidad para el canal

Durante el evento, miembros de OVHcloud Partner Program participaron en una mesa redonda sobre el ecosistema y cómo el trabajo colaborativo entre los proveedores y los partners es clave para generar valor, innovar y sobre todo generar crecimiento conjunto. José Manuel Borrego (CEO de 720tec), Marco Antonio Sanz Molina (CEO de CloudAPPi) y Santiago Lobo Novella (CEO de Lobo Brothers Technology) fueron los encargados de abordar temas clave como la importancia de la especialización entre los partners y la formación, así como las interacciones dentro del ecosistema.

A lo largo de la jornada también se hizo hincapié en la enorme oportunidad que supone el despliegue del PaaS, y el potencial de las nuevas soluciones AI Endpoints y Data Platform de OVHcloud para aprovechar el máximo valor de los datos e impulsar los proyectos de IA. OVHcloud ha visto un crecimiento en la demanda de soluciones PaaS en su universo de Public Cloud por parte del canal, ya que permite una mayor flexibilidad y agilidad.

El partner puede aprovechar este conjunto de herramientas en áreas clave como la gestión de bases de datos, la IA o el almacenamiento para optimizar su tiempo y su esfuerzo, así como evolucionar en sus soluciones y abordar proyectos de mayor valor. Tal y como afirma Ortiz, “en 2024 la adopción del PaaS está marcando el camino hacia la especialización del canal, en un área donde ya estamos viendo un crecimiento brutal. Gracias a un catálogo de herramientas de gran valor los partners pueden desplegar proyectos más evolucionados, de una forma sencilla y con sello europeo”.

Premios del OVHcloud Partner Program

En el evento también se hizo entrega de los premios a los partners más destacados del año, con el objetivo de reconocer su valor y aportación. Los galardonados incluyeron a:

- Rising Star Partner of the Year: W&B Asset Studio
- Business Excellence & Innovation Partner of the Year: CiC Consulting Informático
- New Partner of the Year: Pool Informático
- Partner of the Year: Inmasan Tecnología

Asimismo, también se entregaron menciones especiales por su papel en el desarrollo de la industria espacial tanto en España como Europa a los:

- Space Innovation & Global Expansion of the Year: SERCO
- Space Collaboration & Innovation Promise of the Year: GMV

Enséñale los dientes al ransomware.

OBTÉN LA DEFENSA
MÁS FEROZ CONTRA
AMENAZAS COMPLEJAS.

Barracuda®

Mesa de debate: Ciberseguridad 2024

Celebramos una mesa de debate más sobre ciberseguridad, asunto que ocupa y preocupa mucho a los responsables de los departamentos TI y cada vez más a los de continuidad de negocio. La llegada de nuevas normativas como NIS2 o DORA ya han encendido los pilotos de aviso en los consejos de administración, que empiezan a entender que con los datos de sus clientes no se juega y los mecanismos de defensa contra el cibercrimen ya no son una opción. Para poner en perspectiva cómo pilotar esta estrategia de adopción de las mejores prácticas, contamos con la participación de portavoces de Fortinet, Barracuda, ESET y Bitdefender que nos van a ayudar a alumbrar el camino salvo.

PARA AYUDAR a pertrecharnos y afrontar con garantías este sendero de la transformación digital y el salto a la nube, contamos con cuatro representativas figuras del sector a los que agradecemos su participación: Raúl Benito Álvarez, Territory Account Manager Iberia de Bitdefender; Guillermo Sato, Channel Account Manager de Fortinet; Miguel López, Regional Sales Director Iberia de Barracuda; y Carlos Tortosa, Key Account Director de ESET España. Y sin más preámbulos, esto es lo que dio de sí la provechosa conversación.

REPASO AL PANORAMA ACTUAL

¿Qué balance hacéis de lo que va del 2024, cómo va el negocio? ¿Se está cumpliendo el guion marcado en cuanto al roadmap de productos?

Bitdefender: Para nosotros este año está siendo bastante ajustado a lo que estábamos previendo, no tanto al volumen de revenues que es algo que poco a poco vamos empujando y que al final como todos dependemos de los últimos Qus para ver cómo acabamos el año, pero de momento yo creo que la tendencia es bastante buena, sobre todo han ayudado las nuevas soluciones y cómo está evolucionando el portfolio de productos que tenemos.

Sí que es verdad que hace unos cuantos años solamente vendíamos lo que es la parte de EDR en el endpoint, pero llevamos incorporando muchos addons, y nos metemos con la parte de XDR, con todos los sensores, con la parte de MDR de gestión, con ciertos servicios para ayudar al partner, para dar toda esa extensión. Entonces toda esa evolución que sí que se programó en el año pasado de nuevas features, para poder consolidar nuestra estrategia de native XDR, yo creo que ha servido para seguir con esa tendencia de crecimiento en todos los segmentos, tanto en el mercado Big Enterprise como en la parte de SMB o la parte de MSP, que son negocios bastante consolidados.

Fortinet: Desde Fortinet lo que estamos viendo es que todos los clientes siguen inmersos en la transformación digital y yo creo que el gran cambio de los últimos años es que ya nadie duda de esta necesidad. La parte de la ciberseguridad es clave en toda esta transformación y la continuidad de negocio, y al final esto es un empuje tremendo. Sin embargo, hemos notado cierta desaceleración en segmentos que han sido claves como motor fundamental de nuestro crecimiento en el pasado, como puede ser toda la parte SD-WAN, y sin embargo otras áreas como la parte de SASE o la de SecOps y toda la parte de operación del SOC, pues sí que están creciendo mucho. No seguimos creciendo a un ritmo de por encima del 30% como veníamos acostumbrados, pero sigue siendo un crecimiento por encima del doble dígito.

Barracuda: Pues 2024 comienza con las expectativas que teníamos el año pasado cumpliéndose,

fuimos una de las regiones de Europa que más creció y para este año contamos con casi el doble de plantilla. Poco a poco el mercado va asumiendo la necesidad de considerar la ciberseguridad como un elemento clave a la hora de hacer inversiones. Probablemente todavía no al ritmo que sería necesario o deseable, teniendo en cuenta que siguen existiendo amenazas muy importantes y de gran impacto, pero pensamos que al menos la tendencia es positiva. Existe una preocupación creciente por todo lo relacionado con la ciberseguridad, y eso evidentemente tiene un impacto positivo para nuestro sector.

ESET: Nosotros estamos también cubriendo las expectativas. Hay que tener en cuenta que veníamos de un año muy bueno, y ahora lo que estamos intentando es mantener las cifras con el que terminamos el 2023, y esto de 2024 ha comenzado relativamente bien. Hemos introducido cambios sobre todo a nivel de canal de distribución con un nuevo programa y eso está favoreciendo a la captación o en cualquier caso fidelización de partners que ya estaban trabajando con nosotros.

De lo que era la parte básica del antivirus y el cortafuegos hace años se ha ido evolucionando hacia los MDR y ahora lo ha extendido los XDR, incluso SASE. ¿Vosotros tenéis integrado todas estas siglas en vuestra oferta ya o cómo estáis rediseñando los productos?

Bitdefender: Confieso que la parte de antivirus nos suena ya muy viejo, aunque sí ha evolucionado muchísimo. Igual que MDR ya es algo muy maduro. Se ha democratizado su uso y hoy cualquier empresa puede adoptar este tipo de soluciones. Para nosotros es nuestra principal solución, aparte de XDR. Por los ataques que estamos viendo y sufriendo a través de nuestros técnicos que tenemos in-house monitorizando lo que está pasando, habitualmente fuera del horario laboral normal. La parte de MDR es una tendencia que nadie puede ignorar. La necesidad de ese 24x7 de gestión de incidentes y de alertas por personal muy cualificado es algo que cualquier empresa, por pequeña o grande, va a necesitar. Esto las grandes lo han adoptado desde hace bastante tiempo, a las medianas les cuesta el poder adoptar esos SOCs por el tema del coste, y yo creo que la mayor parte de los fabricantes estamos adoptando este tipo de servicios para poder proveerlo de forma masiva. Los precios que se están manejando sí que permiten que un servicio 24x7 de gestión de incidencias y alertas pueda estar al alcance de cualquier tipo de empresa.

Para nosotros es esencial ese crecimiento con lo que es y poder monitorizar qué es lo que está pasando en el endpoint para tener una visibilidad más completa. Igual de necesario con toda la parte de Cloud Security Posture Management, pero además con cualquier movimiento que pueda haber dentro de esa infraestructura cloud, incluso en red, el tener sensores de red que nos pueda ayudar realmente a esos movimientos laterales, esa exfiltración de información, de saber exactamente por dónde ha venido o hacia dónde ha ido. En las integraciones con Office 365 o G-Suite cada vez son más necesarias. Todo esto ha ayudado también por esa visibilidad que tenemos cada vez más de la parte de identidad en el Azure Active Directory, nos da una capacidad de entender muy bien qué es lo que ha pasado en el incidente y hasta dónde ha podido llegar, que para nosotros es clave a la hora de poder mitigar cualquier brecha que haya sufrido un cliente. Sí que es verdad que en la parte de firewall es algo que no hemos trabajado, y no vamos a trabajar, estamos mucho más focalizados en esos conectores que podamos tener a disposición en la cloud o esos firewalls virtuales para que el cliente pueda adoptar cualquier medida de revisión o de recuperación rápida y eficiente y eficaz en el minuto o en el segundo cero.

Fortinet: Al final estas soluciones MDR/XDR son pilares fundamentales. Nuestra visión Security Fabric lo que propone a los partners y clientes es un acercamiento de plataforma, donde hemos puesto nuestro portfolio que está conformado por 57 soluciones distintas que interactúan de forma conjunta. En este sentido, hemos reorganizado toda la parte del offering este año en tres planes fundamentales. Todo lo que es la parte de Security Networking, que vendría siendo la parte como un Netflix a la carta de Next Generation Firewall, SD-WAN y demás producto tradicional. Luego está la parte de SecOps, donde está englobado todo el MDR/XDR y donde estamos teniendo un crecimiento muy importante, dado que históricamente quizás no hemos sido un fabricante muy posicionado en esta área. Y el tercer pilar que tenemos que es precisamente SASE, donde estamos compitiendo de forma muy positiva porque al final los players hasta ahora de este segmento, se fundamentaban en SSE, principalmente de lo que es el control de la postura de seguridad hacia la nube y demás. Como single vendor de SASE, o sea el mismo fabricante que provee de la solución no solo de SD-WAN sino también de la parte SSE, pues estamos teniendo un tirón importantísimo y creemos que aquí además hay una oportunidad de negocio y crecimiento tremenda para nuestro canal.

Barracuda: La verdad es que todos estos nuevos conceptos son algo que llevamos años trabajándolos, toda la oferta de MDR/XDR es algo que está incorporada a nuestro portfolio desde hace tiempo y también todo el planteamiento de SASE. De hecho toda nuestra oferta de firewall viene incluyendo Zero Trust, SD-WAN, gestión del tráfico inteligente y demás desde hace bastantes años.

El foco ahora mismo es plantear todo esto como una plataforma, de manera que nuestros partners y nuestros clientes puedan integrar aquellas piezas que mejor encajen o que necesiten en cada momento y puedan hacerlo de manera escalable, tratando siempre de simplificar la adopción de estas tecnologías, porque muchas veces el gran freno es el grado de complejidad que perciben a la hora de implementarlos. De manera que lo que intentamos es que la adopción de estos nuevos estándares sean cada vez más sencillos, sean manejables, con un equipo técnico que nunca va a ser tan amplio como nos gustaría que fuera, de forma que los clientes se sientan cómodos utilizando e integrando cada vez nuevos elementos dentro de la plataforma común de gestión que nosotros proporcionamos.

Por encima de todo esto, además, tenemos toda esta parte de gestión de MDR, de XDR, donde vamos a dar todos estos servicios 24x7 de gestión de seguridad, sea sobre nuestros propios productos o sobre productos de terceros, que esto también es muy importante. No es necesario contar con una infraestructura de ciberseguridad monocolor para poder contar con servicios de gestión de MDR/XDR, no solo a nivel de puestos, sino a nivel de servidores, a nivel de firewall, a nivel de seguridad en el cloud. Con lo cual, un cliente puede tener realmente un servicio 24x7 de MDR proporcionado por nosotros, con nosotros, respaldando a su partner para dar este servicio y donde va a poder integrar no solamente, los productos de Barracuda, sino aquellos que pueda tener de otros fabricantes que todavía ha decidido no cambiar o que siguen siendo válidos. De manera que puede tener una adopción de estos estándares que no va a ser disruptiva, que no le va a forzar a tener que licenciar o jubilar, por decirlo así, elementos de ciberseguridad de otros fabricantes. Va a poder amortizarlos hasta el fin de su vida útil utilizando nuestras tecnologías.

ESET: Nosotros tenemos dentro de nuestro catálogo de productos un EDR y un XDR desde hace varios años. Lo que hicimos en 2023 fue precisamente integrarlo todo en una única solución, ESET Protect Elite. No fue únicamente MDR/XDR, sino que compramos todas nuestras tecnologías, es decir, desde la identificación de usuario hasta el endpoint o el MDR, las sandbox, protección de Office, etc. Le dimos muchísima importancia a que el usuario final tuviera muy claro que con un único nivel podía tener acceso a toda la protección. Nosotros les podíamos facilitar todo esto, se construye en una especie de pirámide que está basada principalmente en nuestra consola de administración de ESET Protect. También facilitamos a nuestros partners para que gestionen la seguridad de sus clientes, y por otra parte nuestro servicio de soporte. Este SAT está basado en los técnicos que tenemos de nuestra sede central aquí en Valencia, que dan soporte y servicio a todos nuestros clientes a nivel nacional.

Nos centramos mucho en nuestros productos, pero dejamos muy claro que no queríamos competir con nuestro canal de distribución facilitando servicios que ellos ya podían dar. Es decir, lo vendemos o lo facilitamos al cliente final por medio del canal de distribución, dejando claro que si ellos incorporan tecnologías diferentes, dependa únicamente de ellos el poder facilitar este servicio.

Independientemente de esto, nuestro MDR sí que está gestionado por nosotros. En el caso de que el cliente general o de que nuestro partner no tenga suficiente especialización para poder facilitar este servicio, es verdad que cada vez más es necesario contar con estas tecnologías de cualquiera de los fabricantes. Sabemos que va a ser muy difícil conseguir una garantía de seguridad 100%, pero como

mínimo intentar mitigar cualquier amenaza antes de que afecte al cliente.

Por lo que veo estáis todos evolucionando en tener unas soluciones unificadas. ¿Cómo creéis que os defendéis mejor ante el mercado: con una propuesta propia de extremo a extremo o preferís tener una solución muy especializada y muy buena que se puede integrar dentro de un ecosistema de terceros fabricantes?

Bitdefender: Yo creo que tienes que tener una, vamos a decir, una capacidad de adaptarte. Sí que es verdad que en un segmento small business o medium, a lo mejor una solución única que permite un casi plug and play sin necesidad de tener que definir conectores, de tener que parsear logs, de tener que correlar cosas, pues simplifica bastante la gestión. Y todos vamos también un poco hacia allí, a poder integrar con nuestros elementos el darle un servicio, vamos a decir, en one-shot al cliente sin que tenga que trabajar para desarrollar código. Al final la simplificación es necesaria, y una plataforma única lo es. Pero sí que es verdad que cuando vas a un mercado Enterprise, lo que no puedes es pretender, bueno, hay algunos que sí que lo pretenden, por supuesto, es que tengan todo de tu mismo color. Entonces sí tienes que estar abriendo a través de API, a través de conectores. Todos estamos trabajando en data lakes que permitan ingestar datos de terceros, de conectarte con un Office 365, de conectarte con el Active Directory, de permitir coger logs de los firewalls, independientemente de quiénes sean.

Pero sí que es verdad que para diferentes tipos de mercado o de clientes tienes que tener aproximaciones diferentes, que sean flexibles y que se puedan adaptar un poco a las necesidades. Por supuesto que la simplificación de tener todo cubierto con nuestras soluciones, nos ayuda a poder llegar antes a un cliente y dar una solución al día siguiente. Pero sí que es verdad que nos tenemos que adaptar a un ecosistema de soluciones donde el cliente también ha invertido. Esa adaptabilidad en función a lo que el cliente necesita, es donde estamos.

Fortinet: Recientemente llevamos a cabo nuestro evento en Bilbao, el Security Day, y estábamos comentando que en ediciones pasadas, en el 2020, el 80% de los clientes se planteaban un poquito la posibilidad de intentar consolidar soluciones dado que empezaban a tener demasiadas y era complicada la gestión. Y sin embargo, el año pasado hablábamos de que el 95% no es que se lo planteasen remotamente, sino que lo veían como una necesidad.

Estamos en una espiral donde los ciberataques cada vez son más complejos. Todos coincidimos en que hay una escasez tremenda de recursos de personas especialistas en torno a la ciberseguridad. Los vectores de ataque y todo lo que es el perímetro no hace sino expandirse, con lo cual realmente trabajar estos entornos se hace muy complejo. Y además la seguridad 100% es muy complicada de obtener, con lo cual este acercamiento del Best of Breed, de tener soluciones específicas para cada vector de ataque, que sí que puede ser lo mejor del mundo y luego ya veré cómo me integro con el resto, esto es demasiado complicado y los clientes así nos lo trasladan.

Raúl Benito Álvarez,
Territory Account Manager Iberia de Bitdefender.

De hecho, en nuestro caso, yo creo que era cinco o seis años antes de que Gartner lanzase su famoso CSMA, su acercamiento como Cibersecurity Mesh Architecture, donde recomiendan que los clientes deben tener no más de quizás un par de plataformas generales que les permitan gestionar y operar todo lo que sería el riesgo de ciberseguridad. Pues nuestro acercamiento venía siendo el de Security Fabric, donde todo el portfolio está desarrollado internamente y cuando hay cualquier compra puntual, lo que se hace es embeberla y se integra sobre nuestro sistema operativo para que podamos directamente detonar un montón de playbooks y automatismos para utilizar esa información y mejorar los tiempos de detección sobre todo, pero por supuesto, reacción y recuperación. Y esta es la piedra sobre la que trabaja Fortinet y que además el canal lo está aceptando muy bien.

«La ciberseguridad ha sido como un stopper para ciertas facetas del negocio, aunque cada vez más se ve como un facilitador para la continuidad del mismo. Por tanto, zero trust por supuesto que sí, pero tenemos que dejar una parte abierta, una parte de flexibilidad. Esa parte es la que podemos cubrir con la inteligencia artificial» (Raúl Benito, Bitdefender)

Barracuda: Estamos hablando ahora mismo en un entorno en el que vemos que prácticamente todos los clientes se enfrentan a grandes retos relacionados con la falta de talento en el sector TI en general y en el de la ciberseguridad en particular. Vemos que un porcentaje muy elevado de los ataques, de las brechas que se producen, están originados por fallos de configuración, fallos humanos, errores a la hora de operar las herramientas que tenemos. Si metemos todo eso conjuntamente, llegamos a la conclusión de que realmente un entorno donde la industria del cibercrimen crece a unos ritmos similares a los de, por desgracia, otras industrias también malvadas, por decirlo así, como pueden ser el tráfico de armas o el de drogas, estamos viendo una potencia en el lado oscuro que realmente la única forma de contrarrestarlo con los recursos que podemos tener en el lado bueno, es apostar por la simplicidad, es decir, apostar por tratar de contar con una plataforma de seguridad que nos permita paliar esa falta de recursos humanos que muchas veces tenemos, a veces también recursos económicos o técnicos, y que podamos contar con herramientas que tengan un nivel de integración, que sean horizontales, que puedan cubrir la mayor cantidad posible de vectores de ataque.

Este planteamiento de simplicidad, que antes era más habitual en entornos de pequeña o mediana cuenta, está empezando en los segmentos Enterprise. Es decir, incluso las empresas grandes son conscientes de que mantener un nivel de complejidad Best of Breed también es muy difícil con las plantillas, con los recursos que incluso estas grandes empresas pueden tener. De manera que empiezan a decantarse por plataformas de seguridad integradas donde con una única puedan cubrir la mayor cantidad de vectores de ataque posible. Y eso es algo que desde Barracuda llevamos haciendo ya 20 años. Es decir, nuestro foco precisamente ha sido desde siempre el contar con una plataforma de ciberseguridad a la que hemos ido añadiendo cada vez mayores elementos, muchos de ellos desarrollados integralmente, en otros casos por adquisiciones, pero siempre dentro de una oferta que permite que nuestros clientes puedan coger y tener una plataforma a la que ir añadiendo más funcionalidades, contando con una única gestión, una única configuración, un único punto de soporte, lo que reduce muchísimo la curva de aprendizaje.

Se puede pasar de tener una solución de Barracuda para proteger el vector de ataque de correo, por ejemplo, a proteger el vector de ataque de aplicaciones web o el vector de ataque de conexión a la red mediante firewalls, todo ello en una única plataforma y con un look and feel común, con un sistema de gestión común que va a facilitar mucho la adopción de esta tecnología y que va a permitir que todo lo que es la curva de aprendizaje, como mencionaba, sea muchísimo más rápida que si se trata de ir adoptando diferentes tecnologías, pero siempre con la flexibilidad de poder integrar aquella parte que se requiera. De manera que yo creo que sí, esto es una tendencia de mercado muy clara, en la que nuestro canal claramente está apostando y que es una de las claves del éxito que estamos teniendo.

Cibercrimen e Inteligencia Artificial, la tormenta perfecta

La utilización de inteligencia artificial (IA) para robar credenciales y acceder a redes de alto valor por parte de los ciberdelincuentes está empezando a tener un impacto visible en el número e importancia de incidentes de seguridad detectados. Las credenciales robadas con estas herramientas basadas en IA son extremadamente valiosas para los criminales cibernéticos, ya que les permiten acceder a sistemas y tomar control de cuentas con un riesgo reducido de activar alertas de seguridad. Una vez que acceden a un sistema, comienzan tareas como reconocimiento de red, escalada de privilegios y exfiltración de datos, lo que puede desembocar en ataques de ransomware o en la creación de amenazas persistentes avanzadas.

Los ataques basados en contraseñas no son el único método para acceder a un sistema; los actores de amenazas también explotan puntos de acceso remoto y utilizan técnicas de adivinación rápida de credenciales. La IA les ayuda a extender el "tiempo de permanencia" en la red, facilitando que se mezclen con el tráfico normal de la red utilizando credenciales robadas.

Entre las técnicas más destacadas impulsadas por IA están:

1. *Phishing y la ingeniería social*: La IA puede generar correos electrónicos de phishing que imitan el lenguaje y estilo de comunicaciones legítimas, lo que aumenta su efectividad para capturar credenciales o engañar a usuarios autorizados para que proporcionen acceso a los atacantes.
2. *Deepfakes*: Los actores de amenazas utilizan IA para crear videos o clips de audio que imitan a ejecutivos o figuras de autoridad para engañar a los empleados y realizar transferencias de fondos a cuentas fraudulentas.
3. *Desarrollo de malware*: La IA se emplea para crear malware "inteligente" que puede alterar su código y evitar la detección por sistemas de seguridad tradicionales, facilitando el robo de credenciales.
4. *Reconocimiento automatizado*: La IA procesa datos rápidamente para identificar objetivos y vulnerabilidades, usando información de fuentes públicas y escaneando repositorios de código y sitios web en busca de configuraciones erróneas y otras vulnerabilidades.
5. *Chatbots IA para ingeniería social*: Automatizan ataques de phishing para engañar a los usuarios y obtener acceso indebido.

Los sets de credenciales de alto valor no solo permiten a los atacantes acceder a sistemas como si fueran usuarios autorizados, sino que también se venden en foros de cibercrimen. Un estudio reveló que las credenciales pueden venderse entre 5 € y 50 € por cuenta, dependiendo del tipo de cuenta y la información disponible.

Para protegerse contra el robo de credenciales impulsado por IA, es esencial adoptar políticas de seguridad robustas, educar y concienciar a los usuarios, y utilizar soluciones de seguridad avanzadas. Algunas medidas incluyen el uso de contraseñas fuertes y únicas, autenticación multifactor, actualización y parcheo de sistemas, herramientas de seguridad alimentadas por IA, y la adopción de principios de Confianza Cero que verifican continuamente la identidad y la confiabilidad de dispositivos y usuarios, incluso cuando los actores de amenazas tienen credenciales válidas.

Si bien es cierto que la utilización de herramientas de IA por parte del cibercrimen puede poner contra las cuerdas a mas de una organización también lo es que la mejor forma de afrontar esta nueva amenazas es, precisamente, mediante herramientas de protección que incorporen a su vez la IA como elemento estratégico y clave en su funcionamiento.

Miguel López
Regional Sales Manager – Iberia
Barracuda Networks

ESET: Nosotros también consideramos que es mucho más fácil para el cliente final de que se dé de manera conjunta todas las tecnologías que nosotros podemos facilitarle a nivel de protección. Por eso tenemos una solución en la que integramos absolutamente todas ellas, desde la identificación de usuario hasta la línea de software. Hay niveles inferiores donde el cliente final va a decidir qué tipo de protección necesita, porque igual prefiere no casarse con una única marca, sino utilizar diferentes niveles con diferentes tecnologías. Todo esto nosotros lo gestionamos directamente o facilitamos al cliente en una única herramienta, se llama ESET Protect, donde se gestiona absolutamente todos nuestros productos integrados, tanto en un formato cloud que nosotros certificamos y estando esta consola de administración dentro de la Unión Europea para un posible cumplimiento normativo de los verticales, o como por otra parte realizar la instalación de esta herramienta en un CPD interno o subcontratado por el mismo.

Aparte de esto, también damos mucha importancia a un servicio de seguridad llave en mano, es decir, el cliente puede tranquilamente realizar una solicitud de nuestros productos, nosotros acordaremos con él evidentemente la finalización del proyecto, nuestros técnicos certificados por ESET serán quienes le pongan en marcha el funcionamiento de la herramienta y quienes la optimicen al máximo, complementando con el MDR un formato 24x7 para dar la mejor protección posible que nosotros podemos facilitar.

Está claro que la IA está en boca de todos y en vuestros productos, pero también en manos de los malos. ¿Cómo estáis aplicando vosotros la inteligencia artificial? Me imagino que sobre todo para automatizar tareas y detectar ataques, aunque… ¿no sería más fácil ir al zero trust y cortar por lo sano?

Bitdefender: Yo creo que el zero trust lo tenemos todos metido, no es una cosa o la otra. Tenemos que ir al zero trust, pero la ciberseguridad siempre ha sido como un stopper para ciertas facetas del negocio. Aunque cada vez más la ciberseguridad se ve como un facilitador, realmente ahora se empieza a ver dentro del comité de dirección como una necesidad más para poder ser eficiente y para poder continuar en el negocio. Por tanto, el zero trust por supuesto que sí, pero tenemos que dejar una parte abierta, una parte de flexibilidad. Esa parte es la que podemos cubrir con la inteligencia artificial. Con motores basados en comportamiento, correlación de datos, aprendizaje y machine learning.

Vemos a la inteligencia artificial como algo que está fuera y que tenemos que entender para poder protegernos. ChatGPT ha logrado democratizar el que cualquier persona sin conocimientos técnicos pueda estar desarrollando, pueda estar modificando, pueda estar lanzando un ataque a cualquier empresa por grande que sea. Tenemos que desarrollar soluciones que detecten este tipo de, vamos a decir, de nuevos vectores de ataque. Entonces ahí es a donde vamos, el poder utilizar la IA. Yo creo que llevamos más de diez años utilizando inteligencia artificial. Sí que es verdad que se ha desarrollado ahora mucho más y que nos ayuda para automatizar ciertas acciones dentro de nuestro propio SOC.

Es el incorporar estos nuevos algoritmos y el permitirnos con un lenguaje natural el poder hacer ciertas acciones que antes era complejo, necesitabas a alguien que supiese programar, donde nos está ayudando. Pero para mí ha sido una evolución de lo que estábamos utilizando desde hace bastante tiempo. Los malos lo utilizan, los buenos lo utilizamos y tenemos que basarnos en la tecnología y en el avance de la tecnología para estar preparados.

Fortinet: No puedo decir toda la vida, porque esto, inteligencia artificial o conceptos como machine learning son un pelín más modernos, pero realmente no podemos trabajar de otra forma. Hace tres años ya, yo creo que era IDC quien decía que uno de cada dos firewalls que se vendían a nivel mundial son de Fortinet, son nuestros. Todos estos equipos al final están actuando como sondas y están mandando una telemetría con la que hordas de expertos de ciberseguridad están trabajando y haciendo el threat hunting desde nuestros Fortigate NGFW, es fundamental el utilizar y apoyarte en herramientas de tipo inteligencia artificial y machine learning, como decía, para realmente poder sacar el jugo y ser capaz de detectar ataques, lanzar firmas y poder reaccionar y solventar la problemática.

Pero claro, la democratización de la IA también me pone los pelos como escarpias, porque ChatGPT lo conocemos todos, pero el WormGPT está en la dark web, y con lenguaje natural y sin gran conocimiento técnico me meto, le digo, "oye, dame aquí un ataque multivector", esto con cuatro palabrejas y de repente, efectivamente, ahí te lanza un código que funciona y depende cómo lo utilice, pues la podemos liar muy parda. La IA ha llegado para quedarse y tenemos que sacar el máximo rendimiento para contrarrestar y mejorar esos tiempos de aviso de cuando empiezan a ocurrir cosas, de detección temprana.

Hemos embebido tecnología AIOps en nuestra subida de gestión de logs internos en el SIEM y en el SOAR para que técnicos con unos conocimientos quizás no demasiado profundos puedan interactuar con nuestros sistemas y vea estas alertas, qué puede ser esto, cómo debería reaccionar. De esta forma podemos automatizar, venga aquí tienes un playbook, venga pues déjalo cargado para que la próxima vez que ocurra automáticamente se detonen y ya de paso generar un informe y que avise a través del sistema de ticketing que tenemos un mail, un mensaje y aparte, oye, por favor genérame un reporte pues para que esto quede recopilado y la próxima vez automáticamente sepamos de qué estamos hablando y esa reacción sea automática. Esto es la aplicación, directamente sin coste. Esto no es un producto, no es simplemente una función nueva, es aprovechar al máximo esos recursos especiales que quizás con técnicos menos cualificados puedan interactuar.

Barracuda: Conceptos como el machine learning, la inteligencia artificial es algo que todos los fabricantes que estamos en este mercado llevamos años trabajando con ellos. Recuerdo que cuando me incorporé a Barracuda hace algo más de once años en el training inicial ya nos mencionaban estos conceptos dentro de nuestra nube para poder detectar patrones, comportamiento de los atacantes y demás. Evidentemente en la última década todo esto ha evolucionado mucho y parece impensable ahora mismo no tener una estrategia de ciberseguridad a nivel fabricante, a nivel de solución, pero también a nivel de clientes y de integradores que no contemple de alguna forma la inteligencia artificial como forma de enfrentarse a su vez a la inteligencia artificial que los malos van a utilizar. Todo lo que podemos pensar que es factible hacer desde el punto de vista positivo se puede hacer también desde el otro lado.

Pero debemos hacerlo desde una perspectiva que nos permita sacarle el máximo partido, como es una plataforma integral que nos va a permitir capturar, obtener mayor visibilidad de lo que está sucediendo en toda nuestra red en sus diferentes posibles vectores de ataque, esta inteligencia va a tener más información. Y sabemos que la inteligencia artificial se basa en la cantidad de información que sea capaz de procesar, cuanta más información, mayores posibilidades de poder detectar y actuar correctamente.

En cuanto al zero trust, de nuevo es otro de estos términos que se ponen de moda, pero que bueno, básicamente yo creo que es algo que parece bastante lógico el tener una estrategia basada en el mínimo privilegio para acceder únicamente aquello que realmente necesitan. Es un parámetro de prudencia bastante común. Nosotros llevamos también años implantando todo lo que sea la parte de zero trust en nuestras soluciones y la verdad, cuando se despliega una solución, sea de firewall como tal o simplemente una solución de zero trust para la conexión remota, directamente se está planteando de forma nativa en temas como VPN, que contemple realmente de forma global todos los posibles accesos e incluya los accesos al mundo cloud. Tenemos una gran cantidad de servicios en la nube, en diferentes nubes, que es necesario tener en consideración, y contar con una herramienta que permita hacerlo con simplicidad. Una de las grandes ventajas de nuestra estrategia zero trust es que es posible implementarla sin ni siquiera tener que cambiar el firewall existente. Es decir, no vamos a obligar a de nuevo a tener que jubilar herramientas o soluciones que igual todavía están dentro de su vida útil

ESET: Yo comenzaría haciendo un poco de historia, porque ya por el año 2002, en ESET construimos una gran base de datos que discerniera el futuro. Sí que es verdad que ahora se ha democratizado muchísimo lo que es el acceso a inteligencia artificial y ya realizábamos análisis de comportamientos para poder definir alertas con todos los radares que tenemos desplegados. Y aplicando esta inteligencia artificial poder determinar o facilitar a nuestros clientes finales por una mejora de producto, que nos permitía poder aplicar este machine learning o inteligencia artificial para promedio de análisis de

La doble vertiente de la IA en ciberseguridad

La popularización de la inteligencia artificial, y especialmente la IA generativa (GenAI) plantea nuevos retos a los directores de seguridad de la información (CISO). Los datos son contundentes: el año pasado dos tercios de las organizaciones confirmaron que ya estaban empezando a emplearla y sólo **el 3% de las empresas** no tenían previsto adoptar esta tecnología.

La IA se ha convertido en un arma de doble filo para la ciberseguridad: ha reducido la barrera de entrada a los atacantes y puede ser aprovechada por los ciberdefensores para la automatización inteligente y las estrategias de defensa.

Una tecnología que puede facilitar la actividad de los cibercriminales…

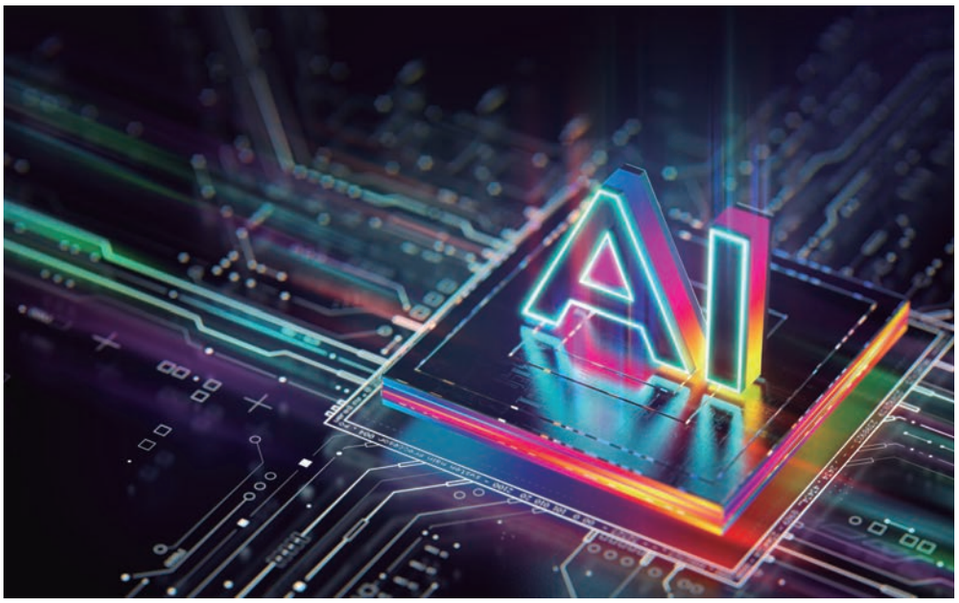
Gracias a GenAI, un posible ciberagente malicioso ya no necesita conocimientos de programación para crear malware, ya que las herramientas de IA de modelos de lenguaje extenso (LLM) lo permiten. La IA también se usa para explotar rápidamente vulnerabilidades de software conocidas públicamente, lo que da a los ciberdelincuentes la capacidad de aprovecharlas antes de que muchas organizaciones apliquen parches o actualizaciones. GenAI puede aumentar la sofisticación de los ataques de spear-phishing al evitar contenido repetitivo, errores ortográficos y gramaticales que solían ayudar a identificar el malware. Además, puede analizar el contenido de correos electrónicos comprometidos para generar mensajes personalizados que coincidan con la sintaxis y los asuntos utilizados anteriormente. Por ejemplo, la suplantación de voz y vídeo generados por IA son un método complejo de detectar.

Por otro lado, hace una década, sólo los Estados-nación tenían la capacidad de procesar grandes conjuntos de datos en CPDs. La revolución de la IA en la minería de datos y el aumento del poder de cálculo y el almacenamiento por uso hacen que los datos masivos sean objetivos atractivos para los criminales y los Estados-nación.

…y a la vez, contribuir a reforzar la acción de los ciberdefensores

Los profesionales de la ciberseguridad utilizan el término `superficie de ataque´ para describir la complejidad del entorno digital, que es difícil de mapear o entender por completo. La IA y las **arquitecturas de malla de ciberseguridad** ofrecen la oportunidad de convertir esta complejidad en una ventaja. Los sensores conectados permiten a los operadores de red y a los defensores generar datos en tiempo real, que la IA y el ML pueden analizar al instante.

Los ciberdelincuentes, incluso utilizando IA, rara vez tienen éxito en su primer intento, pero confían en que sus ataques fallidos pasen desapercibidos entre las numerosas alertas de seguridad. La IA ayuda a detectar y responder a actividades anómalas en tiempo real, protegiendo los activos digitales de la organización contra nuevos ataques. La eficacia de la IA y el ML depende de la cantidad de datos disponibles para su entrenamiento. Por lo general, los defensores tienen acceso a más datos que los atacantes. Aunque en ciertos casos, como el spear phishing, el atacante puede tener ventaja, la tendencia favorece al defensor en la “carrera armamentística de los macrodatos”.



Aunque la IA ofrece beneficios significativos para los CISO, su implementación en el lugar de trabajo enfrenta desafíos. Entre ellos cabe destacar las preocupaciones sobre la privacidad de datos en las consultas de GenAI infracciones de los derechos de autor, la revelación de información personal identificable, el uso de datos sesgados o censurables y resultados erróneos, conocidos como “alucinaciones” de la IA.

Las organizaciones son cautas con GenAI; pero los trabajadores a menudo no comprenden las razones detrás de esta precaución ni conocen las medidas de seguridad implementadas. Por tanto, GenAI se ha convertido en una forma de TI no oficial a la que deben enfrentarse los CISO y los CIO.

comportamiento, desplegar una mejora y el uso racional que nos daría ventaja.

Un tipo de protección donde no nos mitigue o no nos prohíbe el acceso a información que va a ser necesario. Es decir, tenemos que tenerlo bien planificado, tenemos que tener claro qué herramientas vamos a utilizar para este nivel de protección, para que realmente sea eficiente o no. Muchas veces estamos llegando a un nivel de protección que en algún caso nos encontramos con usuarios que finalmente no pueden realizar su trabajo del día a día. Esto suele ocurrir bastante con los falsos positivos. Consideramos que el Zero Trust tiene que estar bien definido para que sea una herramienta realmente robusta.

APOYO EN EL CANAL

Pasamos al capítulo del canal. Me gustaría que me contáis cómo lo tenéis estructurado y si es la versión de mayorista y después distribuidores y qué niveles tenéis.

Bitdefender: Seguimos con la versión tradicional de lo que es el canal, con ese tier 2. Todo nuestro negocio, tanto el de MSP como el de un reselling tradicional, sigue yendo a través de mayorista y el mayorista a través de partners, especialistas de seguridad que tienen que estar referenciados dentro de nuestro portfolio de partners. Dentro de ese portfolio seguimos teniendo el gold, silver y bronze en función del volumen de ventas y de la especialización que tenga de los conocimientos técnicos a la hora de poder desplegar y operar nuestras soluciones.

Aparte los programas de canal, que al final todos manejamos más o menos algo parecido. Para nosotros es esencial seguir trabajando y apoyando a este canal, donde hay una transformación muy importante: donde antes los canales eran como muy especializados en ciertos vendors y tenían a gente dedicada con un conocimiento muy alto, ahora cada vez vemos más que necesitan un apoyo por parte del fabricante. De ahí toda esta motivación de ir hacia el MDR, de tener servicios que puedan ponerse a disposición de nuestros partners para que ofrezcan un servicio de muy alto nivel.

Con este win-win que nosotros siempre hemos fomentado exclusivamente 100% a través de canal, ponemos a disposición herramientas para que puedan utilizarlas y generar negocio, y también dependiendo un poco el segmento, a lo mejor en Enterprise se está empezando a ver, pero se ve cada vez más en SMB y midmarket una orientación hacia ciertos mayoristas que trabajan muy especializados ese negocio MSP con partners igualmente especializados que ven la ciberseguridad como un servicio y donde al final el cliente es un poco lo que quiere, ese pago por uso. Estamos en entornos cada vez más flexibles, mucho más elásticos y donde la adaptabilidad no es solamente cuestión de precio. Contar con ese canal especializado es vital y por eso lo apoyamos con más soluciones, con más servicios y con más herramientas.

Fortinet: Nosotros también somos un fabricante 100% a través de canal, también tenemos dos niveles, trabajamos en local en España con dos mayoristas y de ahí cuelga toda nuestra estructura de partners. Hay una parte de modelo de canal más tradicional donde más o menos coincidimos todos, y hay hasta cuatro niveles de partnership dependiendo de la cifra de clientes, el plan de negocio conjunto y las certificaciones, y la capacidad técnica y de autonomía. Y luego hay sobre esto unos niveles que ya son regionales cuando ese partner tiene un ámbito de EMEA, LatAam, USA o APAC, y uno global cuando está en tres de las cuatro regiones.

«En 2020 el 80% de los clientes se planteaban intentar consolidar soluciones dado que empezaban a tener demasiadas. El año pasado el 95% no es que se lo planteasen, sino que lo veían como una necesidad. Mientras Gartner lanza su famoso CSMA donde recomiendan tener no más de dos plataformas» (Guillermo Sato, Fortinet)

La parte más interesante de nuestro programa de canal, que se llama Engage, es que aparte de este eje principal, consta de otros dos ejes. Uno que llamamos Business Model, que básicamente viene a explicar cómo el partner gana dinero y sus beneficios a través de nuestros productos y soluciones, y donde hay distintas figuras. Una que llamamos Integrator, donde al final se hace una reventa tradicional y el partner gana en ese margen de la reventa y sus servicios de instalación, implantación, integración y demás. Otra que sería la parte del MSSP, que es una línea de negocio creciente para un segmento más mid y small, donde claramente ya no sólo tienen complejidad en tener un responsable de TI, sino ya ni hablamos de la parte de ciberseguridad. Y luego también la parte de cloud con los CSP.

Guillermo Sato, Channel Account Manager de Fortinet.

Esto no es excluyente, un partner teniendo un determinado nivel de partnership puede optar luego a revender, dar servicio gestionado o dar soluciones de seguridad de las cargas y aplicativos que se suban a la nube. Es por ello que estamos lanzando una plataforma que se llama Fortiflex dentro de la línea de MSSP, donde pueda encontrar la práctica totalidad de nuestras soluciones, ya sea la de correo, la parte endpoint o la parte SASE y demás, pues están en formato de pago por uso, donde el partner adquiere una serie de puntos y directamente puede activar, desactivar, renovar, cargar funcionalidades y demás servicios al cliente. Lo que le da una total autonomía y libertad para controlar perfectamente sus costes, poder montar un catálogo de servicios adaptado al segmento que quiere atacar y esto está teniendo una muy buena aceptación.

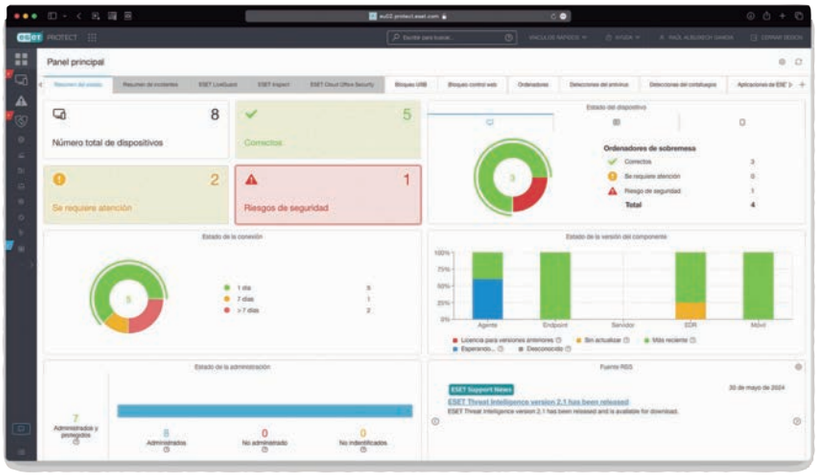
El tercer eje sería el de la especialización. Esto es una cosa totalmente opcional pero que todos los partners han interiorizado y están trabajando muy bien. Tenemos un catálogo de soluciones muy amplio que permite al canal hacer un acercamiento multivectorial, todo basado en plataforma, y les interesa a los partners y nos interesa a nosotros identificar cuáles son los socios especializados en un SASE, en un entorno industrial OT, en una parte de NAC, etc.

Estos serían los tres bloques de impulso de negocio que tenemos, que es Network Security, la parte SASE y operaciones de seguridad, y todas las soluciones están enmarcadas dentro de estos tres ámbitos y existen especializaciones específicas para que el canal se pueda diferenciar por un lado del resto de partners y por otro también poner en valor ese conocimiento para posicionarse de forma diferencial.

Barracuda: La estructura que tenemos es la tradicional de un fabricante con canal tier 2 de mayorista e integrador, donde el 100% de nuestras ventas se realiza a través del canal, no existe modelo de venta directa en ningún caso y donde el partner tiene total flexibilidad a la hora de elegir los modelos que más le encaje. Puede ser un partner que simplemente revende licencias; puede ser que utilizando las características de nuestra consola completamente gratuita y sin necesidad de instalar nada gestione las soluciones de sus clientes, lo permite también añadir los servicios de gestión que necesite; y tenemos una modalidad ya completamente de servicio gestionado con pago por uso, donde existe una flexibilidad total a la hora de funcionar, y donde el partner proporciona los servicios basados en nuestra tecnología.

Además de estos modelos que a día de hoy suponen ya un porcentaje de nuestras ventas cercano al 25%, tenemos modelos más avanzados que están empezando a tener bastante buena acogida, como es la venta a través de los marketplace oficiales de los grandes hiperescalares AWS, Azure, Google. En estos casos existe la posibilidad de que el proyecto

La ciberseguridad en el ámbito empresarial: el rol del EDR, MDR y XDR y la importancia de un servicio técnico profesional



LA CRECIENTE cantidad de ataques que se está produciendo en los primeros meses de 2024, DGT, Iberdrola, Banco Santander, por poner algunos ejemplos, plantea a las organizaciones la necesidad de aumentar la protección aplicada en las mismas, incorporando tecnologías que anteriormente ni se valoraban. Carlos Tortosa, director de Grandes Cuentas de ESET España comentaba esta reflexión durante su participación en la mesa-debate virtual de Ciberseguridad organizada por Taipricebook, y destacaba que "entre estas tecnologías se encuentra el EDR, en cualquiera de sus variantes, la cual se ha convertido en una herramienta imprescindible para la mejora de la seguridad. Y en esta evolución, el nacimiento de la sigla MDR ha supuesto que prácticamente todos los fabricantes invirtamos en proporcionar la mejor experiencia de usuario posible con la mayor protección disponible."

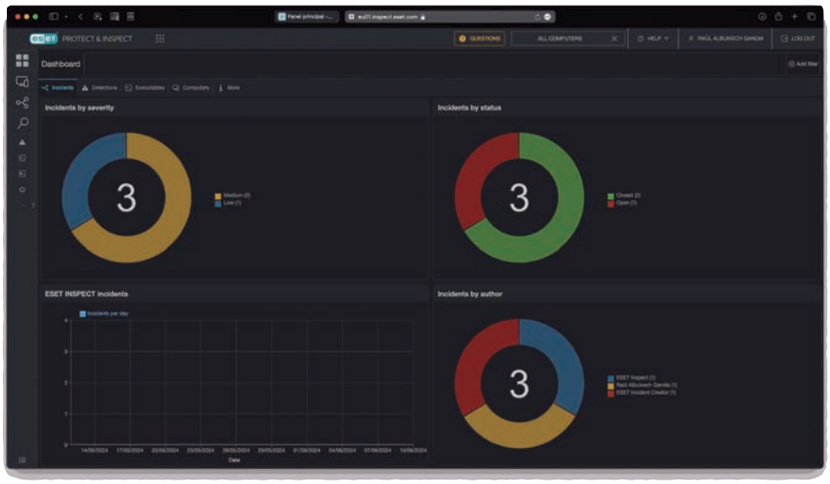
Tortosa añadía que "basándonos en nuestra herramienta centralizada de gestión ESET Protect estamos trabajando en ofrecer a todos nuestros clientes una gestión especializada de nuestro XDR, este Manage Detection and Response posibilita a las organizaciones acceder no solo a nuestra tecnología, sino también a nuestro talento, ahora que resulta cada vez más complicado poder disponer de él." ESET España lanzaba a principios de 2024 un nuevo programa de canal, que incorporaba mejoras en la relación con su amplio canal de distribución construido durante más de 20 años, distribuyendo las soluciones desarrolladas por ESET, e incorporando a nuevos partners que contribuyen a conseguir las cifras de negocio marcadas como objetivo para este año. Tortosa subrayaba que "en ese sentido estamos creciendo en compañías que han visto la necesidad de incorporar la ciberseguridad como nueva línea de negocio y aportando su experiencia en el sector tecnológico".

Este programa de canal mantiene la esencia de aquellas ventajas competitivas que ya ESET España desarrollaba anteriormente, una apuesta 100% por el canal de distribución, la fidelización del cliente, los altos márgenes comerciales o el apoyo técnico por nuestra parte. Pero también han añadido características que son muy valoradas por cualquiera de sus partners, como la estratificación en diferentes niveles que confieren ventajas a aquellos que más apuestan por la marca ESET, o la creación de planes de negocio personalizados donde se aporta experiencia y conocimiento del sector.

Todo ello sin dejar de lado aquellos aspectos que refuerzan la positiva valoración que los clientes hacen de la marca ESET, apostando por un soporte técnico de confianza, accesible y con un alto nivel de compromiso para dar respuesta a cualquier incidencia surgida a cualquier de sus miles de clientes.

Además, finalizaba Carlos Tortosa asegurando que "seguimos trabajando activamente con la incorporación de aquellos partners que gestionan la seguridad de sus clientes en formato MSSP, facilitando herramientas de gestión como ESET Protect de fácil manejo e interconectada con el ecosistema ESET de generación y gestión de licencias. Actualmente la ciberseguridad no puede entenderse sin la intervención de profesionales conocedores de los riesgos a los que nos enfrentamos, pero también de las tecnologías con las que contamos para defendernos."

Carlos Tortosa,
Director de Grandes Cuentas de ESET España.



que esté acometiendo un partner mediante una oferta privada a través de estas plataformas pueda ser adquirido por el cliente final directamente en estos marketplace, pero nosotros mantenemos al partner implicado la recompensa correspondiente por su esfuerzo y el canon por el valor añadido. Es un nuevo modelo de funcionamiento que creo que tiene mucho sentido en un entorno donde vemos cómo cada vez más la oferta de soluciones TI empiezan a funcionar dentro de estos grandes marketplace y en los que llevamos ya años integrando nuestras soluciones de forma nativa y que pueden ser directamente adquiridas, facturadas y gestionadas.

ESET: Teniendo en cuenta que ESET en España llega desde una pequeña empresa de informática fundada en 1992, la política de venta ha estado siempre basada en el canal de distribución, es decir, nuestra evolución ha sido la lógica, partiendo de la base de conocer bien lo que se supone estar al otro lado del fabricante como partner. Por lo tanto, llevamos ya 30 años apoyando a todos nuestros partners de la mejor forma posible, y precisamente este año lo que lanzamos es una actualización de nuestro programa de canal, que pone en marcha diferentes niveles de partner y además intentamos mejorar el beneficio económico en relación al perfil del partner, los servicios dados, el tipo de cliente, etc. Esto nos está ayudando a consolidar esta buena relación con nuestro canal de distribución, con partners que llevan trabajando con nosotros más de 20 años y también ayudando a contratar con nuevos partners.

Además, dentro de este programa realizamos la gestión de formato MSP, MSSP y en todos estos niveles existe siempre la posibilidad de utilizar nuestros servicios, nuestros técnicos y evidentemente dar soporte a todos nuestros clientes, que creemos que un valor diferencial. El referente es llegar a ser un fabricante a nivel global y 100% europeo, pero a nivel local consideramos que nuestra relación es muy buena con toda la distribución y aportamos ese valor adicional que puede dar el factor humano.

«Hace años podría plantearse si invertir en ciberseguridad o no; hoy el que no invierta va a estar más temprano que tarde fuera del mercado. La opción de poder contar con un CISO as a Service es algo que el canal ha entendido, no todas las empresas pueden permitirse tener un CISO en plantilla, y la labor de los fabricantes es dar todas las herramientas necesarias para llevar a cabo su trabajo» (Miguel López, Barracuda)

Ya habéis mencionado que todos tenéis ya integradas las modalidades de gestión de servicios como MSP, pero ¿llegaremos al punto de tener un CISO as a Service, sobre todo para empresas pequeñas que no pueden disponer no ya de un departamento específico, ni siquiera de una persona ocupada en la ciberseguridad?

Bitdefender: Para mí la respuesta es un sí rotundo. De hecho, la mayor parte de nuestros partners están ofreciendo ya ese servicio. Cualquier empresa, por pequeña que sea, tiene que tener una figura o alguien que se responsabilice de la ciberseguridad. Para su tranquilidad, cada vez es más sencillo proveerse de este servicio. Un poco por eso, por la unificación de plataformas, por la simplicidad de su uso, por el expertise que hay en nuestros partners y sobre todo por las necesidades que hay en el mercado. O sea, cualquier empresa, por pequeña que sea, no puede estar sin tener en cuenta una planificación que haga a uno, dos, tres, cuatro o cinco años, qué es lo que va a pasar con sus herramientas informáticas, con su tecnología, y sobre todo cómo va a proteger uno de los bienes más más importantes que tienen, que son los datos de sus clientes. Y eso se llama CISO virtual, se llama servicios de ciberseguridad que pueden proveer cualquiera de los partners especialistas en seguridad, solo hay que servirlos de una forma sencilla encima de la mesa de los clientes.

Fortinet: Nosotros de hecho desde hace un par de años hemos sacado un servicio que se llama SOC as a Service, donde la idea para nada es saltarnos los servicios y el valor que aporta nuestro canal, sino ayudar un poco a una evolución donde la gran mayoría de nuestros partners que todavía a día de hoy no tienen montados servicios de SOC o de asesoramiento cibernético, o lo que estáis llamando CISO as a Service, pues poder ayudarles en esta andadura. La aceptación es buenísima y al final lo que hacemos es que se apoyen en un equipo experto capaz de nutrirse de toda la parte de telemetría que obtienen de la base instalada y aportar directamente recomendaciones, informar de cualquier cosa que se detecta, nuevas amenazas y demás. Y esto al final lo hacemos a través del partner, es decir, el partner puede decir revenderlo y que el cliente interactúe directamente con nosotros, actuando de puente entre estos servicios y el cliente final para aportar después también su valor de intermediación, por supuesto, temas de idioma, cercanía y demás, e incluso para que evolucione sus servicios. Y está siendo un gran éxito.

Barracuda: Yo creo que es una evolución bastante natural de todo lo que hemos venido hablando. Al final el peso específico que la ciberseguridad tiene dentro del departamento de TI, y en general de las necesidades operativas de cualquier empresa del tamaño que sea, hoy día es cada vez mayor. Hace años podría plantearse si era una opción invertir en ciberseguridad o no; a día de hoy creo que todo el

Miguel López,
Regional Sales Director Iberia de Barracuda.

mundo entiende que el que no invierte en ciberseguridad va a estar más temprano que tarde fuera del mercado. La opción de poder contar con un CISO as a Service es algo que el canal ha entendido desde hace mucho tiempo y que ya está ofertando creo que con muy buen criterio. Y para ello, realmente una de las cosas que estamos haciendo desde el punto de vista de los fabricantes es diseñar las herramientas que pueda necesitar, como SOC as a Service, la posibilidad de tener un DDR o un XDR como servicios gestionados, de que puedan coger lo que necesiten para apoyar estas estrategias de CISO as a service.

Es un signo más de que los tiempos están cambiando, que realmente las empresas entienden esa necesidad. Pero como no todas pueden permitirse tener un CISO propio en plantilla, precisamente para cubrir ese gap se plantea esta figura que yo creo que es muy interesante, y la labor de los fabricantes es dar a esos CISO as a Service todas las herramientas necesarias para ser capaz de llevar a cabo su trabajo.

ESET: Completamente de acuerdo con todos. Hay que tener en cuenta una variable que vamos, que todos tenemos asumido, y es que cada vez resulta más difícil encontrar talento dentro del mundo de ciberseguridad. Nos cuesta a nosotros que somos fabricantes o que somos incluso mayoristas o el propio partner, pero imagínate un cliente final o una pyme encontrar a la persona que pueda cubrirlo de una manera profesional. Por lo tanto, tiene mucho sentido que nuestros propios partners se conviertan en ese proveedor externo de un perfil como puede ser un CISO, para poder gestionar la seguridad interna no únicamente de una empresa, sino de varias, y gestionarlas utilizando nuestras herramientas y nuestras diferentes plataformas de gestión. La ley permite tener un director de seguridad de la información externo, y el cliente final puede optimizar muchísimo mejor sus costes, teniendo en cuenta que con un único proveedor tiene no solo cubierta la parte de herramientas, sino también la parte gestión, que al final le va a resultar mucho más cómodo tener un interlocutor que le facilite el servicio y va a ser mucho más resolutivo.

Bitdefender nombrado Líder en las evaluaciones de The Forrester Wave sobre seguridad de endpoints

La solución de seguridad empresarial de Bitdefender sigue recibiendo los principales reconocimientos de instituciones independientes. En esta ocasión, **Forrester ha otorgado a Bitdefender** la posición de Líder en The **Forrester Wave™ sobre seguridad de endpoints del 4.° trimestre de 2023**. Los resultados de esta evaluación nos recuerdan que Bitdefender sigue especialmente centrado en ofrecer soluciones y servicios de seguridad informática del máximo nivel a organizaciones de cualquier tamaño.

Metodología de evaluación

Para establecer su clasificación, Forrester evaluó 25 criterios que cubrían el más amplio espectro, desde los detalles técnicos de las ofertas actuales de cada proveedor hasta su estrategia y la presencia en el mercado. La evaluación se centró principalmente en la capacidad de los proveedores para ofrecer resultados sólidos en prevención de endpoints. Forrester destacó que contar con una sólida prevención permite a los analistas de seguridad centrarse en investigar cómo han conseguido las amenazas franquear otras líneas de defensa, en vez de dedicar sus esfuerzos a la reparación.

Visión estratégica en un sector en permanente evolución

En la evaluación, Bitdefender fue clasificado como Líder. Ahondando en los detalles de la evaluación, los lectores podrán observar que Bitdefender recibió las mayores puntuaciones posibles en diez criterios, entre los que se encuentran la prevención de malware y la reparación de parches. En nuestra opinión, se trata de puntuaciones que reflejan una filosofía integrada y holística de la seguridad de endpoints.

En el informe, Forrester reconoce que "Bitdefender se diferencia por su filosofía nítidamente enfocada hacia la prevención". El documento destaca nuestras muchas funciones de control de los endpoints, nuestra sólida capacidad en diferentes sistemas operativos, incluida la defensa contra amenazas móviles, y nuestras características integradas de administración de parches y vulnerabilidades. Forrester también señala que Bitdefender brinda uno de los sistemas de precios más flexibles y los clientes de referencia pusieron de relieve el excelente servicio personalizado.

Bitdefender recibió las mayores puntuaciones posibles en los criterios de Prevención de malware, Prevención de exploits, Protección contra robo de identidad, Detección de amenazas de red, Reparación de ataques, Reparación de vulnerabilidades y Reparación de parches. Creemos que estas puntuaciones hablan de la calidad y la solidez de nuestras soluciones consolidadas.

En la categoría de estrategia, Bitdefender recibió las puntuaciones más altas posibles en los criterios de innovación, adopción y flexibilidad de precios y transparencia. Los resultados subrayan nuestra dedicación a ofrecer soluciones sólidas, fáciles de usar y rentables que se adaptan a las empresas de hoy en día.

Forrester también mencionó nuestras importantes inversiones en investigación y desarrollo. Dichas inversiones, lideradas por el **equipo de los laboratorios de Bitdefender**, nos permiten innovar con tecnologías propias como la **mitigación de ransomware a prueba de manipulaciones** y la **Integrity Monitoring** en todo el sistema.

Más que mera prevención

Más allá de las funcionalidades de primer nivel de Bitdefender en cuanto a prevención, con **GravityZone** ofrecemos una transición fluida hacia la **EDR o XDR**, de vital importancia en una era de amenazas digitales sofisticadas con frecuentes ataques de ransomware, filtración de datos y phishing. Con Bitdefender GravityZone, las organizaciones de cualquier tamaño pueden adoptar fácilmente la XDR y disfrutar de una protección integral en diversas fuentes de datos de seguridad. GravityZone XDR amplía su alcance para proteger sistemas, aplicaciones de productividad, cargas de trabajo en la nube, identidad e infraestructuras de red. Consolida los mecanismos de defensa y aporta una filosofía integral que garantiza la monitorización constante, rápida detección de las amenazas y una respuesta optimizada ante los ataques informáticos. Las soluciones de Bitdefender contribuyen a fomentar un entorno en el que las empresas puedan desarrollar sus actividades con confianza y agilidad.

Bitdefender®

www.bitdefender.es

En esta línea me imagino que los cambios legislativos también están ayudando a por lo menos que en ciertos consejos de administración se sienta la preocupación de incurrir en multas... O sea, no sólo el RGPD que ya lleva unos años, sino la nueva directiva NIS2, que ayudará a vender más ciberseguridad o por lo menos a que quien tiene que decidir y firmar el cheque esté más más de acuerdo...

Bitdefender: Como todo, al final la normativa y las leyes, aunque lentas y por detrás de por dónde va la tendencia, nos ayudan. Sin embargo, sigo diciendo que la normativa no es la que nos tiene que sustentar en el negocio, sino las necesidades que tiene el mercado. Con NIS2 está todo el mundo viendo a ver a quién le atañe, cómo va a cumplir, cómo va a hacer ese compliance de una forma segura y sencilla. Y el efecto DORA, cuando venga, pues también ayudará. Pero al final sigo diciendo lo mismo, cuando llegas a un comité de dirección, la reglamentación es muy importante, pero la continuidad de negocio lo es mucho más y ahí es donde yo creo que el cambio de conciencia nos está ayudando a que sea un negocio que siga saludable y siga creciendo a unos ratios bastante dignos y donde vemos que cada vez hay más fabricantes, más soluciones y más más herramientas.

Entonces, lo que estamos haciendo es cómo simplificarle la vida a las empresas, cómo poder pasar en un mismo dashboard de compliance esa NIS2, esa ISO-27000, esa DORA, esa GDPR. Y así minimizar el esfuerzo que tienen que hacer no solamente de implementación de soluciones, sino de justificación y de poder mostrar evidencias para cuando vengan los auditores. Se agradece que la legislación y las normas estén aquí, pero yo sigo inclinándome a que nuestra labor es mucho más de concienciación.

Fortinet: No puedo estar más de acuerdo. Hace relativamente poquitos años, cuando cualquiera nos preguntaba 'a qué nos dedicamos', y decíamos 'a ciberseguridad', pues esto era el gran desconocido: 'ah, los hackers de la serie Mr. Robot', y parece que han pasado años luz. Y ahora, que cada dos por tres salen noticias de ataques en los telediarios, da igual el ámbito, ya sea público o privado, pequeña o gran empresa, esto está al orden del día. Entonces, al final, en ese comité de dirección, cuando estamos llevando a cabo una transformación digital del negocio, pues ya a nadie se le escapa el que la ciberseguridad es una pieza clave. Y si a esto le sumamos la parte legislativa a nivel país, a nivel continente, pues nos hacen reflexionar, pues ya no estamos hablando de las tradicionales infraestructuras críticas, sino que con NIS2 y DORA ahora concierne a empresas que no se veían antes como estuvieran dando un servicio crítico, y que tras la pandemia se ha tenido que replantear hasta qué punto puede tener impacto un ataque cibernético que le pare su servicio, ya no solo a nivel imagen de marca, beneficios o rendimiento empresarial, sino también de cara a sus usuarios. Hoy esa concienciación está presente en los equipos directivos y consejos de dirección, con lo cual sin duda también es una palanca que nos está ayudando el que venga este tipo de normativas.

Barracuda: Sí, sí, completamente de acuerdo. Me gusta hacer la comparación porque creo que se ve se sencillo: en todos los coches que conducimos hoy es obligatorio por ley que lleven cinturón de seguridad; sin embargo, y por desgracia, sigue habiendo accidentes donde la gente no los lleva puestos. ¿Cuál es la solución? Pues poner multas para que la gente se vea obligada a usar esas medidas que son necesarias. ¿No es muy distinto el ámbito de la ciberseguridad esto? No, al final la legislación tiene que existir y yo creo que se están haciendo avances muy importantes y bueno, es en la buena dirección por qué es necesario que exista todo ese ámbito, todo ese marco legal que impulse la ciberseguridad en el camino correcto. Pero no es suficiente con eso, tiene que existir además de ese marco regulatorio, debe existir unas fuerzas del orden público, como sucede en el ámbito de la DGT, que además obliguen al cumplimiento de esas normas, y pongan las multas. Y eso es un poco quizá lo que todavía tenemos que empujar más para asegurarnos que realmente el cumplimiento de la normativa es el que debiera ser. Una de las cosas que estamos haciendo diversos fabricantes es precisamente desarrollar herramientas con el marco normativo en mente, es decir, herramientas que faciliten, la adopción, que den visibilidad de cuál es el grado de cumplimiento y poder tomar medidas correctoras de forma sencilla.

ESET: Desgraciadamente tenemos que recurrir a este tipo de herramientas. Es decir, en un mundo ideal tendremos que ser todos conscientes de los riesgos que corremos y no tener que vernos obligados por medio del temor a la ley. Pero bueno, nos va a ayudar evidentemente a todos, y no es una cuestión de que nos ayude a nosotros precisamente a mejorar negocio, yo creo que se trata de herramientas que sirven para proteger mejor a nuestros clientes en general, y por ende, al ecosistema económico dentro del mercado nacional.

También es verdad, que partimos de la ventaja de que la situación de la ciberseguridad en el mercado nacional es mejor que en muchos otros países de Europa, porque se ha invertido en ello y porque de cierta forma, y ahí sí que rompo una lanza en favor de nosotros cuatro, creo que los fabricantes lo hemos hecho bien. No nos hemos dedicado únicamente a machacar al canal de distribución con nuestra oferta, también hemos intentado concienciar al usuario final, al cliente, al empresario, de que una protección era necesaria si no quería ver en riesgo su negocio o sus datos. Por esa parte la normativa nos va a ayudar, evidentemente, pero yo creo que nosotros ya hemos adelantado muchísimo y España se está moviendo de manera avanzada con respecto a otros países de nuestro entorno.

En esta línea igual también se pueden encontrar nuevos nichos de partners de canal a través de asesorías legales, bufetes de abogados, incluso agencias de seguros para seguir vendiendo ciberseguridad. No sé si vosotros estáis explorando estos segmentos también.

Bitdefender: Cada vez más hay partners muy focalizados donde el discurso de ciberseguridad empieza con un discurso de compliance. Siempre han estado ahí los consultores y los bufetes de abogados profesionales para poder asesorar ese cumplimiento, y tienen cada vez más en cuenta el tema de ciberseguridad, no solamente por la gestión del dato, algo en lo que han sido muy prolíferos. Entonces ciertos partners que antes estaban muy circunscritos a la parte legal, sí que se están moviendo hacia soluciones tecnológicas a la hora de aconsejar a sus clientes e implementarlas para asegurarse el cumplir con la norma.

Ese es el primer punto. Y el segundo punto es el tema del ciberseguro, que cada vez se está viendo más en el mercado, y cómo esos ciberseguros están exigiendo ese compliance o esas soluciones implementadas dentro de la empresa a la hora de poder cubrir los riesgos de un ciberataque, y que además las primas no sean impagables. Así, mientras cumplas con ciertos requisitos y tengas soluciones del tipo EDR, firewalls y similares, pues se va reduciendo esa prima. Muchas empresas ya están explorando esta vía para garantizarse una cobertura. Y por supuesto, los partners evolucionan en función a la demanda que hay en el mercado y se nos acercan algunos perfiles que antes ni siquiera podías contemplar dentro de tu ecosistema y ahora se están metiendo en adoptar o implementar o en recomendar ciertas soluciones de ciberseguridad.

Fortinet: Tenemos partners que cada vez más se están apoyando en este tipo de, digamos, palancas para ir con un mensaje de 'oye, ¿te estás planteando esto?, la normativa va por aquí, vamos a analizar hasta qué punto esto te puede impactar'. Se trata de no sólo cumplir, sino que tu negocio, la continuidad de tu negocio y tu exposición a ese riesgo esté más controlado. Hemos tenido colaboraciones también con distintas compañías de seguros que se han puesto en contacto con nosotros un poco para pedir recomendación, dado que ellos no tienen ese expertise, sobre cuáles son las soluciones digamos básicas para entender realmente la forma de montar un seguro y cómo deben ir las primas. Luego esto nos ha hecho tener cierto conocimiento en este ámbito y con estas compañías, y sigue existiendo un feedback. Pero es un tema muy complejo, porque al final sabemos que cumpliendo determinados mínimos de seguridad, pues las empresas van a estar ciertamente hasta un nivel protegidas, y esto pues debería corresponder a una prima dada.

Pero también sabemos que la seguridad 100% es muy muy complicada de alcanzar si no imposible, y esto hace que los seguros también tengan un riesgo tremendo. Tenemos un caso particular, en la vertical de industria y OT, donde sí que el canal está especializado y además como sí que trabaja y está acostumbrado a apoyarse en normativas específicas de este ámbito, pues están trabajando y apoyándose en estas normativas de cara a proponer la forma de cumplir, y no sólo cumplir, mejorar tu postura de seguridad. Este ámbito de clientes, que por la peculiaridad e idiosincrasia de su

Bitdefender Global Leader In Cybersecurity

¡Detenga más ransomware y ciberataques avanzados!

Automatice, simplifique y centralice la seguridad en: endpoints, redes, nubes, identidades y aplicaciones de productividad.

Bitdefender ha sido nombrado líder en
The Forrester Wave™: Endpoint Security, Q4 2023

FORRESTER®
WAVE LEADER 2023
Endpoint Security

Leer más:

Trusted. Always.

↳ bitdefender.es

sector, siguen trabajando con sistemas operativos o hardware que están tremendamente obsoletos y sabemos que son muy vulnerables, y esto sí que es un poco caso de éxito que está funcionando muy bien en nuestro caso.

Barracuda: Coincido con todo lo mencionado, la verdad es que todo este ámbito regulatorio tiene cada vez mayor peso. Hablando específicamente de los ciberseguros, la verdad es que cada vez vemos más partners interesados en aportar a los clientes soluciones relacionadas o complementarias a los ciberseguros, precisamente porque el mercado las demanda y eso es un signo de madurez. Es correcto pensar en una estrategia de ciberseguridad donde el ciberseguro es otro elemento más, pero es un error que vemos en ocasiones en partners, incluso clientes, que ven en el ciberseguro una especie de forma de ahorrarse la parte de ciberseguridad: es decir, si yo tengo una buena póliza que me cubra ante eventuales ataques, brechas, etc., pues en un momento dado puedo coger y a lo mejor invertir menos en la postura de ciberseguridad.

Este planteamiento es un error de concepto y probablemente en muchas ocasiones de falta de información, porque realmente la póliza de ciberseguro va a valorar el grado de madurez, el grado de implementación de ciertos elementos y planes de contingencia. De manera que si no los tenemos correctamente implementados, la póliza probablemente va a ser más dolorosa. Y de hecho, si no están esas medidas implementadas, podríamos encontrarnos con que la letra pequeña de la póliza no hiciera frente a la cobertura de ese riesgo. De manera que es importante pensar que los ciberseguros son elementos complementarios y parte de una estrategia de ciberseguridad integral donde son un elemento más, no son un sustituto de las auditorías, y donde si estamos llevando a cabo una estrategia de ciberseguridad correcta, precisamente vamos a abaratar los costes de esa ciberpoliza.

Sin embargo, hay un dato que tenemos comprobado, y es que en ciertas ocasiones, y sobre todo específicamente en ataques de ransomware, aquellas compañías que tenían una póliza de ciberseguro, estadísticamente tienen una probabilidad más elevada de ser atacadas una segunda o tercera vez que aquellas que no tenían una póliza. ¿Por qué sucede esto? Pues la interpretación que se hace es precisamente porque el pago frente al ataque de ransomware se ha realizado utilizando esta póliza de forma muy inmediata o sin poner problemas. Y claro, el hecho de tener un cliente, entre comillas, desde el punto de vista de los atacantes, que paga con facilidad, le hace más susceptible a nuevos ataques. De manera que tenemos que ser cautos a la hora de cómo manejamos este tipo de cuestiones.

Una póliza de ciberriesgos, insisto, es una parte más de tu estrategia de seguridad, pero no una sustitución en ningún caso. Análogamente, si tenemos una póliza de ciberriesgo pero no nos hemos dotado de las medidas de ciberseguridad correctas o no hemos sido del todo honestos a la hora de identificarlas cuando hemos firmado la póliza, probablemente la compañía de seguros puede decir que no se hace cargo y entonces tendríamos un doble problema.

«La tendencia a futuro es la orquestación, tanto de servicio por parte del partner como de la herramienta que nosotros facilitamos para que esa protección sea la máxima posible. Hay otra pata que es el acceso a la inteligencia colectiva para intercambio de información para extender esa protección porque lo que no he visto yo igual lo ha visto algún otro» (Carlos Tortosa, ESET)

Carlos Tortosa,
Key Account Director de ESET España.

ESET: Precisamente en un foro esta semana comentábamos que aproximadamente el 33% de aquellas empresas que han sufrido un ataque y han pagado el rescate, después han acabado sufriendo un segundo. Sí que es verdad que el hecho de abonar una cantidad para la recuperación de la información, primero no te garantiza dicha recuperación y segundo, posiblemente seas después un nuevo objetivo.

Volviendo un poco a la pregunta inicial, llevamos muchísimo tiempo detectando que hay una gran diversificación en cuanto al canal de distribución con respecto a aquellos partners que no son específicamente empresas dedicadas al TI, pero que sí que ven la necesidad de poder facilitar a sus clientes una serie de herramientas que ayuden al cumplimiento. Tenemos varias que han decidido ampliar sus líneas de negocio, directamente con nuevos colaboradores no estrictamente TI, porque lo ven bastante complementario. Estoy hablando de, por ejemplo, el tema de seguros, el tema de compliance. Y nos va a ayudar el hecho de tener a nivel interno proveedores de servicios o proveedores de herramientas de los fabricantes para ayudar a la hora de contactar con clientes o fidelizar a clientes, facilitarles una pata más de negocio que puede ser de gran provecho.

Respecto al ciberriesgo, cuando contratamos este tipo de solución o de herramienta o de servicio mejor dicho, tenemos que tener claro a qué nos va a obligar su contratación, cuáles son los parámetros que tenemos que evidenciar que estamos utilizando para que después realmente el servicio nos resulte de utilidad. No nos va a proteger absolutamente de todo, y no tiene que ser un respaldo que nosotros demos por bueno: centrémonos primero en cubrir nuestras necesidades de ciberseguridad y en caso necesario contratemos un servicio de este tipo, pero teniendo en cuenta antes que la primera parte tiene que estar cubierta 100% y con la máxima optimización posible.

ADELANTARSE AL FUTURO

¿Qué se viene en el 2025, qué tendencias o qué tecnologías creéis que van a emerger o se van a consolidar o que hay que tener ya sí o sí en el portfolio?

Bitdefender: Fundamental todo lo que es la parte de cloud security posture. Muchas veces para los responsables de seguridad se trata de un terreno desconocido, no saben ni lo que tienen ahí, para nosotros es esencial dar esa visibilidad y desplegar correctamente esa infraestructura que estamos poniendo en cualquier tipo de cloud tanto privada como o las públicas, pero todo cloud tampoco va a ser, tenemos que vivir en esos entornos híbridos. Por lo tanto las herramientas deben tener en cuenta que no solamente protegemos un entorno on-premise o un entorno cloud sino que tienen que ser plataformas abiertas que nos permitan proteger cualquier tipo de infraestructura independientemente de donde esté hoy y dónde vaya a estar mañana. Por ejemplo, todo el tema de contenedores y de microservicios están teniendo una expansión muy importante.

Pero la falta de expertos, la necesidad de cubrir ese 24x7, la capacidad de poder tener esa supervisión de incidencias y de alertas por un SOC apoyado por el MDR de los fabricantes, es otro de los puntos fundamentales que vamos a ver cada vez más en el mercado, está creciendo de forma brutal. Pero no cualquier SOC, sino SOCs cada vez más más profesionales con un expertise que nos permita monitorizar y poder ver y reaccionar en el segundo cero para minimizar el impacto de cualquier brecha. La parte del XDR como extensión del EDR al network, a la cloud, a

la identidad ya está suficientemente maduro y la parte de estos servicios de MDR nos ayudará a poder asimilar cualquier tipo de tecnología de una forma mucho más sencilla y mucho más rápida, no necesita confeccionar algo ad hoc para un cliente, sino que son soluciones que ya están en el mercado y pueden implementarse.

Fortinet: Comentábamos la parte de seguridad en la cloud, la parte de confianza cero, el tema de la IA, salen conceptos como MDR, XDR, SASE… la ciberseguridad no hace sino expandirse, pero la realidad es que cada vez los ataques son más complejos y elaborados. Al final yo creo que más que una solución es tener un acercamiento de plataforma, donde aúnes distintas herramientas que cubran los distintos vectores de ataque de una forma muy sencilla, con un single pane of glass como una única consola central de gestión SPOG donde puedas ver qué es lo que está ocurriendo, donde puedas lanzar automatismos y que simplifique al final la vida al usuario final, al cliente.

Casi todas las soluciones que hemos mencionado están más orientadas a la parte de detección temprana y poder reaccionar, pero quizás el futuro también vaya por soluciones tipo vigilancia digital. Basándonos en un análisis de vulnerabilidades y Threat Hunting, ver cómo se están moviendo los ataques y qué es lo que se está cociendo en esas redes digamos dominadas por los malos, 'oye, que se están comprando dominios de tu empresa, están apareciendo aplicativos parecidos a los tuyos', y poder anticiparnos, avisando y previniendo a nuestros clientes.

Barracuda: Lo mejor que podemos hacer para apoyar a nuestros clientes y partners es hacer foco en la necesidad de simplicidad. En muchas ocasiones están apabullados por la sopa de letras y la siguiente tecnología disruptiva que van a ser el santo grial de la ciberseguridad y al final pues cada una de estas tecnologías rompedoras es desplazada pocos años después por otra aún más rompedora. Pero la ciberseguridad no es un proyecto que se termine, es un proceso en el que vamos avanzando, nunca va a estar acabada, y esta evolución creo que es crítica abordarlo desde el punto de vista de la simplicidad, porque de lo contrario nos vamos a encontrar con un montón de agentes y consolas y ya podemos tener la mejor herramienta del mercado que si está mal configurada no va a servir para nada. Y además que sea asequible, y no me refiero sólo desde el punto de vista económico sino desde el punto de vista técnico y funcional. Es necesario que como fabricantes nos enfoquemos a hacer soluciones que sean cada vez más sencillas, más amplias, que tengan la capacidad de cubrir la mayor cantidad posible de vectores y hacerlo de la forma más simple posible. Pero también tenemos que avanzar al mismo paso, debemos de adaptarnos a un mundo muy cambiante donde las ciberamenazas crecen y evolucionan de forma muy rápida.

ESET: Yo soy incapaz de visionar qué nueva tecnología o que nuevas siglas van a servir para complicar un poco más el mercado en 2025. La tendencia en todo caso a futuro tiene que ser un poco más de orquestación, tanto de servicio por parte del partner como de la herramienta que nosotros facilitamos para que esa protección sea la máxima posible. Hay otra pata que es el acceso a la inteligencia, es decir, no únicamente que los usuarios finales tengan acceso a una herramienta concreta sino que también los propios fabricantes generemos una serie de inteligencia colectiva que tendremos que intentar democratizar para llegar al punto de intercambio de información, lo cual sería interesantísimo para el mercado para extender esa protección máxima posible, y lo que yo no he visto yo igual lo ha visto algún otro proveedor.

Nosotros intentamos también facilitar un formato o servicio para que se gestione en SOCs o en herramientas de monitorización de cada cliente final. Tenemos que proteger el objetivo del cliente hasta cierto punto de manera personalizada, independientemente del resto de soluciones, herramientas que facilitemos de manera más general, pero hay clientes que son evidentemente más objetivo para los malos que otros.

Y por terminar, en este panorama futuro, ¿veis que vaya a haber consolidación de empresas, va a haber movimientos de grandes adquisiciones y no sólo entre fabricantes sino a lo mejor también entre partners que se vayan juntando para ser más grandes y tener otras economías de escala más más poderosas?

Bitdefender: Lo estamos viendo, esa es la tendencia del mercado. Mercados maduros te llevan a que las empresas cada día sean más grandes para poder aglutinar más cosas, dar servicios integrales que comprendan todo, de simplificar una plataforma, de simplificar un servicio. Esto no podemos hacerlo con diez empresas distintas, sino que al final cuantas menos intervengan pues mejor puede estar el sistema monitorizado, seguido y controlado.

Pero yo no hablaría de consolidación porque eso significa que cada vez vamos a ser menos, llevamos muchos años aquí diciendo que se van a comprar y fusionar estas, o que aquella va a desaparecer, y la realidad es que cada vez somos más fabricantes, hay más soluciones, hay más necesidades de ciberseguridad y esta necesidad requiere de grandes empresas que puedan abordar grandes proyectos y lo tengan todo. Por supuesto que van a aparecer empresas nuevas y por supuesto que va a haber ese tipo de movimientos entre fabricantes, es un sector muy dinámico que está creciendo mucho y necesita alimentar sus LinkedIn de noticias.

Fortinet: Pues es que es el día a día, ¿no? Todas las semanas tenemos alguna noticia de determinado fabricante compra otro fabricante, otra tecnología que va reforzando un poco su portfolio. En alguna encuesta ya se está viendo, los clientes lo ven como una necesidad el tema de ir consolidando soluciones para poder simplificar y poder abordar la ciberseguridad. Yo tampoco tengo la bola de cristal, no sé qué siglas van a aparecer, pero seguro que va a ser así. Habrá nuevos frentes de amenaza y surgirán soluciones para cubrir esos nuevos vectores. Lo que tenemos que hacer entre todos es intentar simplificar, y el intercambiar información y la parte de indicadores de compromiso IOCs en foros como el Cyber Threat Alliance. Va a ir habiendo consolidaciones, compras, pero bueno pues ahí tenemos que estar intentando dar una solución que simplifique todo esto, toda esta complejidad lo máximo posible, tanto a partners como a clientes finales.

Barracuda: Lo que estamos viendo es un proceso en el que se están juntando dos tendencias. Por un lado sí que es cierto que todos los días desayunamos con la noticia de una empresa adquirida con otra y demás, con lo cual parecería pensar que hay un proceso de consolidación, pero a continuación sigue otra noticia que dice que ha surgido una nueva compañía. Es un mercado en expansión, y las empresas existentes pues van cada vez haciéndose más grandes, al menos aquellas que vamos sobreviviendo, porque ya sabéis que este mercado pues efectivamente es muy exigente y no todos lo logran. A lo largo de los 20 años que llevamos en esto hemos visto crearse y desaparecer muchas empresas y otras ser absorbidas y vamos a seguir viéndolo.

Es bueno que sea así de dinámico porque estas nuevas empresas aportan savia nueva al mercado, nuevas ideas, y más competencia, que yo creo que es muy interesante. Seguiremos viviendo este proceso de consolidación porque efectivamente al final el grado de especialización y profesionalización requiere de compañías potentes que puedan hacer las inversiones necesarias para hacer frente a desafíos como la inteligencia artificial y el machine learning.

ESET: Veo también dos tendencias completamente diferentes en el mercado. Se están adquiriendo empresas por parte de grupos de inversores, no están comprando marcas sino tecnologías que quieren incorporar a su portfolio. Hay una gran cantidad de empresas muy de nicho que están sacando soluciones, que gestionan muy bien su imagen y su merchandising, haciendo clientes cuando realmente detrás no hay tanto como se dice. Creo que la consolidación va a ser complicada mientras exista esta segunda parte. En la primera es evidentemente aglutinar a empresas bajo un único paraguas, pero existe una consideración no tanto de ofrecimiento de tecnología sino de servicios que al final gestionan tecnología. Por otro lado, esa agrupación de pequeños partners que se está haciendo por parte de marcas que todos conocemos, al fin así va a suponer una consolidación del ofrecimiento del servicio, no tanto la venta del producto.

MERCANZA

espacyo

El ERP analítico para tu empresa

Integra todas las funciones de tu organización en un único sistema de gestión empresarial **en la nube**

Espacyo recoge la experiencia de los más de **30** años en los que el equipo de desarrollo de **Mercanza** ha diseñado soluciones útiles para cubrir las necesidades de información del mundo de los negocios actual.

Sistema modular

adaptable a cualquier tipo de empresa

Intranet
Almacén
Ventas
Financiero
CRM
Artículos
Compras
Personal
Documentación
CAU
Calidad
Prevención
Proyectos
Escaparate
Producción
Activos Fijos
Marketing
Cuadro de Mando

canal de
distribución
+34 913 603 100
canal@mercanza.es

www.mercanza.es

Moisés Camarero (Compusof): «Quizás hoy sea mucho pedir llegar al 25% como el año pasado»

Compusof, partner de HP y HPE desde hace más de 40 años, presenta su nueva estrategia para generar valor entre sus clientes de iniciativas públicas y privadas con una decidida apuesta por la Inteligencia Artificial. El integrador ofrece a través de sus equipos profesionales un asesoramiento experto para que las organizaciones puedan aprovechar todo el potencial de esta nueva tecnología.

DE ESTA forma, Compusof apuesta por proporcionar a los responsables de TI una visión completa de técnicas de IA para solucionar problemas y lograr importantes incrementos de productividad. Según los últimos informes, los responsables de tecnología y sistemas de las organizaciones ven las posibilidades que ofrece la IA como un recurso para la evolución del negocio, si bien, en la práctica, tienen dificultados para su implementación debido a la escasez de formación entre sus profesionales. Por ello, Compusof ha decidido incluir en sus proyectos las pautas necesarias para orientar desde las fases más tempranas del proyecto y que los clientes puedan comprender y establecer sistemas de IA acordes a sus requerimientos y posibilidades, según sus capacidades de desarrollo.

"Hemos decidido dar este paso por la necesidad que observamos de asesorar y llevar información clara sobre Inteligencia Artificial hasta nuestros clientes de administración pública y privada", indica Moisés Camarero, CEO del Grupo Compusof. "Nuestros profesionales están capacitados para proporcionar la visión que necesitan a la hora de implementar la IA en sus organizaciones y así ayudarles a establecer estrategias que impulsen y beneficien a los clientes y usuarios".

Generar valor en los clientes

Los datos de las consultoras señalan que en los próximos cinco años las empresas y administraciones adoptarán técnicas para una aplicación de la IA más fiable, responsable y en consonancia con la sostenibilidad. Es por ello que se hace necesario potenciar herramientas y habilidades preparadas para la IA, identificar su apoyo para la mejora de las aplicaciones y crear un entorno preparado para su continua evolución. El CEO del Grupo Compusof nos detalló algunos de los aspectos más candentes en un encuentro ante medios:

Moisés Camarero, CEO del Grupo Compusof.

¿IA para todo y para todos?

Como el tema de este encuentro es la IA, me dije, voy a hacer la presentación con IA. Tenía dos caminos, preguntar a ChatGPT, o usar el Copilot de Microsoft, pero finalmente acudí a un amigo entendido en estos temas que me mostró algunas de las ventajas, y de los riesgos, que conlleva su uso. Hicimos una canción muy aparente que podría dar el pego, y hasta un algoritmo para jugar al Go y ganar, y no nos pusimos a descifrar todas las proteínas del genoma humano porque no teníamos tiempo. Pero por el contrario, todo ese contenido sintético hay que manejarlo de manera ética, hay un peligro evidente de poder influir en el pensamiento de las personas y sobre todo de engañar, además de temas sobre la propiedad intelectual que todavía no están muy claros.

Revolución, pero con cautela

Para lo que nos ocupa, lo más interesante son las aplicaciones de negocio que ya están funcionando. En HP nos mostraron un proyecto para generar contenido de marketing y tardando la mitad de tiempo. ¿Significa esto que si duplicamos la productividad del departamento deba pensar que necesito ahora la mitad de gente? Google advierte, y quizás de una manera muy cauta, que el 6% de los trabajos repetitivos serán sustituidos por IA, pero a cambio, solo en España, los incrementos de productividad generarán hasta 120.000 millones de euros. Puede que sea así: un despacho legal que usa la IA en su propia base de datos ha logrado multiplicar por cuatro la velocidad y reducir dos horas el tiempo de una consulta profesional, y estamos solo en el capítulo uno de la IA. Pero, ¿debería decirle al cliente que como te he ahorrado 125 minutos, no te los cobro?

Otro escenario: mayorista preocupado por la optimización de su cadena de valor logística en un entorno de alta incertidumbre geopolítica. ¿Cómo asegurarse el flujo de pedidos sin entrar en rotura de stocks? La IA le puede alertar de manera anticipada de la previsión de necesidades cruzando otros datos para ganar en resiliencia. Nosotros creamos en 2022 en Amazon un chatbot que al principio solo decía 'Hola' y te redirigía, y hoy ya resuelve el 60% de las incidencias.

En el colmo, se ha probado que dos IA se pongan a charlar entre ellas. Al principio puede parecer un poco diálogo de besugos, produciendo una tormenta de ideas, pero luego se van enseñando cosas y podemos tomar decisiones sobre qué look va a funcionar mejor o cual es el claim que mejor resume la campaña. Otro experimento, dentro de la Universidad de Standford (California): se ha creado un pueblo, Smallvillage, donde todos sus habitantes son artificiales, para ver cómo se desenvuelve.

All-in con Windows 11

Microsoft va a forzar a las empresas a la migración masiva de Windows 10 a Windows 11, principalmente porque la gestión de parches y actualizaciones es más rápida y segura, anunciando el fin del soporte en julio de 2025. De hecho, la migración a Windows 11

«Puedo reducir dos horas el tiempo de una consulta profesional. Pero, ¿debería decirle al cliente que como te he ahorrado 125 minutos, no te los cobro? O, si duplicamos la productividad del departamento, ¿significa que necesito ahora la mitad de gente?» (Moisés Camarero, Compusof)

va a ser relativamente rápida en el segundo semestre, sobre todo en las Administraciones Públicas. Además, si quieres IA, la licencia de un Copilot por equipo vale casi tanto como un Office, y requiere equipos preparados. HP ya tiene modelos con el nuevo procesador neuronal NPU que se suma al de cómputo CPU y al gráfico GPU. Permitirá equipos más rápidos y que gasten menos batería. En temas de servicio técnico también se mejora, puesto que se podrá predecir con mayor precisión los recambios que necesites.

Grandes cuentas ya empiezan a preguntar por equipos preparados para la IA en sus renovaciones del año que viene, aunque todavía no la piensen usar masivamente. La IA no se puede aplicar a todo lo que uno quiera, hay que tener antes modelos para crear valor. Pero una empresa no puede ir a la nube a crear modelos propios porque se los queda la nube, por lo que hay que hacerlos en local, y en eso están los nuevos equipos preparados para ejecutar IA.

Marcha del negocio de PC

Los mayoristas vienen quejándose de un primer semestre flojo, a un 65-80% de los objetivos en PC de sobremesa y portátiles. HP ya avisó que sería así, pero que se compensará con crecimientos en la parte final del año. Nosotros hemos aprovechado un par de oportunidades en Cataluña y en la CAM con más de mil ordenadores para Educación y si no hemos llegado al 100% de las expectativas, por suerte nos hemos quedado en el 90%, y queremos ser optimistas: el objetivo de al menos igualar lo del año pasado que crecimos un 25% quizás ya sea mucho. Los fondos europeos continuarán y el gasto de las AAPP no va a parar, además los concursos típicamente se preparan en el primer semestre y se ejecutan en el segundo.

Hay que diferenciar el Kit Digital, que son unos 3.000 millones de euros y solo para algunos epígrafes de la informática, y los fondos NextGen que son 145.000 millones y abarca también sostenibilidad. El problema es que no se ejecutan porque están mal explicados, aunque en informática van algo mejor. España está al 33% y no es de los peores, pero el que mejor lo lleva no llega al 70%. Aun así, seguimos sorprendidos que la gente siga invirtiendo desde la pandemia a un ritmo mayor al que crece el PIB dentro de la UE.

Por contra, el modelo DaaS solo está tirando en el mercado profesional en grandes y medianas compañías. Las AAPP no entran todavía en esto. Quizás falte aclarar quién es el que compra los equipos o tiene la titularidad, si el distribuidor, el fabricante o el Estado. En México, por ejemplo, el Gobierno ha lanzado un decreto donde se reserva la cláusula que puede suspender pagos si las circunstancias lo requiere, y no te debe nada. Aunque en general no nos podemos quejar de cómo vamos en este país, está habiendo una reconversión de las compañías buscando mayor productividad a través de más tecnología.

Expectativas del canal con Poly

Va muy bien. Sobre todo para salas de reuniones con IA embebida, que estaban en un canal muy específico AV Pro, y ahora podemos llegar a ser más de pyme y consumo; y a la vez, partners de ser muy especialistas a tener cuentas con grandes clientes. Quizás en dar un bundle con el ordenador no, pero hay proyectos específicos como el de PwC que se ha dado un buen auricular a todo el mundo.

Y es que los auriculares, por ejemplo, no tienen que ser malos, porque te pasas la mitad del día hablando y si estás rodeado de gente necesitas cancelación de ruido ANC. No es tanto cómo oyes tú, sino cómo te oyen a ti, si de verdad valoras tu mensaje. Cada vez hay más IA en estas herramientas, y por ejemplo Teams con Copilot te transcribe y resume la reunión, y hasta pasa lista para saber si están todos presentes. O si alguien pasa por delante de la pecera que no le confunda con la reunión.

Sostenibilidad y economía circular

Las nuevas claves de Patrimonio han ido muy bien, las AAPP se han puesto mucho más exigentes para el tema de gasto energético, con monitores más eficientes y con certificaciones que no existen todavía. Se va a ir al modelo de escala ABCDEFG y muchos equipos aún no tienen ni la C, que en el antiguo sería la A++. Hay stocks que no se van a poder destinar al mercado público, pero sí al privado, y en consumo hay ofertas de televisores estupendas, pero con la F actual.

Sin embargo, el mayor impacto no es tanto en consumo como en reciclaje y reacondicionamiento. Francia lidera este apartado, exigiendo que el 20% de sus compras públicas sea reacondicionado, y tiene sentido. Pero tiene que haber más empresas que se ocupen de ello, especialmente en el canal. Por nuestra experiencia, en lo que más se está dando es en temas de actualización de almacenamiento a SSD y memoria a DDR, y aunque parezca que no, el recambio de teclas machacadas.

supercomp
MAYORISTA INFORMÁTICO

HUAWEI eKit

Soluciones de red de la mano de Huawei

Los recursos para redes de HUAWEI están diseñados para que puedas disfrutar de una cobertura total que te permita acceder a Internet en cualquier lugar y de forma más estable que nunca. Descubre todos los productos de HUAWEI eKit y disfruta de diseños de red de calidad, más seguros y fiables.

HUAWEI eKit APP

Wi-Fi 7

Routers, AP y Switch

Digitalization for Success

HUAWEI

Supercomp Digital: nuevo distribuidor oficial de Huawei eKit

Encuentra las mejores soluciones para redes de Huawei eKit en:

www.supercompdigital.com

All in One 2201FT: utilízalo como TPV en tu negocio

Disfruta de la mejor potencia en tu puesto de trabajo

21,5" (546,1 mm) FHD

Intel Celeron™ N5095

4GB ram

128GB SSD

Wifi ac

Pantalla táctil

Windows 11 Pro

www.primux.es

primux
Be human. Live simple

Hornetsecurity celebra un encuentro con los partners

Hornetsecurity es un proveedor de seguridad, cumplimiento y backup en la nube de origen germano que está alcanzando cada vez más un mayor predicamento entre empresas de todo tamaño que se han pasado al Microsoft 365. Sus herramientas cubren todas las áreas importantes de la seguridad del correo electrónico, incluido el filtrado de spam y virus, la protección contra el phishing y el ransomware, el archivado y el cifrado conforme a la legalidad, así como la copia de seguridad, la replicación y la recuperación de los datos, los puestos de trabajo y las máquinas virtuales.

PARA DAR a conocer sus novedades de producto en Hornetsecurity, así como la presentación oficial del nuevo country manager para Iberia, Italia y Latinoamérica, la compañía organizó un día de campo con barbacoa y diversas actividades lúdicas, en la finca del Jardín de Somontes en la carretera de El Pardo. El Evento Partner Madrid 2024 contó con la presencia de sus principales integradores y mayoristas que compartieron valiosas experiencias y algunos avances en las novedades del fabricante.

Carlos Vieira, reconocido profesional del sector TI con más de 25 años de experiencia en compañías como Dell o Oracle, y habiendo cerrado una etapa con WatchGuard de más 16 de años, asume el cargo con el objetivo de mantener la trayectoria de crecimiento y liderazgo de la empresa conseguida hasta el momento bajo la dirección de Félix de la Fuente. En su presentación al canal, Vieira se comprometió a trabajar en estrecha colaboración con el equipo de Hornetsecurity y los partners para alcanzar nuevos hitos y mantener el compromiso con la excelencia en el servicio, declarando que está en su ADN la implementación exitosa de estrategias de crecimiento y la construcción de relaciones sólidas con clientes y socios comerciales.

Además de expresar su entusiasmo por asumir este nuevo desafío, Carlos Vieira comentó: “Es un reto asumir la dirección de Hornetsecurity tras la encomiable labor que ha realizado Félix en estos años. Agradezco la confianza depositada en mí y soy consciente del privilegio de asumir esta nueva responsabilidad. Durante mi carrera, he sido testigo del impacto que tiene una sólida estrategia de seguridad informática en cualquier empresa y la importancia de instaurar un buen software que proteja los activos digitales de cualquier empresa. Es por eso que estoy comprometido a continuar por la senda de crecimiento y el liderazgo que hemos establecido durante todos estos años”.

Carlos Vieira, Country Manager para Iberia, Italia y Latinoamérica de Hornetsecurity.

La empresa se ha marcado un objetivo de mantener el ritmo de crecimiento a doble dígito como velocidad de crucero. En otro momento de la presentación añadió: “En mi incorporación, cuento con el apoyo de un equipo excepcional y estoy seguro de que juntos alcanzaremos grandes logros. En Hornetsecurity, cada miembro del equipo aporta una combinación única de experiencia, habilidades y dedicación y estoy impresionado por el compromiso y la pasión que veo en cada uno de mis compañeros. Juntos, formaremos un equipo sólido y cohesionado, listo para enfrentar cualquier desafío que se presente”.

También informó sobre sus primeras actuaciones en el canal de su país de origen, Portugal, donde actualmente cuentan con una escasa presencia, a través del reclutamiento de partners de diverso tamaño para crear un canal mix-size. “Queremos dar un salto significativo en este canal y convertirnos en referentes en Microsoft, con todos los productos que ofrecemos”. Además, respecto a la estrategia SaaS y MPS, señaló la importancia de sus servicios gestionados en su oferta, sobre todo en el tema de la ciberseguridad que exige contar con un personal más especializado, pero sin olvidar que “seguimos trabajando también en la reventa”.

Más canal y mejor formado

Después de Carlos Vieira intervino Paul Canales, responsable de Canal de Hornetsecurity en la región Iberia, Italia y LatAm, que remarcó que la compañía está para ayudar a que los partners incrementen su facturación y por eso la atención prioritaria que la compañía está poniendo en Microsoft 365 para asegurar la continuidad del negocio de los clientes: “El principal vector de ataque sigue siendo un email. Por eso es clave en el O365, que muchos hackers usan para engañar. Tenemos que contrarrestar con un arsenal de herramientas que nos permitan actuar en cuatro frentes, que son los de prevención, protección, respuesta y recuperado, y todo ello gestionado desde una plataforma única, algo que no muchos fabricantes pueden ofrecer para todas estas soluciones”.

«Hay mucho dinero en los servicios de alrededor. No es poner solo más buzones, sino ser más creativo, y el año que viene queremos tener más partners, más formados y certificados» (Carlos Vieira, Hornetsecurity)

Pero en esta estrategia es fundamental la parte de la formación de los empleados. "Cuando algo falla, la culpa es siempre del usuario. Por eso necesita estar más formado. Y luego está la ensalada de siglas y tecnologías, no puede estar a todo eso. Lo fundamental para la empresa y lo que debe pedir a su sistema de ciberseguridad es poder garantizar la seguridad del dato, y si acaso reducir las tareas de administración". A lo que añade Paul Canales: "A través de demos, actuamos como un atacante real y lo medimos. Con ello podemos hacer un proyecto personalizado y adaptado al tipo de empresa y al tipo de usuario, automatizando tareas para minimizar errores y limitar el empleo de recursos superfluos. Con este informe en la mano ya puedes subirte al Consejo de Administración donde los CISOs ya tienen asiento porque ha llegado NIS2 y todos somos ahora responsables".

Es cierto que Microsoft está en la vanguardia de las soluciones de seguridad para sus sistemas Windows y las aplicaciones de negocio que la rodean, actualizando parches a medida que se detectan fallas o brechas que aprovechen los hackers, pero a veces esa misma contundencia conlleva más exigencias en la parte de administración de sistemas. "En términos de gestión de permisos, Office 365 puede ser complicado, especialmente cuando hablamos de archivos y backups. Si al final no somos capaces de protegernos, debemos tener una vía de escape para que la operativa del negocio no se detenga. Lo que buscamos es la continuidad del negocio, que las fábricas y el personal puedan seguir trabajando sin interrupciones".

Lo cual vuelve a llevarnos a la idea fundamental de la concienciación. La ciberseguridad debe entrar en la cultura de empresa. "Por eso decimos que es muy importante la

Paul Canales, director de Canal de Hornetsecurity en la región Iberia, Italia y LatAm.

concienciación en ciberseguridad. Pero no vale hacer una campaña puntual, debe ser una acción continua. Nuestro Go-to-Market ha sido siempre ese, el de la formación continua, incluso antes del NIS. Por ejemplo, nadie revisa ni se preocupa en quitar permisos una vez compartido el archivo, y así se van dejando cientos de puertas abiertas sin vigilar. La empresa ACME de 400 empleados tenía un volumen de 80.000 archivos compartidos cuando intervenimos, y cada día iba a más lo cual presenta desafíos significativos. Hubo que definir las directivas y hacer un ajuste fino en el Office 365, y logramos pasar en pocas semanas de esos 80.000 archivos a menos de la mitad, 39.000 compartidos, y de 2.000 usuarios anónimos a solo 200, mientras que el de usuarios externos se redujo de 600 a 13", comentaba el director de Canal. "Obviamente, la empresa ficticia éramos nosotros, nos gusta probar nuestras herramientas y predicar con el ejemplo. Nuestra tecnología añade una capa superior que facilita la tarea y supervisa todo el conjunto".

«En el MS Exchange hay una proporción de 64% que está aún onprem y el otro 36% en el cloud. Esto según se mire significa que ya hay un tercio del mercado al que puedo atacar con nuestros servicios de valor, y una gran oportunidad de negocio para que lleven 365 a la nube» (Paul Canales, Hornetsecurity)

Esta obsesión por facilitar las tareas de administración de sistemas es lo que les ha llevado al desarrollo de los planes Total Protection para ayudar al canal a llevar sus herramientas por sí mismos. "En el Exchange de Microsoft hay una proporción de 64% del mercado que está aún on-prem y el otro 36% en el cloud. Esto según se mire significa que hay una gran oportunidad de negocio de dos tercios para que lleven 365 a la nube y nosotros estar ahí, y un tercio restante al que puedo atacar con nuestros servicios de valor que están diseñados para facilitar la gestión de permisos, hacer cumplir políticas de cumplimiento, y garantizar copias de seguridad y recuperación eficientes dentro del entorno de 365".

El crecimiento de Microsoft es el crecimiento del canal, y más sabiendo que los ciberhackers se concretan cada vez más en los sistemas estándar más difundidos para aquilatar sus economías de escala y maximizar sus rendimientos. Lo cual exige esa constante actualización de la tecnología y adoptarse la mejora continua, que se refleja en el roadmap de la compañía germana: "Siempre nos estáis preguntando por lo siguiente que vamos a sacar para estar preparados. Os podemos anunciar que vamos a lanzar mejoras en el Permission Manager y en la DMARC (autenticación de mensajes, informes y conformidad basada en dominios). Vamos a incorporar al Total Backup nuevas herramientas como Planner, To-Do o Self-Service. También en el Security Awareness Service los husos horarios, nuevos idiomas y un Tennant Split. Para fin de año tendremos listo como novedad un gestor multitennat con preconfiguraciones y plantillas".

Premios 2023

Como colofón, se otorgaron los reconocimientos a los mejores partners del año 2023, que recayeron en Kyocera como Brand Embassador, en Inetum como Mejor Proyecto, y en Tigloo como Partner Revelación. Carlos Vieira fue el encargado de entregar las placas, no sin dejar de recordar el mensaje a sus socios: "Hay mucho dinero en los servicios de alrededor. No es poner solo más buzones, sino ser más creativo", señalaba. "El año que viene queremos tener más partners, más formados y certificados. Pueden ser muy grandes con sus SOCs o pequeños. Antes a veces eran estos los mejores por el engagement que lograban con el cliente y con nuestros comerciales y el servicio de asistencia".

MUZYBAR computer IMPORTADOR OFICIAL DE PUDU

KettyBot PRO

T300

BellaBot PRO

SH1

BellaBot

HolaBot

FlashBot

CC1

MUZYBAR computer

Avda. Cardenal Benlloch, 47 Bajo. E-46021 Valencia | 960 910 334 | info@muzybar.es| www.muzybar.es

MUZYBAR computer IMPORTADOR OFICIAL DE PUDU

IMPULSA TU SERVICIO

Una experiencia de cliente incomparable

MUZYBAR computer

Avda. Cardenal Benlloch, 47 Bajo. E-46021 Valencia | 960 910 334 | info@muzybar.es| www.muzybar.es

PREMIER
We're a team

TPV

FÁCIL DE COLOCAR,

PLEGABLE

SLIM

ALUMINIO

TPV 15,6" | J6412 | 8GB | 128GB | Opcional : Win 10 IoT | 16GB | 256GB

MUZYBAR
computer

Avda. Cardenal Benlloch, 47 Bajo. E-46021 Valencia | 960 910 334 | info@muzybar.es | www.muzybar.es

PREMIER

We're a team

DISEÑADO PARA IMPRESIONAR .

KT-100

TPV 15.6" | J6412 | 4GB | 128GB
Opcional : Win 10 IoT, 8GB, 16GB, 256GB
2nd screen 11.6"

KT-810

TPV 15" | J6412 | 8GB | 128GB
Opcional : Win 10 IoT, 16GB, 256GB
Customer display 2x20 LCD

KT-2000

TPV 15" | J6412 | 8GB | 128GB
Opcional : Win 10 IoT, 16GB, 256GB
10'1 inch 2nd screen,
2x20 customer display, MSR, iButton

KT-3000

TPV 15" | J6412 | 8GB | 128GB
Opcional : Win 10 IoT, 16GB, 256GB,
9'7 inch 2nd screen

KT-116

TPV 11.6" | J6412 | 8GB | 128GB
Android 11| RK3568 | 2+16GB
Opcional : Windows 10 IoT, 16GB, 256GB

KT-Kiosk

6412 QuadCore 1.99GHz | 8GB | 128GB
Android 11| RK3568 | 2+32GB
Opcional : Windows IoT, 16GB, 256GB

PCP 215

TPV 21,5" | J6412 | 8GB | 128GB
Android 11, 4GB+32GB
IP45 frontal y trasera
Opcional : Win 10 IoT, 16GB, 256GB,
Soporte

KIOSK 27 W/A

J1900 | 4GB | 128GB
Android 11, 4GB+32GB
Impresora térmica 80MM
Lector 2D | NFC | BT+WF | Cámara
Soporte Datáfono
Opcional : Win 10 IoT, 8GB, 256GB

MUZYBAR
computer

Avda. Cardenal Benlloch, 47 Bajo. E-46021 Valencia | 960 910 334 | info@muzybar.es| www.muzybar.es

ENERGY SISTEM

ICON SERIES

Diseñados para revolucionar tu experiencia sonora

80 W

15 H

RGB LED EFFECTS

Altavoz Bluetooth®

hyperbeat

¡La fiesta se desata donde tú quieras!

Altavoz estéreo de 80 W de potencia, resistente al agua, con luces LED y tecnología inalámbrica Bluetooth® 5.3.

ENERGY SISTEM

100 H

HYBRID ACTIVE NOISE CANCELLING

MADE FROM RECYCLED PLASTIC

ESmart Connect for Android and IOS

Auricular Bluetooth®

silentANC

Aíslate del mundo y reconecta cuando quieras

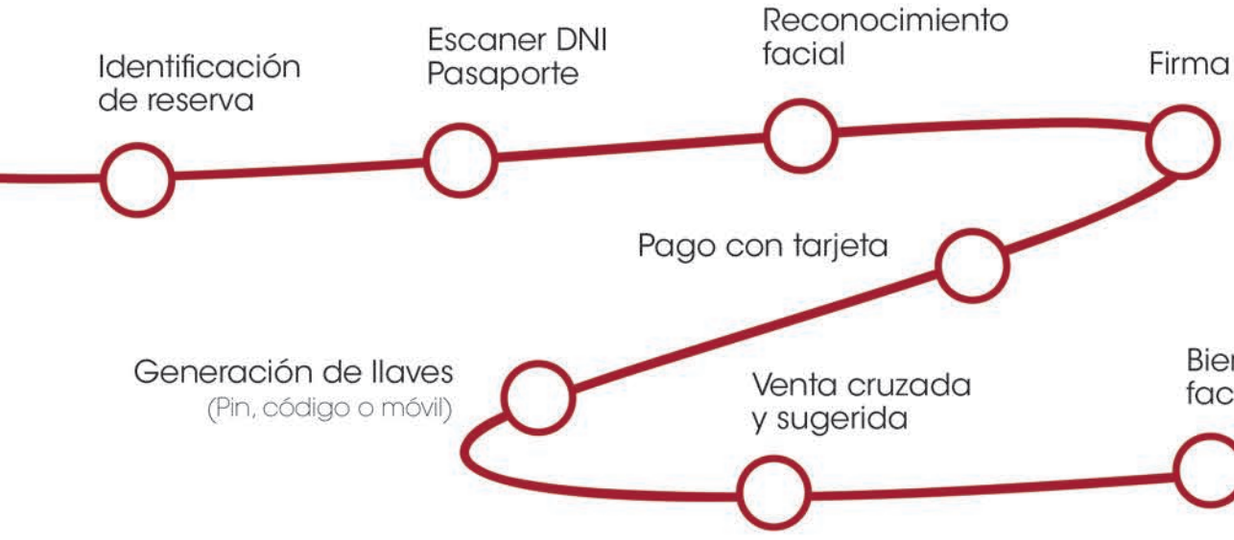
Con tecnología Hybrid Noise Cancelling para que disfrutes de cada matiz de tu música durante sus 100 horas de autonomía. Mantente siempre activo en todos tus dispositivos mediante la conexión multipunto y personaliza tu experiencia con ESmart Connect.

Hoteles sin esperas ni horarios.
FeelFree Check-in.

Partner Tech añade a su catálogo de soluciones 360 la última tecnología en **kioscos autocheck-in de exterior e interior** para el sector hotelero. Una nueva experiencia rápida e intuitiva que revoluciona los conceptos de check-in y check-out. **Rápidos, eficientes y flexibles**.

- Rapidez y comodidad
- Sin esperas ni colas
- Libertad y flexibilidad
- Disponible 24/7
- Agiliza operaciones
- Optimiza personal
- Reduce costes
- Clientes satisfechos

Libertad para el cliente. Eficiencia hotelera.



FeelFree Check-in te lo pone muy fácil

Los hoteles son para disfrutar, no para esperar.

FeelFree CHECK-IN

EXTERIOR

INTERIOR

Rápido, flexible y eficiente.

Partner Tech, soluciones 360°

Una empresa líder con el mayor catálogo de soluciones del mercado.
Nos ocupamos de todo para su negocio. Consultoría, personalización, instalación y mantenimiento.

Quieres concertar una demo?

913 120 632
comercial@partner-tech.eu
www.partner-tech.eu

PARTNER

CARE . TRUST . RESPONSIBILITY

One Ecosystem.
All possibilities.

Partner Tech incorpora en su catálogo todo un mundo de soluciones 360º para el Self Checkout, toda la innovación y tecnología adaptada a cada negocio.

Bora Bora
SCO del futuro, moderno, disruptivo, con holografía táctil.

Alfred
Compacto y modular, configurable según las necesidades.

Ace 2
Innovación, eficiencia y diseño personalizable.

"La mejor solución de SCO es la que utilizan todos los clientes"

Self Checkout Inteligente

RFID Lectura simultánea

Scan & Go Bring Your Own Device

Gestión de listas de selección

Verificación de edad

Crime predictor

Dashboard SeeYourSCO

Un software.
Una API.
Todas las funciones.

Sin restricciones.
Sin terceros.
Garantía de Partner Tech.

One partner. All possibilities.

El futuro del universo **Self-Service** ha llegado

Partner Tech, soluciones 360°

Una empresa líder con el mayor catálogo de soluciones del mercado.
Nos ocupamos de todo para su negocio. Consultoría, personalización, instalación y mantenimiento.

Quieres saber más sobre nuestro Ecosistema sco-E?

913 120 632
comercial@partner-tech.eu
www.partner-tech.eu

PARTNER

CARE . TRUST . RESPONSIBILITY

Cuatro claves que llevarán la videocolaboración al siguiente nivel

En el dinámico mundo de la tecnología, el sector de la videocolaboración está experimentando cambios significativos. Estas nuevas tendencias, están enfocadas en ofrecer una experiencia de calidad, inmersiva y sencilla, con el fin de llevar la colaboración virtual al siguiente nivel y eliminar definitivamente las barreras físicas.

ESTAS SON las cuatro claves que harán posible esta evolución durante el presente 2024:

- *Paneles interactivos all in one para una experiencia más inmersiva*

En los últimos años la videoconferencia se ha convertido en una manera común de realizar reuniones tanto internas, entre los equipos, como externas con clientes o proveedores. Este 2024, las videoconferencias seguirán siendo clave, pero los paneles interactivos all in one se convertirán en los protagonistas como respuesta a las demandas de una experiencia más inmersiva y eficiente.

Estos dispositivos integran pantallas táctiles, cámaras de alta definición, micrófonos avanzados y altavoces de calidad, todo en un único producto. Gracias a la sinergia de estas funciones, no solo se mejora la calidad de las videoconferencias, sino que también facilita la colaboración en tiempo real, permitiendo la creación y edición de contenido de forma conjunta, como si todos los participantes estuvieran en la misma sala eliminando así cualquier tipo de barrera física.

- *Desarrollo de los entornos certificados Microsoft Teams (MTR)*

La integración cada vez más profunda de plataformas de colaboración como Microsoft Teams llevará durante este año al desarrollo de entornos certificados MTR. Estos entornos ofrecen una experiencia optimizada y sin problemas al conectar hardware, software y servicios en una solución integral. La certificación MTR garantiza la compatibilidad y la interoperabilidad, reduciendo los problemas técnicos y permitiendo a las empresas centrarse en la colaboración efectiva en lugar de la gestión de la tecnología para centrarse en lo importante.

- *Espacios sin cables para ganar flexibilidad y dinamismo*

La eliminación de cables en las salas de reuniones es una tendencia que estará muy presente a lo largo de este año y que permitirá liberar a los equipos de las limitaciones físicas, permitiéndoles compartir contenido de manera más rápida y eficiente. La adopción de tecnologías inalámbricas para la transmisión de datos y la conexión a pantallas mejora la flexibilidad y la agilidad en el entorno de trabajo, creando un ambiente más dinámico y propicio para la colaboración espontánea.

«Las videoconferencias seguirán siendo clave, pero los paneles interactivos all-in-one se convertirán en los protagonistas como respuesta a las demandas de una experiencia más inmersiva y eficiente. Estos dispositivos integran pantallas táctiles, cámaras de alta definición, micrófonos avanzados y altavoces de calidad, todo en un único producto» (Álvaro Ausín, MaxHub)

- *El uso del formato 21:9 para displays y led para mejorar la experiencia visual*

El formato de pantalla 21:9 se está convirtiendo en la mejor opción para entornos de videoconferencia y presentaciones. Este formato panorámico proporciona una experiencia visual más inmersiva, permitiendo una visión más amplia y detallada durante las reuniones virtuales. Además, la tecnología led complementa este formato, ofreciendo colores más vibrantes y un contraste mejorado, elevando así la calidad general de las presentaciones y videoconferencias.

En definitiva, el 2024 está marcado por innovaciones que no solo mejorarán la eficiencia en el trabajo colaborativo, sino que también van a redefinir la forma en que las empresas se conectan y colaboran a nivel global.

Álvaro Ausín,
Country Sales Manager de MaxHub para España y Portugal

Y cuatro apuestas seguras para este 2024

En el pasado ISE de Barcelona, la marca de soluciones de videoconferencia y colaboración, presentaba su póker de pantallas para diversos ámbitos: una innovadora serie CMD de pantallas comerciales todo-en-uno, la serie XT certificada para salas Microsoft Teams para potenciar el trabajo colaborativo y la experiencia en reuniones, y una serie de nuevos productos de diseño integrado, que abarcan desde soluciones led hasta soluciones de comunicación unificadas.

"En MaxHub estamos comprometidos con la revolución de la experiencia de trabajo colaborativo. Nuestros nuevos lanzamientos representan nuestro enfoque en calidad, simplicidad y productividad. En ISE 2024, hemos mostrado cómo transformar la manera de reunirse y colaborar, redefiniendo el estándar de la innovación en el espacio de trabajo", señalaba Álvaro Ausín.

La presencia de la compañía en ISE por tercer año consecutivo tenía el objetivo de reforzar su posicionamiento como una de las principales figuras en el sector de la tecnología audiovisual y demostrar su apuesta por el mercado español y su compromiso con la red de socios europeos. Cómo reconocimiento, se llevó el premio Best of Show ISE 2024 en la categoría de Instalación, además de ampliar sus acuerdos de partnerships con demostraciones interactivas.

- *Pantalla comercial MaxHub Serie CMD*. Se trata de una pantalla todo-en-uno diseñada para la colaboración en salas de reuniones pequeñas y medianas. Esta serie combina un monitor, una cámara, un micrófono, altavoces y un sistema operativo en un único dispositivo integrado. Gracias a este diseño compacto, se combina a la perfección todas las herramientas de colaboración esenciales, lo que se traduce en un flujo de trabajo más fluido y productivo. Además, admite conectividad inalámbrica BYOD con terceros dispositivos, un rendimiento de audio respaldado por un micrófono de ocho matrices con un alcance de captación de 8 metros, y un rendimiento de vídeo de primera calidad que aporta una experiencia en persona a cada interacción. Sin necesidad de compras adicionales, esto no solo reduce los costes de adquisición, sino que también simplifica el proceso de instalación y el mantenimiento continuo.

- *MaxHub Serie XT para salas Microsoft Teams*. Incluye el kit XCore básico y dos periféricos UC, S07 y W31, todos ellos certificados para Microsoft Teams Rooms para Windows. El kit de consola táctil Windows Compute, con varias opciones de cámara USB 4K, altavoz y opciones de barra de vídeo, está además diseñado para convertir salas BYOD pequeñas y medianas en salas Microsoft Teams totalmente certificadas. Los clientes también pueden etiquetar varias pantallas de sala, desde pantallas LCD comerciales hasta pantallas DVLed (Direct View Led). Esto garantiza la máxima rentabilidad al tiempo que mejora la experiencia de colaboración de los equipos híbridos.

- *MaxHub Videobar UC S15*. Se trata de una videobarra todo-en-uno, diseñado exclusivamente para salas tipo huddle rooms y otro tipo de pequeños espacios de reunión. Este dispositivo admite conectividad BYOD por cable e inalámbrica, junto con funciones de proyección inalámbrica. El UC S15 cuenta con una cámara 4K integrada con funciones avanzadas de IA como encuadre automático e inteligente o seguimiento de los interlocutores. Con la reducción de ruido basada en la IA, se filtran eficazmente las perturbaciones de fondo, como los golpes, el tecleo o el cierre de puertas, lo que garantiza un entorno libre de distracciones que mantiene la atención a la persona que habla o presenta. Gracias al control con MaxHub Pivot, los administradores de TI pueden supervisar, controlar y actualizar sin esfuerzo todos los dispositivos de la sala de reuniones de forma remota.

- *Soluciones led integradas de MaxHub*. Gracias a un diseño de vanguardia y capacidades de configuración hasta una compatibilidad perfecta con fuentes externas, la nueva gama de pantallas led están diseñadas para satisfacer diversos requisitos de visualización tanto en interiores como en exteriores con una calidad que mejora la productividad y la colaboración.

Entre ellas se incluyen:

- Pantalla led todo-en-uno: Serie Raptor, Serie Raptor Ultra-Wide
- Pantalla led de píxeles finos para interiores: CM27, GV27, GH31
- Pantalla led para exteriores: YM53

Altamente compatibles con la amplia gama de productos de la firma china, tales como altavoces, cámaras PTZ y el atril inteligente, las soluciones led permiten una configuración fácil sin necesidad de buscar dispositivos o aplicaciones adicionales. De esta forma, ofrece una versatilidad y rentabilidad para satisfacer diferentes necesidades de colaboración.

Nuevos partnerships

A lo largo de estos días, la compañía ha cerrado un acuerdo de colaboración con Nureva Inc con el objetivo de revolucionar las reuniones híbridas y mejorar su eficacia. También se ha reunido con importantes partners, entre ellos el recién estrenado Intel, que aportará su excepcional tecnología de chips para impulsar el hardware del fabricante chino, garantizando un sólido rendimiento operativo, una experiencia de usuario fluida y una rápida capacidad de procesamiento de datos, haciendo que cada reunión se realice sin esfuerzo. Y en el ámbito de las plataformas, la mencionada colaboración de MaxHub con Microsoft Teams que ha dado lugar al desarrollo de la serie XT.

"Para nosotros estar en ISE fue fundamental ya que nos permite juntarnos con figuras clave de sector de la tecnología audiovisual, nos sirve de altavoz para dar a conocer nuestras novedades al mundo y posicionarnos como expertos en soluciones de colaboración", concluía Ausín. "Estamos orgullosos de participar un año más en ISE y poder presentar cuatro nuevos productos, cada uno innovador y único en su objetivo de contribuir al futuro del trabajo colaborativo aún más eficaz. Estos lanzamientos también refuerzan el liderazgo de la compañía en el sector de la colaboración y visualización y nuestra consolidación en el mercado español".

La gran migración silenciosa para abandonar el 2G y 3G debe adelantarse a 2025

Se calcula que antes de 2030 se producirá el apagón definitivo de la red 2G (el 3G se apagará antes). Aunque hace años que ya no se utiliza en móviles, continúa siendo la tecnología de acceso estándar de muchos dispositivos IoT gestionados por empresas que dependen de su conectividad. Desde Wireless Logic recomiendan migrar ya a redes de nueva generación y alertan de las consecuencias de esperar hasta el último momento: cuanto más tarde se comience el proceso, será más costoso y habrá más riesgos de que ciertas aplicaciones críticas queden sin conectividad.

EL SECTOR de las telecomunicaciones y las empresas afectadas por el apagón de las redes 2G y 3G dan por hecho que antes de 2030 tiene que estar culminado un proceso que lleva en marcha varios años, aunque a una velocidad inferior a la deseada por muchos expertos. El problema de fondo es que no existe una fecha oficial y unificada para dejar a un lado definitivamente ambas redes. Al ser las teleoperadoras de cada país las que controlan los tiempos, el apagón no es uniforme a nivel global y las empresas no cuentan con un calendario cerrado y unificado para el plan de migración.

"Hacia finales de 2025 ya habrá muchas teleoperadoras que habrán dejado de ofrecer conexiones 3G. Aunque el 2G aguantará en España hasta final de década, conviene iniciar cuanto antes el plan de migración a tecnologías de acceso más actuales, puesto que en muchos casos se trata de un trabajo de una envergadura considerable", explica Jon Mielgo, director general de Wireless Logic España.

Máxime si se tiene en cuenta que, entre las empresas afectadas, hay algunas con aplicaciones del Internet de las Cosas (IoT) de tan variada naturaleza como soluciones conectadas de seguridad, dispositivos de pago, equipos de monitorización eléctrica o sistemas de gestión de flotas que disponen de miles de localizadores GPS en sus vehículos. Es decir: negocios basados en un número elevado de dispositivos conectados que usan cada día formas de conectividad en inminente riesgo de extinción.

El momento es ahora

Hay una paradoja en esta situación, y es que las compañías saben que no tienen mucho margen para migrar su conectividad basada en 2G y 3G a nuevos estándares como 4G y 5G. Aunque la decisión se ha empujado en el tiempo para dar margen a la migración de un parque de dispositivos conectados compuesto por cientos de miles de unidades, el apagón ya está a la vuelta de la esquina.

"El 2G seguirá teniendo vigencia durante unos años, pero conviene tomar medidas cuanto antes. Si una empresa tiene que migrar la conectividad en miles de dispositivos, es mejor hacerlo de forma planificada, durante unos años, que en tan solo unos meses", añade Mielgo. "La tecnología avanza y es un proceso natural que llegue algún día el apagón, sobre todo si tenemos en cuenta que, si estos sistemas migran a 4G o 5G, van a ser más eficientes, seguros y adaptables a un ecosistema IoT que exige nuevos estándares".

Por lo general, las empresas y teleoperadoras tienen el foco puesto en 2030, por lo que muchas compañías simplemente están "ganando tiempo", advierte el director general de Wireless Logic. "Nuestra recomendación es actuar cuanto antes, porque además el apagón ya se ha producido en

«El 2G seguirá teniendo vigencia durante unos años, pero conviene tomar medidas cuanto antes. Si una empresa tiene que migrar la conectividad en miles de dispositivos, es mejor hacerlo de forma planificada, durante unos años, que en tan solo unos meses» (Jon Mielgo, Wireless Logic)

países como Japón y Corea del Sur, donde ya no existe conectividad 2G. Pero, al mismo tiempo, Reino Unido ha puesto como fecha de apagón del 2G el año 2033 y en España se habla de final de década. Es una horquilla demasiado amplia y son los operadores de cada país quienes están estableciendo sus propias fechas. Por eso consideramos que la situación exige actuar cuanto antes y comenzar la migración antes de que sea demasiado tarde, ya que muchas empresas podrían encontrarse trabajando con un sistema de conectividad obsoleto casi de la noche a la mañana, con todo lo que eso implicaría para sus negocios".

Wireless Logic, proveedor global de conectividad IoT, ha elaborado una guía del apagón 2G/3G para informar a la industria y a las empresas sobre sus opciones de migración, y ayudarles a suavizar esta transición tan traumática pero necesaria. "En todo caso, parece que entre 2025 y 2030 quedará el asunto resuelto con la desaparición total del 2G y 3G, por lo que, ante la incertidumbre y dado que muchos sistemas conectados no podrán ser simplemente actualizados, sino que deberán llevar a cabo incluso sustituciones completas, recomendamos planificar y comenzar la migración como tarde en 2025, si no antes, lo que evitará cuellos de botella o descuidar aspectos como la ciberseguridad", asegura Mielgo. "Recomendamos realizar cuanto

Jon Mielgo, director general de Wireless Logic España.

antes un inventario de dispositivos conectados por 2G y 3G, indicando las especificaciones técnicas, las necesidades de comunicación en cuanto a latencia y ancho de banda, la prioridad de actualización para el negocio y los retos operativos en cuanto a la intervención física en el equipo".

Elegir la tecnología adecuada

Una decisión clave a la hora de acometer el plan de migración es la nueva tecnología de acceso de red con la que se desea comunicar los dispositivos. Para ello, se deben tener claras las necesidades y circunstancias de los dispositivos, respondiendo a una serie de preguntas: ¿Cuántos datos consumen? ¿Cada cuánto tiempo es necesario comunicarse con ellos? ¿Utilizan métodos de ahorro energético como PSM o eDRX? ¿Cuál es la ubicación física de los equipos?

Si se encuentran en localizaciones subterráneas podría ser necesario utilizar NB-IoT (banda estrecha), pero si se trata de dispositivos en movimiento podría ser preferible optar por alternativas como LTE-M. En el caso de una implantación IoT a escala global, quizás LTE CAT-1 Bis pueda ser la elección adecuada, dado que no cuenta con las limitaciones de despliegue de infraestructura que afectan a NB-IoT o LTE-M. "Son muchos factores a considerar, y entendemos que puede ser muy complejo tomar las decisiones adecuadas. Es clave, para una migración fluida y exitosa, contar con un proveedor de conectividad que conozca el ecosistema y sepa guiar a las empresas a lo largo de todo el camino", concluye Jon Mielgo.

Es un proceso que puede ser muy arduo, pero que, gracias al apoyo de partners especializados en conectividad IoT como Wireless Logic, puede convertirse en una tarea más sencilla y eficiente, dada su capacidad para detectar las necesidades de cada negocio y ofrecer las garantías necesarias para que el apagón del 2G y 3G, sea cuando sea finalmente, pille a las compañías con los deberes hechos en tiempo y forma.

Una SIM única para proyectos IoT globales

En un mundo cada vez más interconectado, la gestión efectiva de dispositivos IoT se ha convertido en una prioridad para empresas de un amplio abanico de sectores, especialmente en operaciones a escala internacional. Tanto es así, que la inversión del mercado global en IoT supone ya más de 170.000 millones de dólares únicamente en el sector industrial, según la plataforma Statista. Además, según IoT Analytics se calcula que en 2023 se superó la cifra de 500 millones de unidades IoT basados en eSIM/iSIM en todo el mundo.

En este contexto de expansión, Wireless Logic ha hecho una apuesta decidida por la tecnología de aprovisionamiento remoto de SIM (Remote SIM Provisioning o RSP), que promete cambiar el panorama de la conectividad IoT, pues aporta a los dispositivos IoT una serie de ventajas clave para superar los principales obstáculos de conectividad en el futuro de sectores como la logística internacional y la fabricación avanzada.

"En un proyecto IoT la conectividad no termina con la implantación del módulo o tarjeta en el dispositivo; ese es solo el primer paso. A lo largo del tiempo pueden surgir diversos retos, especialmente en despliegues multinacionales", explica Beni Álvarez, director Técnico de Wireless Logic España. Y es que los posibles cambios normativos relacionados con la soberanía de datos, las modificaciones en las condiciones del roaming permanente o incluso los propios cambios tecnológicos pueden amenazar la continuidad de la conectividad.

Frente a estas circunstancias la industria cuenta con una tecnología esencial para preparar los despliegues de dispositivos IoT para el futuro: el aprovisionamiento remoto de SIM, impulsada y estandarizada por la GSMA (Global System for Mobile Communications Association) y recientemente actualizada mediante la especificación SGP.31.

En particular, esta funcionalidad permite "cargar o modificar perfiles dentro de la eSIM a través de la red, sin necesidad de un cambio físico de tarjeta". Algo que, como señalan desde Wireless Logic, conlleva múltiples beneficios:

- *Facilitar la logística*: para fabricantes con despliegues globales, una eSIM con aprovisionamiento remoto simplifica la logística, ya que permite un único stock de unidades (SKU) para dispositivos en diferentes territorios.

- *Cambios en las condiciones de roaming permanente*: el aprovisionamiento remoto permite adaptarse a los cambios sin necesidad de modificar físicamente las tarjetas de los dispositivos.

- *Obsolescencia de las tecnologías de acceso*: ante la desconexión de las redes 2G y 3G, la eSIM puede reducir costos operativos al permitir la carga remota de perfiles 4G o 5G, siempre que el dispositivo sea compatible con estas tecnologías.

- *Re-despliegue de dispositivos en nuevos entornos*: la tecnología eSIM agiliza la adaptación de dispositivos a nuevas ubicaciones al evitar el cambio físico de tarjeta.

Cómo ayuda Conexa

Wireless Logic mantiene un firme compromiso con brindar a sus clientes una "conectividad preparada para el futuro", y busca liderar la evolución de la conectividad IoT en un mundo en constante evolución. Así, ofrece soluciones que se alinean perfectamente con las necesidades de fabricantes, integradores de sistemas y proveedores de servicios IoT, que buscan conectividad sin las ataduras de un operador y la capacidad de gestionar los cambios futuros.

Y en respuesta a esos desafíos actuales surge Conexa, la red desarrollada por Wireless Logic para facilitar que todos los perfiles de empresas puedan llevar el control del ciclo de vida de sus activos conectados a un nuevo nivel, desde la fábrica hasta la implantación. Así, la plataforma SIMPro proporciona un ecosistema único con el que poder conectar y gestionar los activos IoT de cualquier red en todo su despliegue de manera segura.

Beni Álvarez, director Técnico de Wireless Logic España.

Esto es posible mediante la combinación de dos tecnologías clave: la versatilidad de la tecnología eSIM/eUICC para afrontar los desafíos que están por llegar, con la simplicidad de la capacidad multi-IMSI. Por una parte, la tecnología eSIM/eUICC es la que permite el aprovisionamiento remoto para poder subir nuevos perfiles sin necesidad de intervención física, y adaptar así el dispositivo a los futuros retos de conectividad. Mientras, la capacidad multi-IMSI es la que permite a la SIM cambiar entre los diferentes perfiles cargados, para seleccionar aquel que más se adecúe a cada circunstancia, o incluso programar que se activen unos u otros en función de la ubicación.

En este sentido, Wireless Logic pone a disposición del canal una extensa guía "para conocer con todo detalle las características principales de estas tecnologías, así como de las posibilidades del aprovisionamiento remoto de SIM para los despliegues IoT a escala multinacional".

Conexiones verticales

Con más de 13 millones de dispositivos conectados en 165 países y asociaciones directas con más de 50 operadores de telefonía móvil y por satélite, este proveedor ofrece cobertura mundial y servicios de IoT integrales que aceleran el éxito de los proyectos del IoT y ofrece valor en toda la cadena de conectividad que incluye más de 750 redes en todo el mundo. A través de esta plataforma creada específicamente por Wireless Logic y una red dedicada al IoT, permite a los clientes conectar y gestionar activos de forma segura en cualquier red y con cualquier número de despliegues, superando obstáculos de conectividad y brindando a las empresas un acceso sin precedentes a mercados globales. Esto simplifica las operaciones, acelera el time-to-market y reduce el coste total de propiedad, ofreciendo de esta forma una conectividad que, sencillamente, funciona como necesitan.

"Nuestros servicios IoT se diseñan, prueban, implantan y gestionan meticulosamente para satisfacer las necesidades específicas de la flota de dispositivos de cada cliente. Se esfuerzan por ofrecer los servicios de conectividad más fiables, flexibles y seguros del mercado", señalan. "Los clientes de Wireless Logic van desde empresas globales y gobiernos hasta startups y pymes, y operan en una amplia gama de sectores del mercado, incluyendo agricultura, sanidad, fabricación, seguridad, transporte, energía, servicios públicos y ciudades inteligentes".

«En un proyecto IoT la conectividad no termina con la implantación del módulo o tarjeta en el dispositivo; ese es solo el primer paso. A lo largo del tiempo pueden surgir diversos retos, especialmente en despliegues multinacionales» (Beni Álvarez, Wireless Logic)

TERMINALES PUNTO DE VENTA WINDOWS

P.C.MIRA
Tel: 93.410.63.63
comercial@pcmira.com
www.pcmira.com

poslab

> POS-9590 J6412

- > Monitor 15". 400 nits.
- > Pantalla PCAP multipunto.
- > CPU Intel Celeron J6412, Quad-core 11ª generación.
- > 4Gb RAM DDR4.
- > 128Gb SSD.
- > 4xCOM, 3xUSB 3.0, 1xUSB 2.0, 1xGigabit LAN, 1xCajón, 1xHDMI.
- > Opción de visor o pantalla.

> POS-9590 i5-G7

- > Monitor 15". 400 nits.
- > Pantalla PCAP multipunto.
- > CPU Intel core-i5 1135 G7, Tiger Lake 11ª generación.
- > 8Gb RAM DDR4.
- > 128Gb SSD.
- > 4xCOM, 3xUSB 3.0, 1xUSB 2.0, 1xGigabit LAN, 1xCajón, 1xHDMI.
- > Opción de visor o pantalla.

FABRICADOS EN TAIWÁN CON ALTOS ESTÁNDARES DE CALIDAD

DISPONIBLES OPCIONES COMO VISOR TRASERO DE 2 LÍNEAS, LECTOR DE TARJETAS, PANTALLA TRASERA DE 10.1", ADAPTADOR VESA PARA INSTALAR EN PARED ...

EN PCMIRA SOMOS MAYORISTAS E IMPORTADORES DE:

- > TPV WINDOWS.
- > TPV ANDROID.
- > TABLETS WINDOWS.
- > TABLETS ANDROID.
- > SOFTWARE PARA TPV.
- > QUIOSCOS.
- > PDA ANDROID.
- > PDA CON IMPRESORA.
- > LECTORES CÓDIGOS DE BARRAS.
- > CAJAS REGISTRADORAS.
- > CAJONES DE EFECTIVO.
- > IMPRESORAS TICKETS.
- > IMPRESORAS ETIQUETAS.
- > IMPRESORAS PORTÁTILES.

TERMINALES PUNTO DE VENTA ANDROID

P.C.MIRA
Tel: 93.410.63.63
comercial@pcmira.com
www.pcmira.com

iMin
Intelligence for Business

> D3

- > Pantalla 15.6".
- > Opción 15.6" + 10".
- > Gama económica.

> D4

- > Pantalla 15.6".
- > Opción 15.6" + 10"/15.6".
- > Impresora 80mm.
- > Gama profesional.

> SWAN

- > Pantalla 15.6".
- > Opción 15.6" + 10" + NFC
- > Gama profesional.

> KDS K1

- > Pantalla 21.5".
- > Para colgar en pared.
- > Monitor en Cocina.
- > Gama industrial.

> D1

- > Pantalla 10.1".
- > Impresora 57mm.
- > Visor trasero.
- > Gama económica.

> FALCON

- > Pantalla 10.1".
- > Impresora 80mm.
- > Visor trasero. NFC opc.
- > Gama profesional.

EN PCMIRA SOMOS MAYORISTAS E IMPORTADORES DE:

- > TPV WINDOWS.
- > TPV ANDROID.
- > TABLETS WINDOWS.
- > TABLETS ANDROID.
- > SOFTWARE PARA TPV.
- > QUIOSCOS.
- > PDA ANDROID.
- > PDA CON IMPRESORA.
- > LECTORES CÓDIGOS DE BARRAS.
- > CAJAS REGISTRADORAS.
- > CAJONES DE EFECTIVO.
- > IMPRESORAS TICKETS.
- > IMPRESORAS ETIQUETAS.
- > IMPRESORAS PORTÁTILES.

TERMINALES PUNTO DE VENTA WINDOWS

P.C.MIRA
Tel: 93.410.63.63
comercial@pcmira.com
www.pcmira.com

UNICOPOS

> W64NP
- > Pantalla 15.6". 1920x1080.
- > CPU J6412, 4+128GB.
- > Visor o LCD opcional.
- > Base de aluminio.

> W51035NP
- > Pantalla 15.6". 1920x1080.
- > CPU i5-1035G1, 8+128GB.
- > Visor o LCD opcional.
- > Base de aluminio.

> WP64NP
- > Pantalla 15.6". 1920x1080.
- > CPU J6412, 4+128GB.
- > Impresora integrada.
- > Visor o LCD opcional.

> WP51035NP
- > Pantalla 15.6". 1920x1080.
- > CPU i5-1035G1, 8+128GB.
- > Impresora integrada.
- > Visor o LCD opcional.

> UNICO-W2164N
- > Pantalla 21.5". 1920x1080.
- > CPU J6412, 4+128GB.
- > Panel PC o Monitor Cocina
- > Para colgar en la pared.

> UNICO PT15/PT17
- > Pantallas táctiles, VGA+USB.
- > PT15C: 15", 1024x768.
- > PT17C: 17", 1280x1024.
- > Pueden ir en pared.

EN PCMIRA SOMOS MAYORISTAS E IMPORTADORES DE:

- > TPV WINDOWS.
- > TPV ANDROID.
- > TABLETS WINDOWS.
- > TABLETS ANDROID.
- > SOFTWARE PARA TPV.
- > QUIOSCOS.
- > PDA ANDROID.
- > PDA CON IMPRESORA.
- > LECTORES CÓDIGOS DE BARRAS.
- > CAJAS REGISTRADORAS.
- > CAJONES DE EFECTIVO.
- > IMPRESORAS TICKETS.
- > IMPRESORAS ETIQUETAS.
- > IMPRESORAS PORTÁTILES.

SOFTWARE PARA TPV ANDROID

P.C.MIRA
Tel: 93.410.63.63
comercial@pcmira.com
www.pcmira.com

FactoryPOS




> TPV

- > Control de Ventas.
- > Control estadístico.
- > Control de Usuarios.
- > Gestión de Mesas.
- > Estadísticas y Stocks.

> COMANDEROS

- > Gestión de mesas.
- > Gestión de pedidos.
- > Envíos a cocina.
- > Gestión del cobro.
- > Impresión del ticket.

> KDS COCINA

- > Recepción de pedidos.
- > Múltiples secciones.
- > Varias visualizaciones.
- > Orden de platos.
- > Gestión de colas.

> KIOSCOS

- > Gestión de auto-pedidos.
- > Cobro automatizado.
- > Envíos a Cocina.
- > Multi-idioma.
- > Interfaz de uso amigable.

> BACK-OFFICE

- > Alojado en la nube.
- > Multilocal.
- > Configuración.
- > Estadísticas.
- > Copias de seguridad.

> PEDIDOS ONLINE

- > Aplicación de pedidos.
- > A recoger, a domicilio.
- > Pedidos en mesa, Carta.
- > Pagos integrados.
- > Conexión a plataformas.

EN PCMIRA SOMOS MAYORISTAS E IMPORTADORES DE:

- > TPV WINDOWS.
- > TPV ANDROID.
- > TABLETS WINDOWS.
- > TABLETS ANDROID.
- > SOFTWARE PARA TPV.
- > QUIOSCOS.
- > PDA ANDROID.
- > PDA CON IMPRESORA.
- > LECTORES CÓDIGOS DE BARRAS.
- > CAJAS REGISTRADORAS.
- > CAJONES DE EFECTIVO.
- > IMPRESORAS TICKETS.
- > IMPRESORAS ETIQUETAS.
- > IMPRESORAS PORTÁTILES.

TPV ANDROID DE TERCERA GENERACIÓN

P.C.MIRA
Tel: 93.410.63.63
comercial@pcmira.com
www.pcmira.com

SUNMI
Android POS Leader

> D3mini-58

- > Pantalla 10.1". A-13.
- > Impresora 58mm.
- > Visor 1 línea.
- > 3+32Gb. Batería.

> D3mini-80

- > Pantalla 10.1". A-13.
- > Impresora 80mm.
- > Visor LCD 4".
- > 3+32Gb. NFC.

> T3 PRO

- > Pantalla 15.6". A-13.
- > Opción Visor 10"/15,6".
- > 6+128Gb. Lector huella.
- > Cámara 8MP.

> T3 PRO MAX

- > Pantalla 15.6". A-13.
- > Opción Visor 10"/15.6".
- > Impresora 80mm.
- > 6+128Gb. Lector huella.

LA TERCERA GENERACIÓN DE TERMINALES SUNMI, MAXIMIZA EL RENDIMIENTO Y USABILIDAD, CON EL MEJOR DISEÑO.

> V3 MIX

- > Pantalla 10.1". A-13.
- > Impresora 80mm. NFC.
- > Cámara, Scanner.
- > Batería.
- > Cuna de carga opcional.

EN PCMIRA SOMOS MAYORISTAS E IMPORTADORES DE:

- > TPV WINDOWS.
- > TPV ANDROID.
- > TABLETS WINDOWS.
- > TABLETS ANDROID.
- > SOFTWARE PARA TPV.
- > QUIOSCOS.
- > PDA ANDROID.
- > PDA CON IMPRESORA.
- > LECTORES CÓDIGOS DE BARRAS.
- > CAJAS REGISTRADORAS.
- > CAJONES DE EFECTIVO.
- > IMPRESORAS TICKETS.
- > IMPRESORAS ETIQUETAS.
- > IMPRESORAS PORTÁTILES.

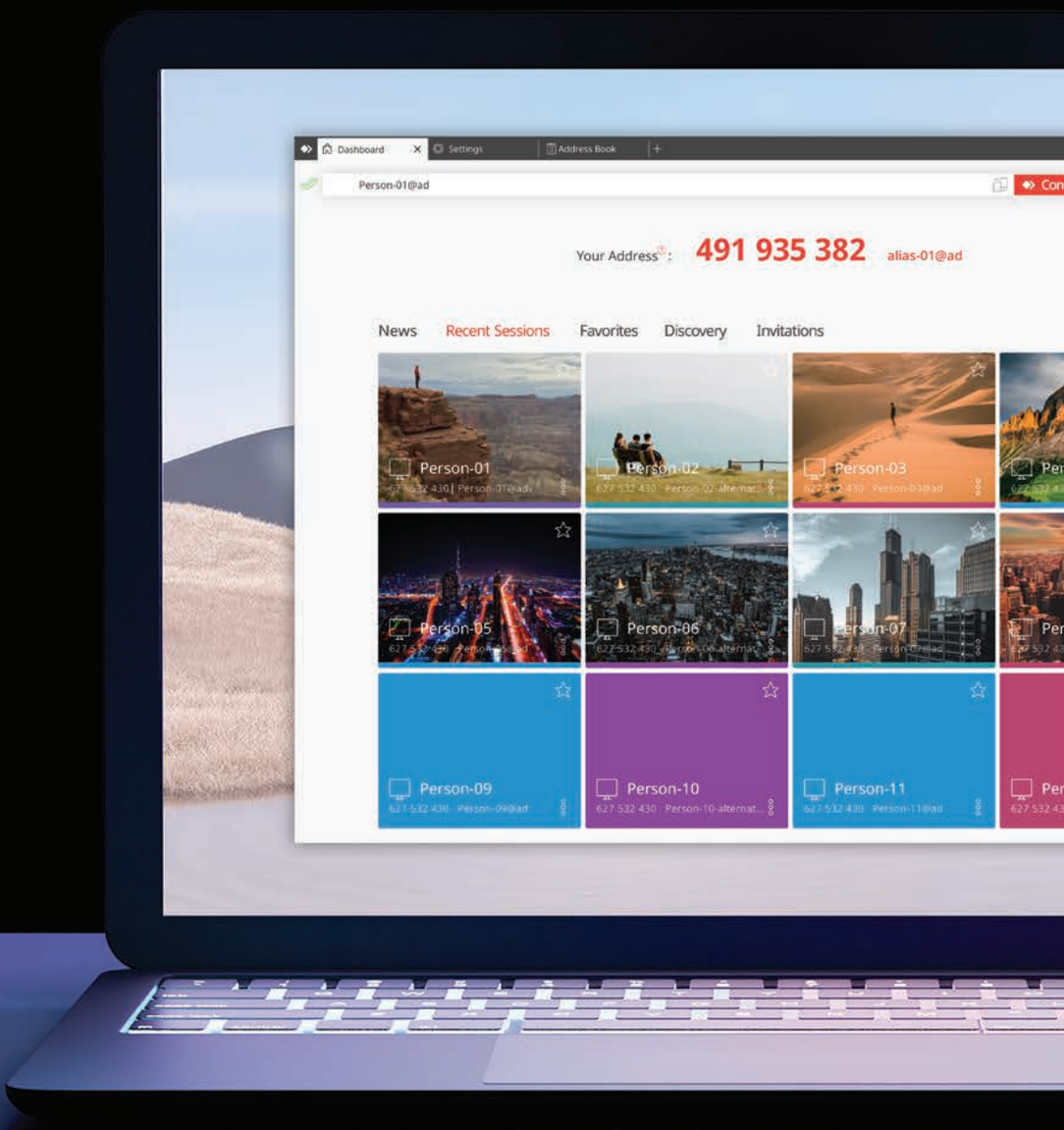
AnyDesk

Access.Now.

Software de Escritorio Remoto

Acceda de forma rápida y segura a cualquier dispositivo, **en cualquier momento** y desde **cualquier lugar.**

- Seguridad **superior**
- Rendimiento **inigualable**
- Administración de **usuarios facilitada**
- Personalización **superior**



Descubre todo lo que
AnyDesk tiene para ofrecer:

https://zaltor.com/anydesk

AnyDesk | zaltor Software Distribution