AÑO XXX Nº335 0.01 Euros

tai price book®

Junio 2023

NP comunicaciones

Si siempre te ha gustado ganar, tarde o temprano llegarás a **Mast Backup Online.**

En Mast Backup Online llevamos 13 años protegiendo la información de los clientes de nuestros partners y creciendo terabyte a terabyte, con márgenes para nuestros resellers superiores al 50% y un panel de control único que simplifica todo el proceso administrativo. Sin pago por licencias, sin costes adicionales, sin largas esperas para disponer de una copia física de la información y sin sorpresas. Si siempre te ha gustado ganar, piensa en Mast Backup Online. Porque aquí encontrarás la solución más rentable de backup online: contratos individuales, premier partner o marca blanca. **Ven a Mast Backup Online, vende y gana.**

Contratos individuales: Un contrato por cliente. Tanto vendes, tanto compras. 0 inversión y 0 riesgo. Bienvenido al backup.

Premier partner: Un espacio único. Lo compras y lo distribuyes como quieras. Divide y gana más.

Marca blanca: Nuestra plataforma es tuya. Crea tus servicios de backup. Gestiona tu canal.

MAST BACKUP ONLINE

*SIN INFORMACIÓN, **NO HAY EMPRESA***

mastbackuponline.com • mbo@mastbackuponline.com • 935 045 330

ven vende gana

tai price book®

Junio 2023

NP comunicaciones

Mesa de debate sobre ciberseguridad: la importancia del canal

Ajoomal cumple 30 años en pleno crecimiento de la IA

Primer seguro de ataque ransomware por NetApp

Apuesta por la conectividad y la videovigilancia de EET Europarts

TD Synnex Explora vuelve a los escenarios

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

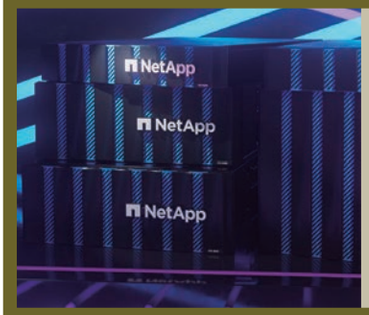
Eduardo Navarro
Director de Marketing y Ventas
eduardo@taipricebook.es

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



Mesa de debate: Ciberseguridad 2023

Celebramos la primera mesa de debate del año sobre ciberseguridad, un tema candente y transversal en toda la transformación digital de las empresas, y que requiere un acercamiento integral y colaborativo entre distintas soluciones y actores del mercado TI. Para poner en perspectiva su vital importancia, contamos con la participación de portavoces de Fortinet, Barracuda, Samsung y Bitdefender que nos van a ayudar a alumbrar el camino salvo.

EN ESTE mundo digital también prevalecen las leyes darwinistas donde no sobrevive el más poderoso, sino el que se adapta mejor a los cambios. Y a la velocidad en que se desarrollan las tecnologías es muy difícil hacerlo sin la cooperación del ecosistema. Fabricantes, distribuidores, integradores, administradores… todos añaden una capa extra que refuerza el resultado final: disponer de unos sistemas informáticos seguros y a prueba de fallos. Y en el peor de los casos, tener las herramientas de defensa, remediación y recuperación más idóneas, porque como en toda jungla, sea de noche o de día, son muchos los ojos que acechan.

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: Guillermo Sato, Channel Manager de Fortinet; Miguel López, Country Manager de Barracuda; Isabel López, Workplace Security de Samsung; y Luis Fisas, Regional Director South Europe de Bitdefender. Y sin más preámbulos, esto es lo que dio de sí la amena conversación.

Panorama actual

Hechas las presentaciones, vamos a hablar del panorama actual. Me gustaría que me dijerais qué ha cambiado desde la pandemia y un poco hacer balance de lo que llevamos de año.

Fortinet: La ciberseguridad va disparada. La previsión de negocio se cifra entorno a los 220.000 millones de dólares, lo que supone un crecimiento de más de un 12%. En realidad, no he visto un crecimiento del mercado inferior al 10% en estos últimos años. Responde a que hay una concienciación real en buena parte del mercado. Todavía tenemos en la memoria la víspera de San Isidro de 2017, estamos muy cerquita de Telefónica, oímos unas sirenas y resulta que estaban mandando a la gente a casa por el ataque de WannaCry. Yo creo que ese incidente marcó un antes y un después, más que la pandemia, el día siguiente amanecimos con todas las portadas hablando de ataque, terrorismo cibernético, ransomware y demás. Y a partir de aquí la ciberseguridad pasó de ser considerada de un gasto secundario a un tema crítico para el negocio, no solo porque puedan parar la producción, sino que tiene un impacto tremendo en la imagen corporativa.

La pandemia también favoreció la explosión del negocio en la nube. Y sabemos que cada nube pues tiene su forma de trabajar y sus peculiaridades. En especial respecto a las políticas de responsabilidad compartida, donde al final pues todo lo que subimos hay que securizarlo y de todo esto no se va a encargar el cloud provider. Se está creando una serie de negocio añadido en todo lo que es riesgo industrial

IT/OT considerado infraestructura crítica y en la adecuación a todas las normativas y regulaciones nuevas como son el NIST o la PSD2, donde se contemplan no solo las compañías de energía, agua y demás, sino también cualquier organización que pueda ser relevante de cara al día a día de la ciudadanía, incluido las administraciones públicas, pues ahora mismo tienen ya que contemplar el protegerse.

Barracuda: El balance de lo que va de año sigue lo visto en los años anteriores: una evolución al alza bastante notable de prácticamente todas las tipologías de ataques. Se está dando una tormenta perfecta, en el sentido de que confluyen múltiples factores que al final alimentan este fenómeno. Por un lado, hemos visto cómo tras la pandemia el teletrabajo, si bien no se ha mantenido a los mismos niveles, ha forzado a la implementación de nuevos elementos, pero también ha creado nuevos vectores de ataque. Por otro lado, la adopción de entornos de nube basados en SaaS que ya existía antes de la pandemia se ha acelerado, y como consecuencia al final todo esto da lugar a la desaparición del perímetro tradicional. Es decir, sigue existiendo, pero ahora está mucho más difuminado y podríamos decir que básicamente el propio usuario ahora es el perímetro.

Otros elementos causantes de esta tormenta perfecta sería la gran cantidad de conflictos internacionales. En Europa tenemos muy patente Ucrania, pero realmente hay tensiones en todo el mundo y al final pues esto genera que exista un nivel de ataques más alto que hace unos años. Por otro lado, la industria del malware, que ha conseguido grandes beneficios fundamentalmente, pero no exclusivamente, con el ransomware, tiene una potencia más devastadora. Y es que es eso, una industria económica, probablemente a la misma altura ya que el tráfico de armas o de droga. Todo esto está dando lugar a la necesidad de abordar la ciberseguridad no solo como una cuestión de mantener la competitividad, sino de supervivencia. Sin las inversiones adecuadas, va a ser muy difícil mantener la operativa tras un ataque, y no desaparecer ante las que sí han tomado medidas de protección. Está calando en el mercado la necesidad de protegerse adecuadamente y aceptando la ciberseguridad como un elemento estratégico.

Samsung: La irrupción de la pandemia supuso que muchas compañías tuvieran que trabajar a contrarreloj para dotarse de una infraestructura para operar desde casa de manera casi obligada y sin planificación. Ya durante 2022 y más en 2023 se han ido acomodando, quedándose con lo que funciona para un puesto híbrido entre la oficina y el teletrabajo. El balance ha sido bueno en lo que respecta a la aceleración de la digitalización de las empresas, pero también ha aumentado la preocupación por el despliegue de servicios para proteger los entornos corporativos extendidos. En telefonía móvil Samsung ha concentrado sus esfuerzos desde la fase de diseño de sus terminales a través de su plataforma Knox, que permite que se implementen toda una serie de servicios MDM, no se venden tanto como servicios de ciberseguridad en sí mismos sino como políticas de administración que se pueden considerar que añaden seguridad: accesos, control de contraseñas, despliegues, encriptación, listas blancas o negras. Las empresas apuestan por la automatización, y añadir seguridad por configuración igual que ya se hace seguridad por diseño en la fabricación.

Bitdefender: La explosión del WannaCry produjo una llamada de atención, pues solo nos acordamos de Santa Bárbara cuando truena. Ello supuso un antes y un después, pero seguimos detectándolo, a pesar de estar resuelto como malware, debió ser que al detenerse al grupo hacker se les olvidó apagar el servidor y sigue por ahí circulando, lo cual no deja de ser un riesgo para parques antiguos, aún se ve mucho Windows XP. Falta un poco más de cultura cibernética, se trata más bien de un hábito como el de la higiene, pero la seguridad y la comodidad no suelen ir de la mano.

Desde una perspectiva global, este sector TI tiene un fuerte crecimiento de doble dígito y no solo de 10 sino más, y de tres veces o de cuatro. A pesar de un crecimiento grande y sostenido, siempre queda mucho por hacer. Los más concienciados prometen un equipo TI dedicado, pero la mayoría de las pymes no tienen suficientes recursos, y la última línea de defensa del perímetro somos nosotros. Hemos pasado de empresas castillo donde teníamos muy claro dónde estaba el perímetro a empresas aeropuerto donde entramos y salimos con paquetes y maletines que habría que inspeccionar, y el tráfico está solo cifrado en el 80%.

Me sorprende compañías que aún no tienen planes de contingencia, y donde se invierte más en limpiar ventanas que en prevención. Y vemos nuevos vectores de ataque al terminal telefónico donde el phishing tiene muchísimo éxito, y como tendencia general atacar a través del cloud a los "aeropuertos" que ya no está ni en tu ciudad, están en otros países.

¿A qué han que tener miedo las empresas? ¿Y cuál sería la receta para protegerse?

Fortinet: Formación y concienciación es fundamental y ha mejorado bastante, pero queda mucho por hacer. Hemos abierto la plataforma de formación no solo a partners y canal sino también a clientes finales a nivel corporativo y de administraciones públicas. Muchos piensan que no son target de nadie, pero cualquiera puede ser diana. Una buena estrategia pasa por una detección lo más temprana posible y capacidad de reacción, adelantarse antes de sufrir el ataque. Y luego un plan de reacción para paliar lo que está ocurriendo. Para ello hay que tener claro qué infraestructuras y aplicaciones tengo para saber qué mirar. Qué hay publicado sobre mis vulnerabilidades abiertas, incluso poner señuelos que emulen mis entornos SAP u otros para ver cómo se me ataca y se mueven dentro del sistema para estar preparados, esto es muy novedoso.

Barracuda: Más que miedo, diría respeto. Hay tal variedad de ataques y el perímetro tan difuminado que hay que ser capaces de tener una estrategia lo más completa posible centrada en los principales vectores de ataque. Aparte de formación en seguridad, es crítico que empresas y administraciones públicas se lo tomen en serio para poder tomar sus propias decisiones en materia de ciberseguridad de la forma más informada posible. Y para ello se necesita, por supuesto, también presupuesto.

Samsung: Quitaría lo de miedo también, más bien respeto a lo que no tenemos conocimiento que está ocurriendo. Hay que controlar la información que hay dentro del teléfono y dónde están los activos de la empresa como móviles y portátiles. Cualquier fuga de información, a veces no intencionada, puede acarrear un uso no legítimo. Hay que tener ciertas prácticas de seguridad y poder bloquear que se puedan instalar aplicaciones no aconsejables, y el Whatsapp pues como que no es para un móvil de empresa. Hay soluciones que nos van a dar ese conocimiento del uso que se le está dando a estas herramientas de trabajo para poder de alguna forma evitar ese comportamiento, digamos anómalo.

Bitdefender: Miedo no, pero ser conscientes del peligro sin entrar en el pánico: como tener un velero con buena mar pero sabiendo que los tiburones están ahí abajo. Por eso, dotarte de herramientas de detección y mucha formación, más algunas prácticas que ya conocemos: segmentar la red, controlar el perímetro, doble autenticación, declarar la identidad… Pero sobre

todo contratar buenos partners profesionales que conozcan la materia, que sepan hacer una buena implantación y una buena configuración.

«Una buena estrategia pasa por una detección lo más temprana posible y adelantarse antes de sufrir el ataque. Y luego un plan de reacción para paliar lo que está ocurriendo. Pero muy pocas pymes pueden disponer de un responsable TI, y en este sentido el canal puede velar por su ciberseguridad de manera gestionada» (Guillermo Sato, Fortinet)

Fondos NextGen

¿Están funcionando? ¿A qué tipo de perfil van dirigidos?

Fortinet: Todo ayuda, estos fondos ponen foco en la recuperación y resiliencia y sí que incentiva, al final hay varias formas de aprovecharlo. Una parte se dedica a la adquisición o fortalecimiento de ciberestructuras, otra parte a impulsar formación sobre la misma pues requiere conocimientos muy específicos, y hay otra parte para desarrollar soluciones innovadoras que otorguen más resistencia para las pymes. Pero la realidad que vemos es que está llegando más lento de lo que querríamos, y al final las pequeñas empresas optan por lo más rápido y no siempre es lo más efectivo.

Barracuda: Lo cierto es que suman y están suponiendo un avance de las administraciones más punteras en su atención a los ciudadanos y estos fondos suponen un primer paso positivo. Sin embargo la manera de ejecutarlos es muy mejorable, las pymes pequeñas no pueden con los trámites, esto genera retrasos que impactan negativamente al tener que postergar compras de ciberseguridad a tener un presupuesto asignado y entre tanto se quedan desprotegidas. Se podría articular de otras maneras que agilice la burocracia y mirando también a más largo plazo, porque a muchas pymes se le genera inquietudes sobre si van a poder mantener y actualizar su solución en años siguientes.

Samsung: Estas ayudas están más dirigidas a la pyme que a la gran empresa, pero hay áreas de mejora. Hay mucho desconocimiento sobre qué le van a aportar y los que sí están concienciados preguntan por para cuando termine la ayuda qué va a pasar. Necesitan un partner que les guíe, pero si no tienen presupuesto para seguir y nadie asume este coste, elegir entre aumentar y proteger o reducir y no invertir, lo tienen claro. Se quedan como están.

Bitdefender: Bueno, nosotros como construimos un producto que es una plataforma software que tanto sirve para 20 usuarios como para 200.000, vemos un abanico de escenarios muy diferente. A priori muy positivo, se trata de una partida enorme para el desarrollo, un golpe de efecto muy bueno que ha generado expectativas muy altas… con resultados decepcionantes, mucha burocracia y se ha perdido bastante tiempo. Sólo en las administraciones públicas sí ha funcionado, a la pyme ha llegado poco, y muchos agentes del kit digital han tirado la toalla decepcionados, han instalado y no cobran.

¿Cómo sería un presupuesto idóneo, en función de la facturación o el número de empleados?

Fortinet: Cada compañía tiene una situación con distintos riesgos como para sacar un baremo único. Un 5% de la facturación podría ser razonable en una grande, pero inasumible en una pyme. Y 1.500 dólares por empleado estarían bien gastados, si también se analizan y contemplan los riesgos y la formación. Otro tipo de empresas que conlleve infraestructuras críticas por normativa van a necesitar un nivel más alto, al margen de facturación o plantilla. Según el panorama de amenazas y a lo que se dedique, estas pautas son solo orientativas y hay que evaluar una a una, según consecuencias financieras y reputacionales. Por eso debe ser vista como una inversión estratégica, y no un gasto, e ir ampliando y mejorando todos los vectores de ataque paso a paso.

Barracuda: Yo respondo a la gallega, no existe un porcentaje mágico, todo va a depender de qué grado de exposición, qué tipo de actividad y en qué ámbito se mueva, cómo de sensible es su negocio, de "qué pasaría si". Una vez valoremos los riesgos que estamos corriendo y el impacto económico que implican, podemos tener una correcta visibilidad del nivel de inversión que debemos tener. Hay buenas prácticas que indican porcentajes de 3, 5, 7 o 10%. Yo pondría atención al si…, e integrarla como un elemento más productivo, no como un gasto sino una inversión para no perder competitividad, nadie quiere trabajar con una empresa que no sea segura. Y no es solo importante la cantidad de dinero que se dedique, sino lo bien gestionado que esté ese dinero, tener una estrategia a largo plazo y coger y planificar esa inversión para aquilatar costes. Una fórmula sería unificar con una única plataforma y consola de control la mayor cantidad de vectores, y apoyarnos en los partners adecuados, porque precisamente los servicios que proporcionen son lo que marque la diferencia.

Samsung: Muy en línea con estos mensajes, no podemos decir lo que cuesta tener seguras las infraestructuras. No es lo que cuesta la ciberseguridad, es cuánto cuesta tu compañía, tus activos, o que acabes cerrando porque has tenido un ataque. Y visto desde otro ángulo, qué te supone tener la administración automatizada. Ahí hay un ahorro en la gestión de terminales cuando trabajas con herramientas adecuadas y la configuración correcta, no solo en personal TI que lo tuvieran que hacer manualmente, sino en evitarte fallos. No es una cifra concreta, sino ver la automatización como un ahorro de costes.

Guillermo Sato, Channel Manager de Fortinet.

Bitdefender: No voy a contestar ni a la gallega ni a la catalana, porque entonces me va a parecer mucho dinero y ya tengo la excusa para no gastar. Los escenarios son muy variopintos, no es lo mismo un taller mecánico de 35 empleados con cinco ordenadores, que un bufete de abogados con 35. Pero ambos piensan que el software debería ser gratis, y luego tienes teléfonos de más de mil euros. Pero me voy a mojar: está claro que hay un abanico de soluciones y de precio desde un antivirus para endpoint con una protección muy sencilla has-

ta un MDR como servicio gestionado, pero una solución básica, nosotros lo podemos ofrecer por 3 euros al mes por usuario. Y aquel que no puede invertir una caña o dos cafés al mes en estar protegida su tienda es un irresponsable que se merece lo que le pase.

Es decir, que no hay excusas. Habrá que adecuarse a cada entorno, a cada empresa y preguntarse si esto es suficiente para mí y hemos de poner más medios detrás. Pero en cualquier caso, y ya para acabar, totalmente de acuerdo en que se doten de un buen partner que sea capaz de hacer la instalación, la configuración, porque al final esto es lo que va a resultar en la eficacia de la herramienta que se está dando.

Modelo de go-to-market

Contadme cómo es vuestra estructura de canal y si estáis apostando por los modelos de pago por uso o si es por venta de licencias…

Fortinet: Nuestra aproximación es 100% canal, donde estamos creciendo bastante en los últimos años en volumen y tamaño. Nuestros comerciales están para dar a conocer las soluciones, para posicionarlas en el mercado, para entender las necesidades de los clientes e identificar esas oportunidades donde poder ayudar al canal, pero nunca para hacer ningún tipo de venta en directo, solo dando valor a la acción comercial. Tenemos lo mejor de los dos mundos: los equipos de hardware son importantes en el Edge, pero también tenemos ese acercamiento como plataforma que permite la convergencia de las redes y la ciberseguridad. Concentramos en un mismo equipo SD-WAN esta gestión inteligente de líneas y enlaces y la gestión del cortafuegos, y así más de 50 productos en el portfolio de manera integrada en un único portal. El producto core está disponible tanto en los marketplace de los cloud providers como por supuesto en modelo licencia virtual y en SaaS, que es un tema fundamental pues al final la escasez de recursos técnicos en torno a la ciberseguridad es brutal. Muy pocas pymes pueden disponer de un responsable TI, y en este sentido el canal puede velar por su ciberseguridad de manera gestionada, tendencia muy creciente que se apoya en formatos de pago por uso, que les permite evitar una inversión importante de arranque y tener totalmente controlado su gasto a la que poder ir añadiendo servicios.

Barracuda: También 100% canal, todo el crecimiento y todas las actividades comerciales en 20 años ha sido siempre así, adaptándonos a todo lo que es el mundo cloud. Hemos sido probablemente uno de los primeros fabricantes en apostar por las nuevas modalidades de venta 'bring your own license', pero siempre desde el punto de vista del canal que va a ser el que despliegue esas licencias. También hemos implementado modelos de venta en el marketplace, pero apoyados de nuevo en el canal, de forma que vea recompensada su actividad.

Tenemos también adaptado desde hace ya varios años un modelo de licenciamiento que va parejo al tradicional, en el sentido de poder permitir la implementación para MSPs en modalidades de pago por uso, pago mensualizado, facturación a medida que se consume, etcétera. Hemos implementado también sistemas de facturación y de ayuda, digamos, a canales basados, por ejemplo, en XDR, donde proporcionamos todo el servicio de monitorización, gestión, atención, soporte y actuación directamente, también en una modalidad de pago por uso desde nuestro SOC, siempre implementando y adaptando nuevas modalidades que van surgiendo, porque el mercado es dinámico.

Miguel López Calleja, Country Manager de Barracuda.

Samsung: También vendemos a través del canal y a través de los operadores. Tenemos un programa muy potente con solo unos 400 partners, premiamos la calidad frente a la cantidad. Tenemos planes Platinum, Gold, Silver y Register con una serie de beneficios según la categoría, y ahí sí que destacamos la cercanía con nuestros socios y su apuesta y confianza por nuestras soluciones. Les apoyamos en formación para que se certifiquen y puedan dar ese buen servicio. Como tenemos distintos productos, tenemos distintos tipos de licencia: licencias que van por dispositivo para cubrir sus necesidades y licencias también colectivas que llamamos por asiento, por ejemplo, una licencia para cubrir cien asientos, cien terminales configurados hoy, y si el mes que viene se quitan diez, pues esa licencia libera esos diez asientos; tenemos luego licencias mensuales, anuales, bianuales, incluso para tres o cuatro años, hay proyectos que se dilatan; licencias para cubrir toda la vida del terminal…

«SASE va a ser uno de los grandes caballos de batalla de los próximos años. Cada vez se va a embeber más tecnología AI/ML dentro de esta aproximación porque es el futuro, es una respuesta a la problemática de la desaparición del perímetro que obviamente tiene que ser multivectorial soportada por una única plataforma» (Miguel López, Barracuda)

Bitdefender: Somos increíblemente flexibles y aunque el software se ha vendido por licencias con un periodo anual, también lo tenemos a dos años, tres años o con lo que haga falta. Pero lo cierto es que el mundo ha ido cambiando y el modelo MSP creciendo, y hoy por hoy, diría que es una tendencia absolutamente clara, pues tenemos más partners que compran el modelo MSP que el tradicional. Es cierto que el modelo tradicional de licencias anuales o más quizá está más concentrado en la Administración y la gran empresa, mientras que el modelo MSP tiene más predicamento entre los partners que venden a la mediana y pequeña.

El modelo MSP que se adapta perfectamente a nuestra consola superflexible. Pagamos o proporcionamos licencias mensuales y el cliente solo paga el mes que lo usa y puede dar de alta una o 153 cuentas este mes y el mes que viene 14 y el mes que viene dar de baja 14 o 17. La consola es exactamente la misma en cualquier forma de pago, y esto el partner lo aprecia porque puede añadir esta oferta a sus servicios que son cada vez más importantes.

Bitdefender BUSINESS SOLUTIONS | Cybersecurity Built For Resilience

La agilidad en una organización se puede entrenar.

La Ciberresiliencia hay que construirla.

Te podemos ayudar.

bitdefender.com

App Store Google Play

Servicios gestionados, un must

Cómo integráis la figura del MSSP en vuestra oferta... no sé si tenéis algo ideado también en forma de prestarle el equipo, de pagarlo en leasing...

Fortinet: Dentro del programa de canal también tenemos tres líneas distintas: Una que llamamos Integrador, que es la tradicional, la reventa, donde el partner gana su margen en el propio margen de la operación más los servicios de implantación o integración. Pero hay otras dos vertientes, una que es Cloud para toda la parte de la suite de soluciones para securizar movimientos de las cargas y los aplicativos en la nube más toda la parte de desarrollo, y otra que es precisamente los MSP. Aquí tenemos prácticamente la totalidad de los productos en formato pago por uso, es fundamental dar esta flexibilidad absoluta según sea lo que se esté consumiendo, esto le permite montar una serie de servicios controlando lo que son sus costes para montar su propuesta de valor.

La mediana o gran empresa sigue teniendo proyectos más quizás on-prem o dedicados, o de otro tipo de acercamiento, pero el MSSP igualmente se está implantando y creciendo a un ritmo tremendo, sobre todo en torno a la pequeña empresa, y en el caso de España también la mediana, donde al final no son capaces de afrontar la ciberseguridad, por su complejidad, por la falta de recursos cualificados. El canal debe aprovecharse de esta situación, y de los 700 partners activos prácticamente todos están dando algún servicio gestionado, entendiendo por ello una gestión remota de algún tipo de appliance o componente de seguridad. Aquí es muy interesante un formato donde al final le permite flexibilidad para activar o desactivar cualquier tipo de funcionalidad tanto en volumen como en profundidad, y a mes vencido qué es lo que se ha utilizado y en base a esto se va a pagar. Esto es clave de cara al canal de MSSP, puesto que cubre prácticamente la totalidad de los vectores de ataque.

Barracuda: El formato de negocio MSSP ha venido para quedarse y realmente es una de las opciones de funcionamiento para el canal más interesantes a día de hoy, fundamentalmente en entornos de pequeña y mediana cuenta. Esto lo vimos claro hace ya varios años, de hecho la forma que tenemos de afrontarlo es diferente a otros fabricantes porque no es simplemente que tengamos una modalidad de partnership para MSP, sino que directamente lo que hemos constituido es una filial de la compañía, que

Isabel López Peral, Workplace Security de Samsung.

es Barracuda MSP, que tiene un funcionamiento independiente para dotar a estos partners de todas las herramientas que necesitan basadas, por un lado, en las tecnologías dentro de Barracuda Core, en la línea de productos tradicionales, por decirlo así, pero además cuentan también con herramientas específicas que son exclusivas de Barracuda MSP y que ayudan a estos partners a proporcionar servicios, que incluso son interoperables con terceros. Por ejemplo, nuestro XDR está pensado para que nuestro SOC pueda dar el servicio a partners que carecen de esas capacidades. Pero además, podemos estar monitorizando perfectamente un endpoint de Bitdefender, un firewall de Fortinet o de cualquier otro, donde al final lo que vamos a darle es la capacidad a los partners de proporcionar un servicio de gran valor añadido, como es todo XDR, y cada partner ver su billing. Lo que hemos hecho es precisamente crear una compañía que se adapte a las necesidades de estos MSP en lugar de tratar de adaptar a los MSP a nuestras características.

«Tener la administración automatizada. Ahí hay un ahorro en la gestión de terminales cuando trabajas con herramientas adecuadas y la configuración correcta, no solo en personal TI que lo tuvieran que hacer manualmente, sino en evitarte fallos» (Isabel López, Samsung)

Samsung: También hemos hecho un poco de MSSP para nuestros partners. Son quienes van a gestionarlo todo, pero cuentan con un canal directo para soporte, para contactar con nuestro equipo de ingenieros para cualquier incidencia. Y luego tienen guías técnicas de configuración de las distintas plataformas de los distintos servicios que tenemos, orientados también a verticales. Y también tenemos material de marketing que les va a ayudar a promocionar este tipo de servicios. Lleva un par de años pero el pasado se le dio un empuje importante, y ya varios partners tienen a todos sus clientes dentro de esta plataforma, y es este año cuando se está viendo el despegue.

Bitdefender: Como fabricante de software somos muy flexibles y tenemos mucha capacidad de desarrollo. Nuestro producto es el mismo, ya sea en la licencia tradicional o sea una licencia de MSP. El partner puede decidir centrar su negocio en hacer una oferta de servicios, una oferta de MSP o según la necesidad del cliente, una licencia tradicional. El mayorista la formación necesaria para un partner que tenga alguna duda. Nosotros nos centramos en que la consola sea fácil de utilizar, sea fácil de implementar, pero que a la vez sea eficaz y que el partner pueda construir su oferta MSSP, que es una tendencia absolutamente clara y ya estar aquí. Desde el momento en que los coches ya se venden así, ¿por qué no se va a vender la informática?

Programas de canal

¿Cuál es vuestro papel en relación con los mayoristas y los distribuidores? ¿Delegáis tareas o estáis muy encima de cada cosa que hacen?

Fortinet: Al trabajar 100% a través de canal, la labor de los mayoristas y distribuidores es fundamental. Nuestro modelo de negocio es 2 Tier. Tenemos dos mayoristas, Arrow y Exclusive Networks, y su labor es clave porque nos ayudan en todo lo que es la cadena de valor desde la captación de partners nuevos, hasta por supuesto su formación y capacitación, ofreciendo todo el apoyo que puedan necesitar a nivel acompañamiento en visitas, configuraciones y demás. Pero también a la hora de implementar servicios profesionales propios, sobre todo mientras este nuevo partner va cogiendo soltura. Tenemos más de 50 productos, y esto no es trivial. La punta de lanza es el firewall FortiGate, pero a partir de ahí hay todo un mundo muy amplio: tenemos SOAR de software, soluciones de EDR para endpoint, mail, cloud… Luego está toda la parte de acciones de generación de demanda y marketing que se llevan a cabo a través

SAMSUNG

Galaxy S23 Ultra

Lo último en rendimiento

Disfrute de un flujo de trabajo fluido con el chipset más potente de Samsung Galaxy

Lleva la productividad al siguiente nivel

El S Pen te permite realizar varias tareas con una sola mano

Seguro con Knox

Mantén tu negocio integramente seguro con nuestro sistema de seguridad integrado

Imagen alterada con fines ilustrativos.
La disponibilidad de funciones puede variar según país o región.
Es necesario la descarga de aplicaciones de terceros

«Falta cultura cibernética, se trata más bien de un hábito como el de la higiene, pero la seguridad y la comodidad no suelen ir de la mano, pues la última línea de defensa del perímetro somos nosotros. Hemos pasado de empresas castillo donde teníamos muy claro dónde estaba el perímetro a empresas aeropuerto donde entramos y salimos con paquetes y maletines» (Luis Fisas, Bitdefender)

de los distribuidores, vamos de la mano a la hora de planificar las necesidades del canal, qué tipo de formación, soporte a nivel de implantación, acompañamiento en marketing y demás requerimientos que puedan necesitar cada uno de los partners. En este sentido, buscamos una especialización de los mismos y es una apuesta conjunta con el mayorista. Es un trabajo de equipo y estamos muy contentos con la labor que hacen.

Barracuda: Nuestra aproximación se basa fundamentalmente en asegurarnos de que el canal cuenta siempre con los conocimientos y la formación y con la experiencia necesaria para implementar nuestras soluciones con el grado suficiente de garantía. Es decir, asegurarnos de que cuentan con el expertise para que la implementación sea exitosa. Y esto lo hacemos básicamente basándonos en dos partes. Por un lado, un modelo muy claro de certificación para los partners que les permite contar con la habilitación necesaria en función de la tecnología que vayan a implementar. Tenemos partners que se especializan en temas de Cloud y otros prefieren más en la parte de protección de correo o protección de red.

Y por otro lado, está el apoyo que podemos proporcionar, tanto desde nuestros recursos locales como fabricante, como desde los propios mayoristas con las herramientas de identificación y protección de oportunidades. A un partner que identifique y registre primero una oportunidad o que tienen presencia en un determinado proyecto incluso si existe un RPC o algún tipo de concurso público siempre le vamos a dar toda la ayuda necesaria, con todos los recursos preventa que necesite para desarrollar el proyecto de manera exitosa, también durante el lanzamiento. Y eso tanto si estamos hablando de un proyecto de diez usuarios como si son 100.000, la única diferencia es que desde el fabricante vamos a aquellos proyectos que tengan, digamos, un grado de complejidad más alto, y va a ser el mayorista el que se encargué de apoyar aquellos otros proyectos donde nuestra presencia no sea tan necesaria.

Entendemos que esta es la manera de que realmente el cliente tenga implementada una solución que cuente con el valor añadido necesario. Si al final todo se convierte en una pura disputa de precios, de a ver quién es capaz de vender más barato, probablemente las ventajas para el cliente de contar con un valor añadido por parte del canal se van a ver muy diluidas.

Samsung: Por nuestra parte, el papel del mayorista, igual, es súper importante. Nuestros mayoristas principales son TD Synnex (la anterior Tech Data), Ingram Micro, Esprinet y MCR, porque lo que intentamos es que haya una relación bastante cercana con cualquier tipo de partner. Tenemos un programa de Business Academy, donde tanto mayoristas como los partners tienen que pasar unos mínimos para estar certificados en las soluciones que comercializan, y depende del grado de certificación que tengan van a llegar a una gestión completa o simplemente no aplicar tal servicio.

Luis Fisas, Regional Director South Europe de Bitdefender.

Por otro lado, se crea un portafolio atendiendo a las necesidades de sus clientes, porque hay revendedores enfocados en verticales donde cada uno tiene su propio portafolio. Mientras los mayoristas se ocupan de todos los procesos de logística, los servicios de consultoría suele ser del integrador, pero la idea es dar al cliente final un buen producto y un servicio de calidad.

Bitdefender: Trabajamos a través del canal de distribución, es decir, mayoristas y partners. Nuestros mayoristas que son Aryan, Ingecom y Esprinet V-Valley, los tres ofrecen las soluciones en modelo tradicional, licencia anual o MSP, y luego tenemos dos mayoristas específicos para MSP, que son Reditelsa y Speed PC. Con esto, cubrimos más que suficiente todo el territorio nacional y Portugal, y los partners trabajan a través de los mayoristas. Como casi todos los programas de canal, está dividido en Gold, Silver y Registers, y nos dedicamos a atender sobre todo a los dos primeros mientras los Registers quedan más en manos de los mayoristas.

La formación es muy importante, disponemos de herramientas virtuales de eLearning y sí que somos exigentes, la formación es clave. Es muy difícil vender aquello que uno no conoce. Y sobre todo, aquellos partners que están bien formados estadísticamente siempre venden un 25% más que todos los demás. Hay que estar continuamente insistiendo en la formación, sobre todo en nuestro campo en ciberseguridad, donde todo cambia y hay que estar permanentemente al día. Ahí, el mayorista también cumple su función y en ello estamos, somos una empresa dedicada al canal, por y para el canal.

Tendencias

Muy bien, pues ya solo queda ver un poco las tendencias de aquí a dos años.

Samsung: Pues seguiremos trabajando el equipo de I+D en línea a los ciberataques para cubrir nuevos requerimientos y esas mejoras que día a día nos están demandando, sobre todo en telefonía móvil, Como un ejemplo, una reunión reciente con un cliente de hostelería que nos pedía el poder activar las llamadas de reservas automáticamente y saber cuándo Internet se caía, por qué se había caído. Siempre escuchamos sus necesidades, lanzamos parches de seguridad y versiones de mantenimiento para protegerlos ante aquellas nuevas vulnerabilidades para sacar un producto cada vez más robusto. Hay que resignarse a que los ataques van a seguir

The Fortinet Security Fabric is the industry's highest-performing cybersecurity mesh platform. Delivering broad, integrated, and automated cybersecurity capabilities supported by a large, open ecosystem makes cybersecurity mesh architectures a reality. The Fortinet Security Fabric empowers organizations to achieve secured digital acceleration outcomes by reducing complexity, streamlining operations, and increasing threat detection and response capabilities. **Learn more at fortinet.com**

FORTINET | ARROW

creciendo, de ahí la necesidad de estar siempre actualizados y protegidos.

Fortinet: Es complicado, porque al final estamos en un mundo imparable tan cambiante que evoluciona muy rápido. Hay determinadas tecnologías o "siglas" que han ganado mucha relevancia en los últimos tiempos y que van a seguir estando ahí. Inteligencia Artificial y Machine Learning se están utilizando cada vez más para detectar patrones de comportamiento anómalos, identificar amenazas, automatizar respuestas. Esto está muy bien porque al final nos permite reaccionar mejor y más rápido. Analítica de Big Data es otra realidad ante la generación masiva de datos, y las organizaciones necesitan cada vez más de técnicas avanzadas de análisis para sacar información relevante y detectar de una forma más rápida estas amenazas o ataques. Pero hay que tener en cuenta que los malos también tienen acceso a estas herramientas y no nos lo ponen nada fácil. Es decir, nosotros mejoramos, pero ellos también, y de seguro que invierten mucho más dinero y recursos que muchas empresas.

Otra realidad es la nube, al final vivimos en un mundo híbrido y el data center y toda la parte local se va a mantener, pero vamos cada vez más a tener partes de la empresa y aplicativos en multicloud, donde cada cloud provider es un mundo en sí. Y todo esto hay que securizarlo, pero ¿cómo ser capaz de gestionar esto de una forma eficiente y óptima si nos falta talento especializado? Añádase a todo ello temas como Internet de las Cosas, que está creciendo de forma exponencial, basado en dispositivos de todo tipo, que esto sí, en la mayoría de las ocasiones tienen una funcionalidad muy concreta, por lo que se buscan que sean baratos y normalmente nunca llevan la seguridad embebida dentro de su diseño. No tenemos en cuenta o no nos damos cuenta hasta qué punto todo esto es de accesible para los malos.

El panorama de la ciberseguridad es muy dinámico y tenemos que estar muy pendientes para ser capaz de reaccionar lo antes posible. Hay dos siglas que yo creo que son la piedra angular, y que van a seguir siéndolo de aquí a dos años, incluso mucho más. Gartner sacaba a principios del año pasado el concepto CSMA, CyberSecurity Mesh Architecture y la cuestión es ser capaces de tener un acercamiento como plataforma y no como soluciones únicas específicas de cada vector de ataque, puesto que esto dispara la complejidad, los costes operacionales y los recursos que tienen que estar formados en cada una de estas plataformas.

Gartner también a finales del año comenzó a hablar del single vendor SASE (Secure Access Service Edge), metiendo en la discusión que qué pasa con los equipos on-prem, físicos, si todo era la nube. Y yo creo que hay que ser capaces de gestionar la seguridad de un usuario, esté donde esté, dentro, fuera, en la nube, el aplicativo dentro, on-prem, en mi operator center en SaaS, de la forma más sencilla posible.

Barracuda: Incluso con la bola de cristal en la mano, es muy complicado, estamos en un mundo donde las novedades se suceden y ya no nos sorprenden. Vamos a seguir viendo ataques de ransomware tremendamente disruptores en muchos casos, pero esto ya casi que no es noticia. Vamos a seguir viendo ataques a la cadena de suministro de software, que como no se entiende muy bien a veces, pues quedan ahí un poco de soslayo. Vamos a seguir viendo ataques en entornos web. Vamos a ver cómo la inteligencia artificial se embebe cada vez más en las tecnologías de los atacantes.

Hace años que ya los fabricantes estamos incorporando tecnologías AI/ML en nuestras soluciones. De hecho, a día de hoy, es imposible contar con una plataforma de protección multivectorial si no se está implementando inteligencia artificial, pero es que los malos también lo están haciendo. Hemos visto hace unos días cómo se daban ataques donde se está suplantando a personas en un vídeo, en tiempo real, gracias a tecnologías de deep fake.

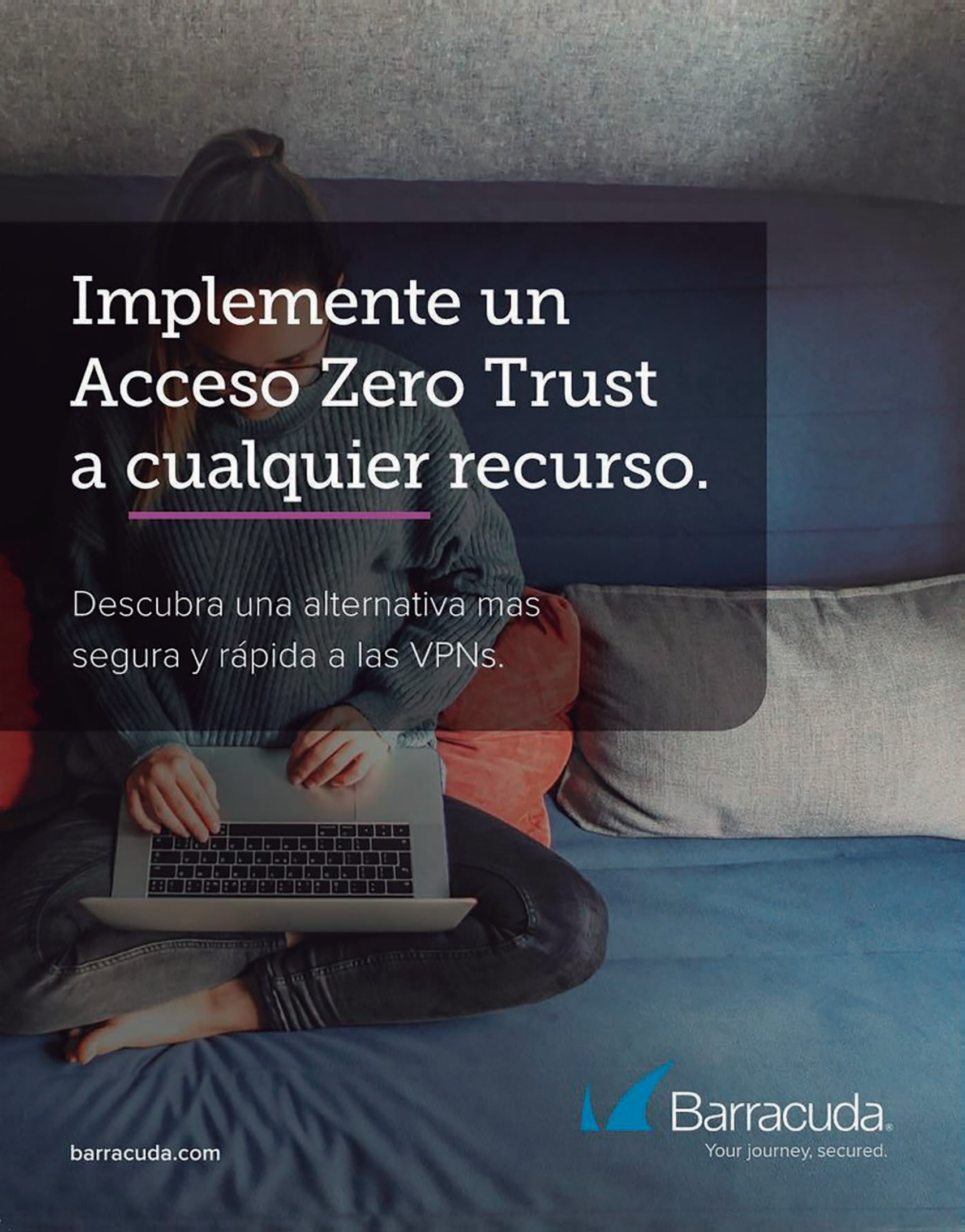
Sobre el tema de las siglas, creo que hay pocos sectores como el de la ciberseguridad donde nos guste tanto y podemos dar aquí una sopa de letras brutal. Pero el SASE sin duda va a ser uno de los grandes caballos de batalla de los próximos años. Cada vez se va a embeber más tecnología dentro de la aproximación de SASE porque es el futuro, es una respuesta a la problemática de la desaparición del perímetro que obviamente tiene que ser multivectorial, tiene que ser en un concepto de plataforma, tiene que ser simplificada y sencilla para que sea manejable y tiene que estar adaptada a los diferentes entornos que estamos viendo de Cloud, de entornos de movilidad, on-premise, de los de toda la vida, pero también con aplicaciones que corren en SaaS.

De cara a los próximos años, deberíamos tener en cuenta un escenario donde los ciberdelincuentes cuentan cada vez con más recursos, donde actores supranacionales o internacionales utilizan las tecnologías de ciberataques como una herramienta más de ciberguerra o de política exterior. En este escenario, yo creo que es muy importante no perderse en este mar de siglas, tener claro que hay que establecer una estrategia, apoyarse en el canal, porque es muy difícil que ningún cliente final pueda mantenerse al día de todo lo que está sucediendo.

Bitdefender: Si tuviera una bola de cristal y pudiera ver el futuro probablemente estaría en el Caribe tumbado en una hamaca. Sí que es verdad que en el mundo de la ciberseguridad tenemos esta afición a crear siglas. El otro día se me ocurrió meterme en Chat-GPT para que me diera un listado de acrónimos y sus significados, cuando ya iba por el 50% lo paré porque era una auténtica locura. Hay conceptos nuevos y esto va evolucionando e ideas que surgen hoy dentro de cinco años van a estar repensadas. Se ha mencionado SASE, pero habéis olvidado ZTNA (Zero Trust Network Access), aunque todo va en el mismo camino. ¿Por dónde van a venir las amenazas? Esa es la gran pregunta y creo que todos tenemos en mente AI/ML.

Los atacantes invierten casi un 80% de lo que recaudan en nuevas herramientas y están continuamente evolucionando. Entonces, hay que estar preparando herramientas que se preparen para detectar aquello que todavía no conocemos. Detectar lo desconocido por análisis de comportamiento, por análisis de despliegues más que por actividades muy concretas, que también. Y lo que sí que vemos, y que quizá haya que poner el acento ahí en el corto plazo, son las nuevas superficies de ataque. El perímetro desaparece, ya lo hemos dicho, somos empresas aeropuerto.

Y como siempre, formación, formación y formación. Quizá esta es la amenaza más grande que yo veo, la falta de personal especializado, no solo en España, en todo el mundo. Se habla que faltan 3 millones de ingenieros. Todos hablamos con partners que están continuamente preguntándonos "¿pero no tienes a alguien?", y que continuamente se están robando ingenieros de unos a otros. Esa yo creo que es la principal amenaza, que no mantengamos el nivel de conocimiento suficiente, no invertamos en personas, que la universidad no esté formando a la gente que necesitamos, porque por ahí es por donde van a entrar los problemas del sector y de la sociedad en general.


Implemente un
Acceso Zero Trust
a cualquier recurso.
Descubra una alternativa mas
segura y rápida a las VPNs.
barracuda.com
Barracuda
Your journey, secured.

Retos actuales de la Ciberseguridad empresarial

La digitalización acelerada de la mayoría de los procesos corporativos ha obligado a implementar nuevas soluciones tecnológicas, migrar ingentes cantidades de datos y actualizar los procesos y formas de trabajo de la mayor parte de la plantilla corporativa.

Simultáneamente, los nuevos modelos de trabajo híbrido y teletrabajo han complicado aún más el panorama de digitalización anteriormente comentado.

El resultado del solapamiento de ambos procesos, digitalización acelerada y teletrabajo sobrevenido, ha dado lugar a una especie de tormenta perfecta en lo que a ciberseguridad se refiere.

Ya antes de la pandemia era evidente que vivíamos un período de crecimiento desbocado en lo que a ciberataques se refiere. Raro era el día en el que no nos despertábamos con la noticia de una gran empresa o AAPP que había sido atacada exitosamente. En la actualidad muchos días son varias las entidades que han sido vulneradas, siendo estos ataques aún de mayor entidad y poniendo en jaque incluso gobiernos locales o nacionales.

Es preciso asumir, cuanto antes mejor, que la ciberseguridad es un elemento vital de la estructura productiva y de funcionamiento de cualquier empresa y AAPP hoy en día. Dotar al departamento de ciberseguridad de los recursos técnicos, económicos y humanos necesarios así como de un peso específico importante y crítico en la dirección corporativa es probablemente el elemento clave que diferenciará, en un futuro próximo, las entidades capaces de seguir creciendo y produciendo de aquellas que terminarán desapareciendo al no poder soportar las constantes pérdidas económicas y reputacionales que los sucesivos ciberataques les originan.

La inversión en herramientas de ciberseguridad que protejan los principales vectores de ataque debe incluir, por ejemplo:

- El correo electrónico; constituye a día de hoy probablemente la principal vía de entrada para los atacantes. Existen multitud de diferentes ataques (Phishing, Suplantación de identidad, Account Takeover,…) pero en los últimos tiempos destaca sobre todos ellos la utilización de herramientas de ransomware que en muchas ocasiones realizan una doble extorsión mediante la que el atacante, además de cifrar los datos, primero los extrae y amenaza no solo con el cifrado de esa información sino con la posibilidad de hacer públicos detalles sensibles si no se accede al pago del rescate. Solo la implementación de medidas de protección en el correo muy avanzadas y que incluyan técnicas de inteligencia artificial que se adelanten a las estrategias de los ciber-delincuentes pueden paliar estos ataques

- La navegación de los usuarios: esta es habitualmente la segunda principal vía de infección por malware en empresas y administraciones públicas. De nuevo son los usuarios los que, al navegar por páginas web que han podido ser infectadas con algún tipo de software malicioso, descargan a la red local dicho malware el cual se extiende por la infectando diferentes recursos. La mejor defensa en este caso es la implementación de políticas de filtrado en la navegación de los usuarios que les protejan frente a la entrada de software malicioso independientemente del dispositivo que estén utilizando para navegar.

- Los servicios web, APIs, aplicaciones móviles y la cadena de suministro de SW de la empresa: lo extraordinariamente peligroso y dañino de los ataques realizados con estas técnicas, así como su crecimiento exponencial en los últimos meses, sitúan esta categoría de ataque como una de las más importantes a tener en cuenta. Los “FW” o cortafuegos, incluso los de “Nueva Generación”, no son eficaces para protegernos frente a este tipo de amenazas. Sólo la implementación de soluciones “WAF” (Web Application Firewall) que incluyan tecnologías de Inteligencia Artificial pueden proporcionar un nivel de seguridad razonable en este caso.

- La mejora en la cualificación y concienciación en ciberseguridad del capital humano: un gran número de ataques utilizan estrategias basadas en ingeniería social. La implementación de herramientas de formación especializadas en ciberseguridad para la plantilla que contemplen tanto un programa organizado de formación en ciberseguridad como la posibilidad de realizar simulaciones de ataques que mantengan alerta a los empleados es imprescindible a día de hoy.

- Los accesos remotos: durante la pandemia se hizo necesario permitir el acceso remoto de los empleados a recursos que habitualmente solo eran accesibles desde dentro de la red corporativa. Es evidente que las VPNs no son capaces hoy día de dotar de un nivel de seguridad adecuado a estos accesos remotos, siendo mucho más conveniente implementar una estrategia de acceso basada en tecnologías Zero Trust

En definitiva, la inclusión de la ciberseguridad como un elemento estratégico clave en los planes corporativos, con una dotación presupuestaria y en recursos humanos suficiente, es la mejor herramienta para protegernos ante una oleada de ataques que, muy probablemente, sólo va a empeorar en un futuro próximo.

Miguel López
Country Manager Iberia – Barracuda Networks

Barracuda

www.barracuda.com

Por qué todas las empresas deberían invertir en seguridad por capas

Los ataques de seguridad pueden ocurrir en las empresas en muchas maneras diferentes. Hoy en día los ciberataques han aumentado y están en un desarrollo continuo con el objetivo de obtener acceso a datos y activos confidenciales. Las organizaciones necesitan más que una única solución para estar completamente protegidas y poder prevenir un ataque, defenderse de uno y recuperarse si se ven comprometidas.

La mejor manera de hacerlo es a través de la seguridad en capas, teniendo múltiples herramientas, sistemas y procesos que se superponen y brindan ciberseguridad preventiva y proactiva. Estas herramientas y sistemas deben informarse entre sí para crear un entorno más seguro.

Los malos actores se enfocan en la superficie de ataque, la parte específica de la TI de una empresa para comprometer y potencialmente entrar en la organización. Cuanto mayor sea la superficie de ataque, mayor será el riesgo en el que incurra una empresa y más tendrá que hacer una empresa para defenderla y protegerla.

En los últimos años, la superficie de ataque promedio ha aumentado en gran parte debido a que ha aumentado el alcance digital del entorno de una empresa, incluyendo:

- Puntos finales: computadoras portátiles, servidores, dispositivos de oficina, remotos o privados que se conectan a la red.
- El uso de la nube con herramientas como Office 365, Slack, Zoom y Google Drive.
- Los dispositivos de Internet de las cosas (IoT): pantallas inteligentes, refrigeradores, impresoras, cámaras, todos conectados a Internet y sin la mejor seguridad.
- Los empleados - el eslabón más débil, cada individuo puede representar un riesgo potencial.
- Múltiples ubicaciones/trabajadores domésticos/trabajadores híbridos requieren mayores medidas de seguridad.

Para tener en cuenta todos los puntos de entrada que ponen en riesgo una empresa, es importante crear una seguridad integral a través de una estrategia de ciberseguridad en capas que incorpore controles preventivos, acción proactiva, capacidades de detección y respuesta. Estos incluyen:

- *Visibilidad* en todo en el entorno puede ayudar a protegerlo.

- *Detección y respuesta de punto final* (EDR), que detecta amenazas y compromisos potenciales a nivel de punto final y proporciona información procesable a un equipo.

- *Detección y respuesta extendida* (XDR), que mira más allá del punto final e incorpora información de seguridad de otras fuentes, incluida la nube.

- *Endurecimiento*: la administración de parches, herramientas y controles de seguridad específicos, como seguridad de correo electrónico, filtros de correo no deseado, herramientas antivirus y cifrado de disco completo que protege los datos incluso si son robados y sacados de la red o de los servidores de una empresa.

- Seguridad en la nube. Las empresas deben tener formas de proteger y asegurar el software como Office 365, One Drive, Google Apps y más.

- *Respuesta*: La forma en la cual una empresa responde a un ataque potencial y lo que hace para prevenir un ataque, ayudar a eliminarlo y minimizar el daño que le puede causar. Incluye herramientas como EDR, XDR, así como detección y respuesta administradas o proveedores de seguridad administrada.

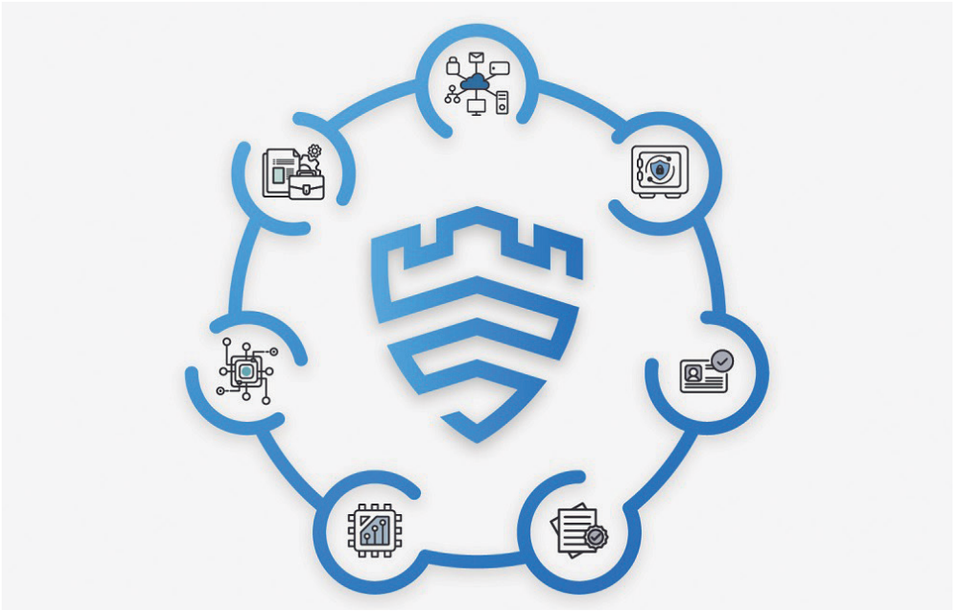
Crear un departamento de seguridad integral puede ser difícil porque requiere muchos recursos. Encontrar el talento y las herramientas adecuados puede ser una tarea casi imposible, por lo que debería considerar asociarse con un proveedor clave de ciberseguridad. Aprovechar los proveedores de detección y respuesta administrada (MDR) que incorporan EDR y XDR para una comprensión integral de su entorno de TI que puede ayudarlo a proteger mejor a la empresa contra ataques avanzados.

Las empresas también pueden considerar trabajar con un proveedor de servicios de seguridad administrados (MSSP) que puede actuar como un departamento de seguridad cibernética subcontratado. Estos proveedores pueden usar herramientas y tecnología y responder a las amenazas rápidamente para evitar que ocurran daños.

Luis FISAS,
Bitdefender Regional Sales Director Southern Europe

10 años de Samsung Knox (y seguimos avanzando en seguridad móvil)

Millones de consumidores y empresas es están protegidos en todo el mundo gracias a la plataforma de seguridad integral **Samsung Knox**. Knox permite reducir los riesgos del mundo hiperconectado gracias a una serie de mecanismos de defensa solapados que se incluyen en los dispositivos de Samsung.



Durante el proceso de fabricación de nuestros terminales, incorporamos la plataforma Knox en el hardware y en el sistema operativo. De esta forma, aseguramos la integridad del dispositivo en todo momento, desde su iniciación hasta la ejecución de tareas, para que los usuarios siempre puedan confiar en su smartphone o tablet, así como en cualquier aplicación o dato que se encuentre en él. Esta es una función diferenciadora, clave del modelo de seguridad de Samsung Knox, que se consigue realizando una serie de comprobaciones de seguridad de los componentes clave del sistema operativo.

Lo hacemos así porque como diseñadores o fabricantes de todos los componentes del dispositivo, tenemos la capacidad de crear el hardware y el software para que trabajen juntos tal como queremos que lo hagan. Además, la innovación forma parte de nuestro ADN, y más de un 25% de nuestra plantilla global se dedica a I+D. Continuamente avanzamos para resolver los desafíos en seguridad móvil, sobre todo en un momento donde los ciberataques son cada vez más sofisticados.

Sin ir más lejos, existen **más de 14 mil millones de dispositivos conectados en el mercado**, lo que demuestra que una mayor conectividad puede originar un mayor número de brechas y vulnerabilidades. Y por eso hemos diseñado **Knox Matrix**, nuestra visión de futuro donde los dispositivos conectados en un ecosistema pueden protegerse entre sí: cuantos más dispositivos estén conectados, más protegidos estarán en conjunto.

Knox Matrix es solo el último eslabón en la historia de Samsung Knox. En 2021 se anunciaba **Knox Vault**, una solución que aísla los datos más sensibles de los usuarios para protegerlos frente a posibles ataques. Anteriormente, se añadió TrustZone, que proporcionaba un entorno seguro dentro del sistema operativo principal para ejecutar aplicaciones y procesos sensibles de forma independiente con respecto al software.

Samsung Knox también evolucionó hacia **Knox Suite**, para ayudar a las empresas e instituciones de todo el mundo a implementar y administrar eficientemente su flota de dispositivos, con el objetivo de gestionar el software y las actualizaciones de seguridad de forma personalizada y sencilla.

Todas estas innovaciones se han visto validadas por múltiples agencias gubernamentales, que han otorgado sus recomendaciones para que Samsung Knox se utilice en el entorno empresarial. Las soluciones de gestión Knox Mobile Enrollment (KME), Knox Configure y Knox Efota han sido validadas por el Centro Criptológico Nacional en España, lo que garantiza que puedan ser implementadas en empresas y organismos públicos del Gobierno. De la misma forma, el CCN ha cualificado nuestros dispositivos Galaxy de la gama S y A, así como los plegables de la serie Z, nuestras tablets y los dispositivos rugerizados X Cover.

Durante este tiempo, la continua evolución de la plataforma ha sido un fuerte impulso para el crecimiento de los dispositivos Samsung en las empresas. Un informe de IDC revela que, desde el nacimiento de Samsung Knox en 2013, las organizaciones perciben el sistema Android de los dispositivos Samsung como una implementación segura y estable del sistema operativo de los teléfonos inteligentes.

Por eso estamos orgullosos de poder decir que Knox es una de las plataformas de seguridad más fiables del mundo gracias a sus altos niveles de seguridad y que está en la mejor posición para definir la próxima era de la seguridad de dispositivos.

SAMSUNG

https://www.samsungknox.com/

DAKEL

La **seguridad y gestión** de los endpoints no se pueden confiar a soluciones del pasado.

End User Computing (EUC)

IGEL WORKSPACE

Máxima seguridad en el endpoint

IGEL OS es la plataforma gestionada más segura para el endpoint con acceso a servicios cloud de VMware, Citrix, Microsoft y AWS. Es la evolución de la tecnología Thin client, optimizada para entornos VDI (Virtual Desktop Infraestructure), para proporcionar máxima seguridad en el endpoint.

CONTROL UP

Gestión 360º del endpoint

ControlUp es la plataforma de monitorización más potente para optimizar la experiencia digital de los usuarios, estén donde estén. Ofrece herramientas de control y remediación a nivel de usuario, aplicación y dispositivo, para garantizar la productividad del endpoint.

En Dakel proponemos ambas tecnologías como solución de EUC (End User Computing).
¿Quiere una **DEMO guiada**? dakel.com/solicitar-PoC/

IGEL | control UP | LG

La seguridad de las impresoras: una tarea pendiente que puede poner en riesgo a las empresas

La impresión es una de las tareas más comunes en cualquier empresa, y a menudo se subestima la importancia de su seguridad. Sin embargo, si no se toman las precauciones necesarias la impresión puede ser una puerta de entrada para los ciberdelincuentes que buscan infiltrarse en una red empresarial.

Según el último estudio de la firma de investigación de mercados **Quocirca**, realizado sobre una muestra de 531 responsables de TI en cuatro países, el 68% de las empresas han experimentado algún problema de seguridad relacionado con la impresión en 2022. Además, el estudio muestra que el 64% de las organizaciones no tiene ninguna política de seguridad para responder a este tipo de incidentes y sólo el 26% confían plenamente en la seguridad de su infraestructura de impresión.

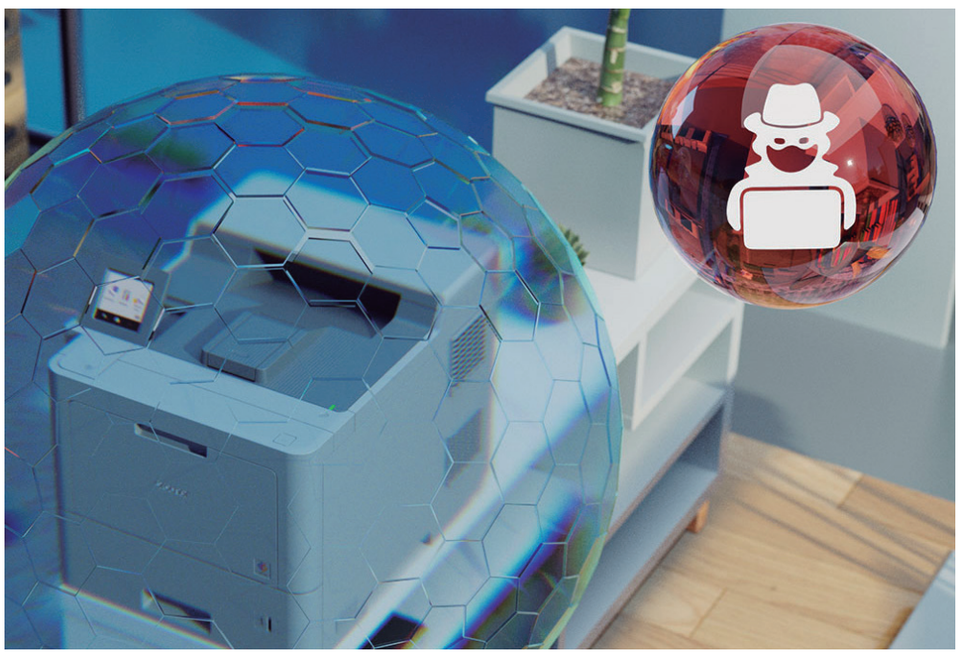
La falta de atención a la seguridad de la impresión puede resultar en una serie de riesgos de gran trascendencia para una empresa, pudiendo llegar incluso a la interrupción de su negocio.

La primera línea de defensa

Uno de los principales riesgos de seguridad asociados con la impresión es el robo de información, como por ejemplo, contratos, informes financieros y datos de los clientes. Los piratas informáticos pueden explotar vulnerabilidades en la red para acceder a las impresoras y robar esta información, al igual que pueden utilizarlas para lanzar ataques cibernéticos. Si estos documentos caen en manos equivocadas, pueden causar daños reputacionales muy significativos.

Además, la pérdida de datos confidenciales puede resultar en costosos pleitos y multas regulatorias. Según el mismo estudio de Quocirca, las pérdidas de datos relacionadas con la impresión supusieron un coste medio de más de 700.000 euros para las empresas.

Para protegerse contra el acceso no autorizado a las impresoras, las compañías deben implementar políticas de seguridad y medidas concretas tanto a nivel de red como de dispositivos y documentos.



Seguridad en tres capas: red, dispositivos y documentos

Una forma común de mejorar la seguridad de la impresión es implementando firewalls y sistemas de autenticación de usuario. Esto significa que los usuarios deben ingresar sus credenciales para imprimir un documento, lo que ayuda a prevenir que información confidencial caiga en las manos equivocadas. Este tipo de herramientas permiten también restringir ciertas funciones a usuarios específicos para evitar el mal uso de los dispositivos.

Además, las empresas pueden utilizar soluciones de gestión de impresión que permiten a los administradores de la red supervisar el uso de las impresoras y detectar cualquier actividad sospechosa. Estas soluciones pueden ayudar a identificar y mitigar cualquier riesgo de seguridad antes de que se convierta en un problema grave.

Como último aspecto importante, destacamos el cifrado. Los documentos confidenciales que se imprimen deben ser cifrados durante la transmisión para garantizar que no sean interceptados por ciberdelincuentes. Los dispositivos de impresión profesionales, más modernos, están equipados con esta capacidad y deben configurarse para que los trabajos de impresión se transmitan de forma segura.

No está de más recordar que mantener los dispositivos y softwares actualizados es prioritario, y no sólo para obtener su mejor rendimiento. Las actualizaciones a menudo incluyen correcciones de seguridad para vulnerabilidades conocidas.

Para conocer cómo Brother puede ayudar a mejorar la seguridad de las soluciones de impresión, tienes toda la información en **este enlace**.

brother
at your side

Las soluciones de impresión de Brother para empresas se han reforzado para adaptarse a cualquier entorno profesional que precise trabajar de forma segura y eficiente.

Este es el...

ESPACIO DE TRABAJO BY BROTHER

brother.es/espacio-trabajo-brother

Utilizar la robótica para evitar los cuellos de botella en los almacenes y mejorar el rendimiento de las empresas

Cuando hablamos de "cuello de botella", probablemente recordamos la imagen de 109 buques portacontenedores que estaban atascados frente a la costa del sur de California hace muy poco. Ese cuello de botella empezó en enero y tardó casi hasta finales de octubre de 2022 en resolverse; pero eso no significó su fin. Cuando los barcos salieron de los puertos de Los Ángeles y Long Beach apareció otro problema: todos los productos crearon un nuevo cuello de botella, esta vez en los almacenes.

ACTUALMENTE, LOS almacenes se pueden convertir en un obstáculo y, por tanto, es necesario conocer cuales son las soluciones para poder afrontar este reto y cómo pueden ayudar los robots móviles autónomos en todo el proceso para desbloquear la situación:

Problemas de almacenamiento

Siguiendo con el ejemplo anterior, los bienes y productos de los buques portacontenedores tenían un destino final, pero antes de llegar debían pasar por los almacenes que los encargaron en función de las necesidades del momento. Con los productos atrapados allí durante meses, la necesidad estacional ya había pasado para algunos de los artículos (piscina, jardinería, o suministros para la vuelta al cole). Como estos ya no eran de necesidad inmediata, los productos tuvieron que almacenarse hasta que volviera a haber demanda.

Tanto si se trata de existencias inesperadas por imprevistos, de devoluciones de temporada como las rebajas o navidad, o simplemente de material cotidiano que entra en el almacén, el mayor reto es el almacenamiento junto con la gestión de la circulación.

Muchos almacenes gestionan la entrada en stock almacenando cajas y palés hasta que se necesitan los productos. Pero esto no resuelve el problema del almacenamiento. Una forma de resolver los problemas relacionados con esto es contar con un sistema de entrada en el almacén eficaz, que puede incluir flotas completas de robots móviles autónomos para el transporte. Estos robots tendrían una verdadera funcionalidad de intercalación de tareas, lo que ayudaría a los almacenes a maximizar la productividad mediante la preparación simultánea de pedidos, la gestión de devoluciones y la reposición del espacio de picking utilizando la misma tecnología robótica.

La preparación de pedidos es uno de los aspectos de la integración de tareas y los AMR facilitan el proceso a los empleados de su almacén al evitarles tener que caminar kilómetros cada día llevando paquetes pesados. El proceso de entrada en un almacén es el siguiente:

1. Los palés y las cajas de productos llegan en un camión al muelle de un almacén.
2. Los operarios escanean y descargan los palés y las cajas en una cinta transportadora que sale del muelle y entra en él.
3. Los trabajadores cargan las cajas y los palés en los robots móviles autónomos que puedan transportar hasta 1.000 kg.

4. Estos llevan el material a los empleados del almacén, que sacan los productos y los guardan, dejando el embalaje sobrante en el AMR.
5. A continuación, los AMR dejan el material en el compactador de basura y se dirigen de nuevo al muelle de camiones para recoger más material y almacenarlo.

Automatización flexible para todo tipo de infraestructuras

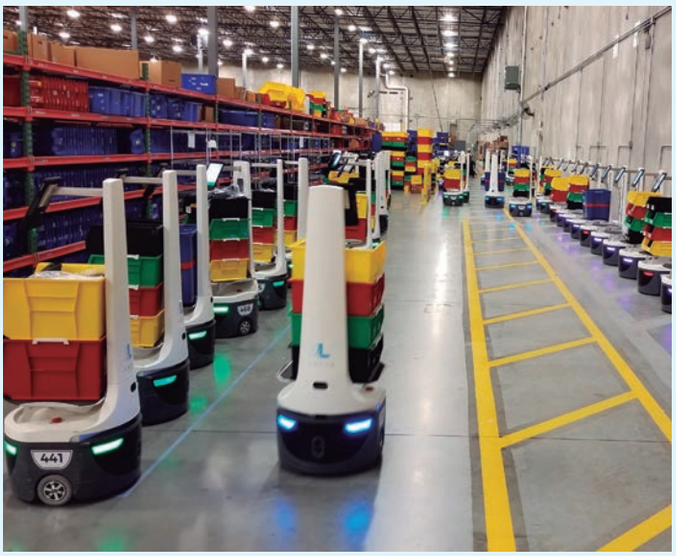
Si el espacio de almacenamiento también es un problema en el almacén y hay más productos entrando que saliendo, hay varias opciones. La primera es trasladarse a una nueva ubicación con más metros cuadrados, pero eso no siempre es factible. Otra opción es adoptar la verticalidad y crear niveles de entreplanta automatizados.

La mejor práctica para las entreplantas de almacén es disponer de automatización coordinada; para cada pedido, por ejemplo, puede haber pickings que deban completarse en tres niveles diferentes. Con la solución adecuada, el sistema gestiona y optimiza el proceso de picking y reparto sin problemas en todos los niveles.

En definitiva, para evitar los cuellos de botella en los almacenes, es necesario mejorar la planificación, tener un plan de contingencia en caso de que se produzca una interrupción en el suministro o en la capacidad de distribución y contar con la mejor innovación tecnológica posible que flexibilice y agilice los flujos de trabajo de las empresas.

Inés Alcántara,
Sales Engineer en Locus Robotics

Cinco claves para aumentar el rendimiento de tu almacén durante los picos de venta en 2023



En la industria de venta minorista, la temporada de rebajas es una época en la que es evidente el aumento en volumen de pedidos, y a la que todos conocemos como "temporada alta". Según un estudio sobre la cadena de suministro elaborado por Supply Chain Dive's studio ID en colaboración con Deposco, tres de cada cinco (59%) empresas consideran que su temporada alta será difícil. Para los almacenes y proveedores de logística de terceros (3PL), esto no sucede sólo durante las rebajas sino también durante San Valentín, en las compras de la vuelta al colegio, durante el verano o en las próximas navidades.

Si echamos la vista atrás y pensamos en el último gran pico de venta de nuestros almacenes, ¿podríamos asegurar que estábamos preparados para optimizar el tiempo de trabajo de nuestros empleados y aumentar el rendimiento sin reducir el alto número de pedidos? A continuación presentamos cinco claves para sobrevivir en un almacén durante las temporadas altas en 2023.

Planificar y prevenir las ventas con tiempo

Para algunos almacenes y 3PL, el momento para prepararse para la temporada alta es justo cuando finaliza la anterior. "Cuanto antes los almacenes comiencen a planificar su próxima temporada alta, mejor. De esta manera evitamos interrupciones de última hora que pudieran afectar a su capacidad para atender adecuadamente a sus clientes y cumplir sus SLA".

Una forma de hacerlo es analizar las temporadas altas pasadas a lo largo de los años. Cuando se ha creado un plan de acción será el momento de difundirlo; la comunicación es clave para el éxito. Es importante asegurarse de que todos los empleados, supervisores, directores y clientes (para proveedores 3PL y centros de distribución) entiendan el plan general para establecer unas expectativas y poder aliviar más fácilmente las preocupaciones o inquietudes, logrando así una mayor acogida por parte del equipo.

Reducir los tiempos de formación

Al atraer empleados temporales, estos necesitarán formarse. Pero la formación no es solo para empleados nuevos, sino que los gerentes de almacén deberán evaluar cuántas personas del equipo han pasado antes por una temporada alta. Se debe prestar especial atención a aquellas personas nuevas de la organización que no hayan pasado antes por estas épocas con picos de trabajo elevados y dedicar tiempo para formarlas y entrenarlas.

Las empresas que han incorporado robots móviles autónomos han visto reducido el tiempo de formación de más de una semana a solo unos minutos. Uno de nuestros clientes declaró que había reducido el tiempo de formación en un 80%. Esto es de gran ayuda para la temporada alta, cuando pueden formar a sus auxiliares de almacén más deprisa y asegurarse de que sean productivos más rápidamente.

Mejorar la productividad de los empleados

Al incluir robots móviles autónomos, se consigue duplicar la productividad de los empleados todo el año y durante temporadas altas. Estos son capaces de duplicar, y casi triplicar, la productividad de los trabajadores. Un empleado, por lo general, puede manejar cien pedidos por hora con métodos de recogida tradicionales. Pero, cuando ese empleado trabaja con robots, podría encargarse de 200 a 250 pedidos por hora.

Nuestros clientes, por ejemplo, opinan que los empleados disfrutan trabajando con robots móviles autónomos gracias a su tecnología atractiva que permite la reducción de fatiga de los trabajadores. Los bots hacen la mayor parte de los paseos, así que no tienen que preocuparse por caminar de 19 a 22 km al día en el almacén.

Apostar por la inversión en robots

Si el almacén ya cuenta con una flota de robots en sus instalaciones, se pueden añadir con facilidad más durante la temporada alta con el modelo de Robots as a Service. En caso contrario, no hay mejor momento que ahora. Este tipo de tecnología puede ayudar a tu almacén, centro de distribución o 3PL a lograr que esta temporada alta sea un éxito memorable al reducir el tiempo de formación, duplicar la productividad de los trabajadores, atraer empleados temporales y poner en marcha su plan antes.

Acerca de Locus Robotics

La solución multibots de Locus Robotics incorpora potentes e inteligentes robots móviles autónomos que operan en colaboración con los trabajadores humanos para mejorar drásticamente la productividad de la manipulación de piezas, cajas y palés entre dos y tres veces, al tiempo que se optimiza la mano de obra y se hace un uso eficiente del espacio del almacén. Locus ayuda a los minoristas, a los 3PL y a los almacenes especializados a cumplir y superar con eficacia los requisitos cada vez más complejos y exigentes de los entornos de distribución. Al integrarse fácilmente en las infraestructuras de los almacenes nuevos y existentes a gran escala sin interrumpir los flujos de trabajo, Locus transforma la productividad sin transformar el almacén.

Reinaldo Rodríguez (Ajoomal): «La Inteligencia Artificial cogerá cada vez más protagonismo en el campo de ciberseguridad»

Ajoomal Asociados es una empresa de Technorizon Group (con intereses en Reino Unido, Emiratos Árabes y la India) que cumple ahora 30 años de vida aportando valor añadido a la distribución de soluciones de seguridad e infraestructura informática. Desde su nacimiento en 1993 suma un crecimiento constante del negocio que transmite a su selecto canal de España y Portugal, trabajando con fabricantes clave, buscando la mejor relación calidad-precio y siempre respaldado los proyectos con un servicio técnico tanto para pre como post-venta.

CON UN portfolio de soluciones basado en la seguridad e infraestructura de red, tanto on-premise como en nube, soluciones WiFi, protección y securización del dato, back-up y autenticación, así como soluciones para dispositivos móviles, Ajoomal se ha convertido en un mayorista de valor añadido especializado referente en Iberia con delegaciones en Madrid, Barcelona y Lisboa. "Nuestro objetivo es ofrecer a nuestros clientes las mejores soluciones disponibles en el mercado actual", señala Reinaldo Rodríguez de Asevedo, CEO de Ajoomal Asociados. "Con una aproximación de valor real diferente a lo existente en el mercado ibérico, nuestras soluciones reflejan la actualización y crecimiento constante de la compañía, siempre a la última en tendencias de mercado. Nuestro mayor valor diferenciador es nuestro foco técnico, estando un tercio de nuestra plantilla compuesta por técnicos e ingenieros preventa, dando un servicio pre y post venta especializado, cercano y rápido a nuestro canal de distribución".

Queremos conocer un poco más a este directivo que un día dejó las Fuerzas Armadas brasileñas para adentrarse en la guerra cuerpo a cuerpo en la implementación y gestión desde start-ups a compañías de energía liderando equipos multidisciplinares y multiculturales en distintos entornos industriales y geográficos, incluida restructuraciones. Tras ocho años en Telefónica América Latina y luego cuatro en Lidera, aterriza en marzo de 2022 Ajoomal Asociados como director general. "Siempre he estado orientado a resultados, y tengo especial interés en el desarrollo de negocios, innovación, tecnología, digitalización y procesos de transformación de compañía".

Reinaldo Rodríguez de Asevedo, CEO de Ajoomal Asociados.

¿A qué se dedica Ajoomal y en qué es fuerte? Rasgos distintivos frente a la competencia.

Somos un mayorista de valor añadido especializado en soluciones de ciberseguridad y nuestro punto más fuerte son nuestras capacidades técnicas. A parte de esto, creo que nuestro mayor valor está en nuestra capacidad de entender claramente cuáles son los principales atributos de cada tecnología de nuestro porfolio y, gracias a esto, identificar cuál es el camino más corto para que la tecnología llegue de manera eficaz a los partners y a sus usuarios finales.

Esto lo conseguimos con especialización, focalización y competencias técnicas capaces de traducir en números las expectativas de cada uno de los eslabones de la cadena de valor del sector.

Tendencias del mercado a las que prestar atención.

Entre las tendencias más importantes que hay ahora mismo en el sector, me gustaría destacar dos de ellas que veo más relevantes y con derivadas para todo el ecosistema.

Para mí, la primera de ellas está relacionada con la evolución del modelo y del alcance del ciberdelito. La ciberdelincuencia dejó de ser una actividad de jóvenes desarrollada en un garaje para transformarse en una cuestión de Estado. Pasando antes por bandas de delincuentes altamente especializados que han migrado a actividades más rentables y de mucho menor riesgo. Hoy, nos enfrentamos a atacantes profesionales patrocinados por estados que actúan tanto contra gobiernos como contra empresas privadas y su potencial de daño es inmenso.

La segunda, tiene que ver con la Inteligencia Artificial, que cogerá cada vez más protagonismo en el campo de ciberseguridad. Como cada día son más altos los intentos de ataque, es prácticamente imposible para los expertos actuar sin el apoyo de herramientas que puedan ayudar a predecir dónde se van a producir los próximos ataques. A través de algoritmos es posible examinar y analizar en tiempo real una cantidad enorme de información y reconocer los patrones que indican una potencial amenaza.

¿Cómo está afrontando la pyme española la transformación digital?

Hasta la llegada de la crisis de la covid-19, las pymes españolas no tenían la consciencia de la importancia de la digitalización de sus procesos y de cómo esta digitalización podría ser, no solo diferenciadora sino también

una cuestión de mejorar sus posibilidades de supervivencia en el caso de la materialización de una amenaza cibernética. Se aplicaba la ley del "malo conocido" y, sobre todo, la creencia de que por qué dar este paso si todo ha funcionado "perfectamente" hasta ahora.

El detonante de esta transformación terminó por empujar las pequeñas organizaciones en la dirección de la renovación o asumir el riesgo de dejar de existir de la noche a la mañana. Las que apostaron por los cambios de la digitalización son de verdad las que mejor han afrontado esta crisis. Además, las ayudas ofrecidas por el Estado han incentivado este proceso de aceleración y cada vez hay más empresas que apuestan por ella en sus modelos actuales.

¿Qué busca en los fabricantes que representa? ¿Y qué valora más de un programa de partners?

Los fabricantes que se acercan a nosotros están buscando principalmente la cercanía y el trato personalizado que ofrecemos. Ven en nosotros un mayorista muy "taylor made" y muy comprometido con el adecuado posicionamiento de la tecnología en el perfil adecuado de partner capaz de transformar en realidad sus deseos.

¿Cuál es la estrategia de canal de Ajoomal?

Nuestra estrategia de canal sigue siendo posicionarnos como este eslabón imprescindible entre nuestros fabricantes y nuestros partners.

¿Está apostando Ajoomal por los servicios gestionados en especial MSSP?

Indudablemente, el canal va desde hace tiempo en esa dirección y, lógicamente, nosotros también hacemos una apuesta tanto a nivel de porfolio como a nivel de servicios en ese sentido.

Para que te hagas una idea casi el 50% de los fabricantes incluidos en nuestro porfolio se pueden comercializar y gestionar en modelo MSP, desde la seguridad perimetral, pasando por el endpoint y llegando a soluciones tan dispares como pueden ser las soluciones de backup como de HSM o SIEM.

A nivel interno, hemos hecho una apuesta clara por los servicios y en particular por la gestión de éstos como aporte de valor a nuestro canal. Para ello, hemos creado un grupo específico de trabajo dentro del departamento técnico dedicado a la parte de gestión y servicios para darle un plus de calidad en este sector.

¿Cómo han influido las tensiones inflacionistas, guerra en Ucrania, ransomwares… en vuestro negocio?

Desde el comienzo de la guerra de Ucrania hemos empezado a ver un incremento de ciberataques a nivel global. Rusia siempre fue uno de los países desde los que se originaban más ciberataques pero, en estos últimos meses, esto se ha incrementado siendo lo más común los ataques de ransomware con el objetivo de extorsionar y dejar sin servicio a grandes corporaciones o instituciones públicas, como ayuntamientos.

El otro tipo de amenaza que se ha incrementado son los correos de phishing que, a pesar de no ser un ataque muy sofisticado, es muy sencillo de que tenga éxito.

Debido a esto, hemos notado una mayor demanda de soluciones de EDR, para tener una mayor visibilidad de los entornos, servicios de antispam o sistemas de backup y recuperación en caso de recibir un ataque de ransomware.

¿Y el cambio de la oficina al teletrabajo en cuanto a la seguridad?

Aquí hemos detectado una evolución en el tema de trabajo desde el inicio de la pandemia hasta el día de hoy. En un principio fue una oleada en el que el canal demandaba:

- *Infraestructura*: tanto a nivel de dispositivos como de servicios Cloud
- *Seguridad en las comunicaciones*: securización de las mismas tanto a nivel VPN, ya sea clásica o con soluciones tipo ZTNA como de la validación de la identidad del usuario, con aplicaciones MFA
- *Seguridad del dato*: en el que al desaparecer el perímetro completamente las empresas demandaban, sobre todo, soluciones de cifrado de información y gestión de derechos de los usuarios en estos entornos mixtos

Hoy en día, con una vuelta parcial a las oficinas, en muchos casos, lo que nos demanda el canal es "complementar" esta seguridad inicial con soluciones de gestión y control de la productividad de los empleados, optimización y securización de las comunicaciones con soluciones SD-WAN y SASE.

¿Cuáles son sus previsiones para acabar el año?

Al igual que en 2022, estamos teniendo un muy buen año, vamos cumpliendo con nuestro plan estratégico, con nuestro presupuesto y confirmando nuestra tasa de crecimiento prevista para 2023 que supera los 23%. Llegaremos al final 2023 pudiendo celebrar, una vez más, un muy buen año. No solo en términos financieros y económicos sino también en la mejora de nuestros procesos, recursos y capacitación de nuestros colaboradores.

Ajoomal cumple 30 años

El pasado 8 de junio se celebró el Ajoomal Day, una completa jornada de mañana y tarde con charlas técnicas, networking y mucha diversión. No era para menos, pues el mayorista VAD soplaba sus 30 primeras velas. "Un día muy especial en el que celebraremos nuestro 30 aniversario junto a nuestros partners y fabricantes en una jornada de conferencias en la que discutiremos los puntos clave de la ciberseguridad y del mundo actual, culminando con un cóctel, deejay, ¡y mucho más!", señalaban en la empresa.

El evento tuvo lugar en el antiguo teatro Albéniz de Madrid, ahora rebautizado UMusic y que incluye hotel de cinco estrellas y salas de ocio para espectáculos y eventos. El acto estuvo arropado por algunos de sus fabricantes más veteranos y fieles, algunos con 20 años en su catálogo, como WatchGuard (1998), Sophos (2001), Thales (2002) o Barracuda (2004), y otros de más reciente incorporación, como Datto (2020) y LogPoint (2022).

Mucho ha llovido sobre las espaldas de *Ayumal* desde que en 1993 su fundador Girish Ajoomal dejara su restaurante Tagore después de regentarlo durante cinco años para comenzar a vender "seguridad" con un cortafuegos bajo el brazo. "Por aquella época solo se conocían los paquetes de antivirus; imaginar protegerse vía hardware era impensable. Casi 25 años después, llegó el momento de subirse a la nube y redefinir la manera de protegerse y entender la ciberseguridad. Pero todavía queda mucho por hacer. Todos vamos al cloud, es muy bonito, ¿pero el flujo de datos está protegido? Allí sí, pero de la oficina al CPD de ellos no tanto", declaraba su fundador en la inauguración de las nuevas oficinas de 2017. "A medida que las empresas se van concienciando de la importancia de la seguridad para proteger sus activos, este sector no ha dejado de crecer. Llevamos experimentando crecimientos de doble dígito prácticamente desde el inicio".

Ajoomal es un mayorista "atípico, de la vieja escuela, de los que nos gusta hacer los negocios cara a cara, de hacer la calle y visitar tiendas", como se autodefine. Hace seis años se instalaron en el llamado Silicon Alley de Madrid, un entorno con más de 200 empresas del sector tecnológico, cuajado de centros de datos y kilómetros de fibra óptica. Su optimismo sobre el comportamiento del mercado, y la necesidad de alinear sus infraestructuras y recursos a las actuales necesidades del negocio son los otros motivos de haberse mudado en 2017 al edificio Diapasón, aunque no los únicos: "Parece mentira, pero en el Campo de las Naciones solo teníamos conectividad con Telefónica. Aquí están todas y tenemos más que cubiertas nuestras necesidades y redundantes nuestras capacidades".

Sin duda aquel fue un paso necesario para afianzar su propuesta de valor a lo largo de la vida de un proyecto dado, y poder abordar con garantías la próxima estrategia comercial de ofrecer pago por uso de todo su catálogo, con una sala de servidores que correspondería por tamaño al de una empresa seis veces más grande, y un almacén logístico de 200 m2. Se trataba de crear la plataforma de su crecimiento y que diese soporte a la próxima generación de servicios gestionados, que es a donde se mueve el mercado: preventa y consultoría, pago por uso más postventa, gestión y mantenimiento.

Y todo ello apoyado en un portfolio completo de fabricantes líderes capaz de cubrir cualquier necesidad, criptografía por hardware, tokens de autenticación, cifrado fuerte, firma digital, recuperación de datos, servicios gestionados de seguridad MSSP… Porque igual un cliente no puede soltar 150.000 euros de golpe, pero sí pagar 1.000 o 5.000 euros al mes que permita gestionar sus operaciones de TI de manera más eficiente y flexible, al transformar sus inversiones de capital en TI en costes de operación.

Como mayorista y VAD especializado, Ajoomal se sitúa de manera natural entre el fabricante, el integrador y el usuario final. "Somos el punto de enlace entre fabricantes, conocedores y creadores de la tecnología, e integradores, conocedores de las necesidades y demandas del mercado, con claro potencial de desarrollo y capacidad para acceder a grandes cuentas. Si no participa todo el mundo esto no funciona, cada uno debe llevarse su parte y el margen que le corresponda. Igual una parte del canal informático no tiene recursos para servicios de gestión remota y nosotros le ofrecemos soluciones as-a-service, o un fabricante solo tiene una persona para toda Iberia y nosotros le proporcionamos servicios de soporte certificado y en español", dice Girish.

Ajoomal también está capacitado para cubrir todo el ciclo de proyecto y asegurar la calidad de TI en cualquier escenario: servicios de preventa, que incluyen auditoría de TI, y consultoría de proyectos, servicios de formación y soporte técnico post-venta. "Uno de los valores diferenciales de Ajoomal es el profundo conocimiento de todos los productos que distribuye. A veces viene el fabricante y nos forma, otras vamos nosotros a su país y nos certifican. La formación muchas veces ni la cobramos, pecamos de ingenuos, pero es que preferimos un canal que esté formado y sepa defenderse, que no vaya solo a vender. Al fin y al cabo, esto es un negocio tecnológico".

Ajoomal se preparaba para afrontar un prometedor futuro en el entorno de la ciberseguridad y los servicios gestionados en sus nuevas oficinas, pero nunca se pensó en que una pandemia mundial arrasaría todo el orbe y multiplicaría la necesidad de digitalización de las empresas con tanta urgencia. Superado ya aquellos meses de conmoción, llegó la guerra en Ucrania y la inflación se disparó. Un mundo en constante y acelerada evolución que necesita gurús como Ayumal. Dice Chat GPT sobre el significado del nombre: "Ajoomal tiene un don extraordinario para percibir algo más grande que ellos mismos y traerlo a la vida en la tierra. Las ideas visionarias y los grandiosos objetivos de Ajoomal son evidencia de su capacidad única para soñar en grande. Ajoomal está motivado para dejar un legado duradero y está dispuesto a trabajar incansablemente para que esto suceda". Y si lo dice Chat-GPT...

SUMINISTRADORA DE COMPONENTES ELECTRÓNICOS, S.L.

PROFESIONALES CON MÁS DE 25 AÑOS DE EXPERIENCIA

CoolBox · GIGABYTE TECHNOLOGY · tp-link · ASUS

Telef.: 913 041 211 / 910 612 229

comercial@sce.es

C/ La Fragua, 18
28522 Rivas Vaciamadrid - Madrid

www.sce.es

NetApp anuncia una garantía de recuperación frente al ransomware

NetApp continúa dando salida a su roadmap de este año con el lanzamiento este mes de varios productos y programas innovadores, incluyendo una nueva oferta SAN de almacenamiento en bloque all-flash y una garantía que destaca la capacidad de NetApp para recuperarse de los ataques de ransomware.

ESTOS DOS anuncios abordan los retos críticos de los clientes, incluyendo la creciente complejidad de las TI, los presupuestos cada vez más limitados, la necesidad de sostenibilidad y el continuo crecimiento exponencial de las ciberamenazas. La nueva familia ASA (All-Flash SAN Array) A-Series de NetApp simplifica el despliegue de una infraestructura SAN moderna, pensando en la alta disponibilidad con una licencia única que ahorre costes y además proporcione reducción en huella de carbono. NetApp también anuncia una Garantía de Recuperación de Ransomware por SLA, en un momento en el que se espera que los costes del ransomware para las organizaciones globales aumenten de 20.000 millones de dólares en 2021 a 265.000 millones de dólares en 2031.

Jaime Balañá, director técnico para Iberoamérica de NetApp.

"El mundo moderno necesita sacar partido a los datos, pero el entorno TI es cada vez más complejo, a lo que cabe añadir incertidumbre sobre el futuro. Esto está produciendo una pequeña constricción en el gasto en TI y obliga a hacer más con menos", señala Jaime Balañá, director técnico para Iberoamérica de NetApp. "El mundo moderno no es tan bonito como se pintaba, pero NetApp está ahí para tratar de facilitar la navegación en este entorno tan complicado haciéndolo más sencillo. Las organizaciones buscan simplicidad y seguridad y NetApp ayuda a los clientes a resolver los retos del almacenamiento de datos con simplicidad operativa a escala, seguridad integrada para gestionar y recuperarse de las amenazas del ransomware, y almacenamiento Flash respaldado por eficiencias garantizadas para alcanzar o superar los objetivos de sostenibilidad y ahorro".

Aprovechando más de dos décadas de experiencia en almacenamiento de datos y más de 20.000 clientes de aplicaciones SAN, NetApp amplía su oferta en almacenamiento NAS y unificado con una línea de cinco productos dedicada al almacenamiento en bloque, permitiendo a los clientes eliminar los silos de infraestructura y simplificar sus entornos de datos estructurados y no estructurados on-prem y en nube pública.

Su familia ASA A-Series es una nueva línea de sistemas de almacenamiento flash específicos para SAN que ofrece un rendimiento superior, escalabilidad, disponibilidad de datos, eficiencia y conectividad de cloud híbrido para aplicaciones y bases de datos críticas para el negocio tipo SAP, Oracle, Microsoft SQL o VMware: "Un on-prem preparado para la nube pública", resume Balañá. "Los clientes nos han dejado ver que la estrategia que seguimos en el cloud es la que querían, pero también querían que el centro de datos no dejara de ser como ha sido siempre. Estos equipos que van desde los de entrada a los de más alta disponibilidad se adaptan a sus necesidades, por ejemplo para un entorno de no tanto rendimiento pero que tuviera los beneficios de un datacenter moderno en cuanto a eficiencia para la reducción de huella de carbono basado en flash, reforzando la parte de almacenamiento en bloque y el que no necesite NAS pueda beneficiarse de la nube híbrida sin costes ocultos".

Las principales mejoras del nuevo portafolio de NetApp son:

- Garantía de disponibilidad de datos de seis nueves (99,9999%).
- Alta relación capacidad efectiva/utilizable combinadas con la garantía de eficiencia de almacenamiento 4:1 de NetApp.
- Basándose en el compromiso de la compañía con la sostenibilidad, NetApp ASA ofrece hasta un 50% menos de consumo energético y emisiones de carbono asociadas que algunas ofertas de la competencia.
- Almacenamiento de datos moderno basado en flash de alto rendimiento NVMe con protocolos NVMe/FC, NVMe/TCP, FC e iSCSI.

«Los datos son el recurso más valioso, pero vulnerable. El coste y tiempo de recuperación puede multiplicarse por diez al monto del rescate hasta volver a poder funcionar con normalidad, al margen de la pérdida de clientes y el coste reputacional» (Jaime Balañá, NetApp)

- Acceso continuo a los datos en todos los sistemas ASA gracias a la arquitectura simétrica activo-activo que normalmente solo se encuentra en sistemas de gama alta con un coste más elevado.
- Storage Lifecycle Program, que ofrece a los clientes actualizaciones no disruptivas a la última tecnología de sistemas de almacenamiento cada tres, cuatro o cinco años sin coste adicional.
- Protección de datos integrada y conectividad de nube híbrida para garantizar que los datos estén seguros y puedan extenderse a AWS, Azure y GCP.
- Nuevo licenciamiento de ONTAP One basado en una única licencia 'todo-incluido', no solo para los nuevos clientes, también para las anteriores en vigor para que puedan ser unificadas. "El precio sigue estando acorde a todos los servicios dados, pero por lo menos se simplifica la gestión y siempre sabes lo que tienes, en vez de tener como antes licencias por separado para cada funcionalidad (mirrors, sistemas operativos…)", apunta el CTO.

Seguro frente a ransomware

Partiendo de la estrategia de NetApp basada en tres capas de protección, detección y recuperación, ahora se añade la disponibilidad de una nueva garantía frente a ransomware que aprovecha la combinación de funciones integradas de seguridad y protección frente a ransomware del software ONTAP para bloquear automáticamente tanto tipos de archivos maliciosos conocidos, como también a administradores y usuarios malintencionados. Gracias a la verificación multiadministrador de doble llave se puede también proporcionar copias de los datos (snapshots) indelebles que no pueden ser eliminados, ni siquiera por el administrador de almacenamiento.

Con la protección autónoma contra ransomware de ONTAP se pueden detectar los ataques, tomar snapshots adicionales de forma instantánea y recuperar los datos en cuestión de minutos. Con esta combinación de tecnologías, NetApp garantiza la recuperación de los datos desde los snapshots, en caso de ataque de ransomware. Si las copias de datos no pudiesen recuperarse con la ayuda de NetApp o de un partner, NetApp ofrecerá una compensación (siempre que se cumpla las condiciones de la letra pequeña).

Según TechCrunch, el valor de los datos para 2025 será de 280.000 millones de dólares. Pero los ataques de ransomware seguirán creciendo, así como los costes de recuperación, que podrían ser de 4,35 millones de dólares por ataque. "Las compañías se dividen entre las que han sido atacadas y las que lo van a ser, bueno y hay una tercera categoría que son las que han sido atacadas y aún no lo saben", dice Balañá. "Los datos son el recurso más valioso, pero vulnerable. El coste y tiempo de recuperación puede multiplicarse por diez al monto del rescate hasta volver a poder funcionar con normalidad, al margen de la pérdida de clientes y el coste reputacional. Es cierto que ya hay seguros especializados, pero también que se están disparando los precios de las primas y de las condiciones para hacértelo. Nuestra nueva garantía de recuperación por contrato viene incluida en la licencia. La duración del seguro ante ciberataques de NetApp es de quince meses desde la entrega del último componente o de doce meses desde que Professional Services notifica que se ha completado la configuración".

Anuncios menores

Además de la nueva familia ASA de NetApp y la garantía de recuperación de ransomware, este lanzamiento viene acompañado de:

- Nuevo "cacharro" de entrada FAS2820, actualización de FAS2720 con hasta un aumento del rendimiento del 50% y una actualización sin interrupciones en el chasis del FAS2620 o FAS2720.
- ONTAP One, el software de almacenamiento integrado y todo incluido, ya disponible para todos los sistemas AFF, ASA y FAS. NetApp también pone las funcionalidades integradas en ONTAP One a disposición de los sistemas desplegados existentes bajo soporte.
- ONTAP 9 May 2023 Release, que mejora la protección contra ransomware y la gestión de cargas de trabajo consolidadas.
- StorageGRID 11.7, una nueva versión del software para federar equipos dispersos geográficamente, con capacidades avanzadas para la recuperación ante desastres, actualizaciones para la seguridad y el cumplimiento normativo y experiencia de usuario simplificada.
- StorageGRID SGF6112, nuevo appliance de 1U de almacenamiento de objetos all-Flash de nueva generación con rendimiento y densidad mejorados, para soportar cargas de trabajo de objetos con gran demanda de rendimiento y grandes cantidades de datos en rápido crecimiento, incluyendo IA, analítica y data lakes.
- NetApp Advance se ha ampliado, aumentando el portafolio de programas y garantías de NetApp, que permiten una evolución sencilla y fiable de los entornos de almacenamiento.

Tpv para Windows

Queremos ofrecer al distribuidor lo más nuevo y con diferentes prestaciones, para que siempre puedan elegir el mejor modelo para su cliente.

Tpv Android

Equipo con pantalla táctil de 14” capacitiva anti reflectante
Disponible en color negro con la versión de Android 7.1
Con numerosos puertos y con conexión Wifi, Bluetooth y Ethernet.

REELSA

C/ Destornillador, 30 P-29 Collado Villalba 28400 (Madrid)

918519711 www.reelsa.es pedidos@reelsa.es 637 75 56 13

Software de gestión

En REELSA trabajamos con tres marcas: BDP, GLOP y nuestro Software propio de gestión TOWASANKIDEN.

TOWASANKIDEN

Software válido tanto para Windows como para Android. Con este programa puedes controlar el stock y gestionar las comandas, los pedidos...

BDP

Glop

TOWA SANKIDEN

REELSA

C/ Destornillador, 30 P-29 Collado Villalba 28400 (Madrid)

918519711 www.reelsa.es pedidos@reelsa.es 637 75 56 13

Impresoras de Tickets

Contamos con una de las mejores marcas, XPRINTER, porque la calidad de la impresora, de la impresión y la rapidez son fundamentales para dar el mejor servicio

Impresora de Etiquetas

Impresora térmica directa con diseño compacto, imprime diferentes tipos de etiquetas con una anchura máxima de 108mm y longitud máx. 2286mm.

REELSA

C/ Destornillador, 30 P-29 Collado Villalba 28400 (Madrid)

918519711 www.reelsa.es pedidos@reelsa.es 637 75 56 13

Avisadores de camareros

Con estos dispositivos llamas al camarero para que acuda a la mesa del cliente, evitando esperas.

Gestores de clientes

Con estos dispositivos avisas al cliente para que pueda levantarse a por su pedido para recogerlo.

REELSA
C/ Destornillador, 30 P-29 Collado Villalba 28400 (Madrid)
918519711 www.reelsa.es pedidos@reelsa.es 637 75 56 13

Sonia Marcos (EET): «Queremos seguir apostando por nuestras áreas clave impulsando especialmente las de conectividad y videovigilancia»

EET Spain es parte del Grupo EET, un mayorista TI de valor añadido que brinda a proveedores y clientes conocimiento experto de la industria, soluciones logísticas inteligentes, servicio de ventas y herramientas de marketing inteligentes. Entrevistamos a su directora general para España, Sonia Marcos.

Sonia Marcos, directora general de EET Spain.

EL GRUPO EET opera en 24 mercados en Europa, tiene más de 1.100 marcas y atiende a más de 31.000 clientes compradores al año. "Nuestra visión es ser el distribuidor de TI de valor añadido preferido y más eficiente en el mercado europeo con el surtido más sólido y el conocimiento más profundo dentro de nuestras líneas de negocio", asegura Sonia Marcos, Country Manager de la filial española. A continuación, tenemos más información.

Haz un breve resumen sobre EET. ¿Cuál ha sido su evolución en los últimos cinco años y cuáles son las principales áreas de actividad de la compañía en la actualidad?

EET ha cambiado mucho en los últimos cuatro años, nos hemos reorganizado para ser un distribuidor TI de valor añadido. Ahora somos un proveedor global de soluciones y podemos ofrecer al cliente un catálogo completo de productos.

Hemos adquirido varias empresas que nos han ayudado, tanto a expandirnos, como a acercarnos mucho más a nuestro objetivo, (Express-Parts, CCTV Center, Avant Video). De esta manera, hemos conseguido añadir marcas de fabricantes de primer nivel a todas nuestras líneas de negocio y hemos reforzado nuestro equipo con perfiles técnicos y comerciales especializados y con una gran experiencia en el sector. Todo, con la única intención de dar al cliente siempre el mejor servicio.

También hemos invertido mucho en nuestra parte digital. Hemos querido que los clientes puedan acceder a nuestro catálogo de la manera más sencilla posible, por eso lanzamos una nueva página, más dinámica y atractiva para el cliente.

En Iberia, EET apuesta especialmente por cinco sectores en crecimiento: piezas y componentes informáticos; seguridad y videovigilancia; audiovisual profesional; redes y conectividad; y POS.

¿Cuál es la principal ventaja competitiva de EET frente a otros mayoristas del mercado?

En EET contamos con varios puntos que nos diferencian de nuestra competencia y que son claves para construir nuestra ventaja competitiva. Somos una marca que ofrece un gran portfolio de producto en todos los sectores en los que trabajamos. Nos sentimos orgullosos de poder ofrecer a nuestros consumidores soluciones completas de un gran catálogo de productos, stock y disponibilidad.

Además, apostamos por la tecnología web, por lo que contamos con una plataforma logística de primer nivel que da servicio y soporte a nuestros clientes de manera rápida y sencilla.

Otro de los puntos que nos posiciona como mayorista líder sin duda es el trato al cliente. Contamos con un gran equipo técnico y comercial que va creciendo poco a poco. Grandes entendidos del sector que acompañan y asesoran a nuestros clientes durante todo el proceso.

¿Cuál ha sido el producto estrella en el último año?

Todos los productos tienen su mercado, pero en concreto este 2022 hemos visto una gran evolución en productos relacionados con el sector de redes y conectividad.

¿Cuál diríais que ha sido el hito más importante al que os habéis enfrentado en 2022?

El año pasado ha sido un ejercicio que sin duda no olvidaremos a nivel social y empresarial. Estos últimos tiempos han sido años de recuperación tras la crisis sanitaria mundial que vivimos que, sumado a otros incidentes como la guerra de Ucrania, potenciaron una crisis de componentes a nivel global. Para nosotros, que somos una empresa dedicada al sector tecnológico, creo que el hito más difícil, caro y complicado de superar ha sido conseguir disponibilidad en ciertos productos.

«En Iberia, EET apuesta especialmente por cinco sectores en crecimiento: piezas y componentes informáticos; seguridad y videovigilancia; audiovisual profesional; redes y conectividad; y POS» (Sonia Marcos, EET)

¿Qué áreas de negocio son las que más se han desarrollado en 2022?

Sabemos que 2022 no ha sido un año fácil para la industria de la tecnología, pero nuestros resultados han sido muy buenos para este año. Estamos muy orgullosos de haber crecido en todas las áreas de negocio que llevamos en Iberia.

¿Qué balance hacéis de 2022? ¿Se han cumplido las previsiones y los objetivos marcados a principio de año?

2022 ha sido para nosotros un año de consolidación, dejamos atrás la integración de CCTV Center y Avant Video para concentrarnos en dar el mejor servicio a nuestros clientes. Estamos muy orgullosos de poder poner al cliente en el centro de nuestra estrategia y de ofrecerles un valor añadido diferencial en todas nuestras propuestas.

Si nos limitamos a mirar los números, en 2022 hemos crecido un 22% nuestra facturación frente al 2021 siendo un gran año para nosotros.

¿Qué novedades tenéis preparadas para 2023? ¿Hay nuevos sectores o áreas a las que EET quiera llegar?

Tras el año de consolidación, para 2023 queremos seguir apostando por nuestras áreas clave impulsando especialmente las áreas de conectividad y videovigilancia. Además, queremos seguir trabajando por convertirnos el mayorista de referencia y por seguir ofreciendo el mejor y el más completo servicio a nuestros clientes.

¿Cuál es vuestro principal objetivo para el año 2023?

Tenemos que seguir creciendo y firmando acuerdos con fabricantes de reconocido prestigio. Además, este año por fin, organizamos nuestro EET Day en el Metropolitano de Madrid, la oportunidad perfecta para que nuestros clientes tuvieran acceso directo y privilegiado con nuestros fabricantes y equipo comercial.

Primera edición del EET Day

El pasado 25 de mayo se celebró en el Estadio Civitas Metropolitano de Madrid el EET Day 2023, la primera edición del evento organizado por EET Iberia que reunió en un mismo espacio a más de 40 fabricantes del sector tecnológico, líderes de las distintas divisiones de negocio de EET mostrando sus últimas novedades.

El mayorista quiere posicionar su cita con sus partners como un punto de encuentro del sector, donde todas las marcas principales de su porfolio pueden presentar las mejores y más innovadoras soluciones en Seguridad y videovigilancia, ProAV, Redes y conectividad, POS & Auto-ID, Almacenamiento, Electrónica de consumo, Piezas de servidor y PC e impresora.

Entre las empresas expositoras se encontraban grandes marcas como: Adder Technology, AVer, Bixolon, Bosch, B-Tech, Cambium Networks, Capture, Castel, Dahua, Datalogic, Davantis, Ecler, Ernitec, eStuff, Gearlab, GJD, Hanwha Vision; Hikvision, Honeywell, Idis, i-Pro, Lanaccess; Lanview, Legrand, Magos Systems, Matrox, Micro Connect, Milestone, Mobile Pixels, MyDefence, Newland, Pelco, Paxton Access, Pelco, PPDS (Philips), Robotto, Sandberg, Senstar, SharpNEC, Vivolink y Vogel´s.

Sonia Marcos afirmaba: “Estamos tremendamente ilusionados con esta nueva iniciativa, donde no solo reunimos a las mejores marcas del mercado TI, si no que, como mayoristas, con nuestra experiencia en el sector, les ayudaremos a generar negocio. Esta primera edición de EET Day es un paso al frente de la compañía como mayorista de valor, ofreciendo soporte y acompañando y ayudando a crecer tanto a nuestros clientes como a nuestros fabricantes”.

Con este encuentro EET pretende dar la oportunidad de generar nuevas oportunidades de negocio, realizar un networking entre fabricantes y asistentes, mejorar la red de contactos de estos y conocer nuevas soluciones y líneas de negocio para los distintos proyectos que quieran llevar a cabo. La jornada acabó con un cocktail para que los asistentes pudieran disfrutar de su visita al EET Day en un ambiente agradable y distendido.

PUDU

Ya están aquí

BellaBot

Robot de entrega

KettyBot

Robot publicitario

CC1

Robot de limpieza

HolaBot

Robot de recogida

PuduBot 2

Robot de reparto
y recogida

TPV

PREMIER
We are a team

Serie KT: J4125 | J6412 | 4GB | 8GB | 16GB | 128GB | 256GB | Win 10 IoT
RK3288 | 2GB+16GB

KIOSKO Y PC PANEL

PCP 215 W/A | KIOSK 27 W/A

MONITORES TÁCTILES

Serie TM: 15" | 17" | 21,5"

STAND ITP-FRONT Y TABLET

IMPRESORAS TÉRMICAS DE TICKETS Y ETIQUETAS

Serie ITP: 58mm | 80mm | Serie | USB | Ethernet | Wifi | Bluetooth | Sobremesa | Portátil

LECTORES DE CÓDIGO DE BARRAS

Serie MS3: 1D | 1D RF | 2D | 2D BR | Desktop

PDA´s

MAXI 20 | MAXI 21 | MAXI 50P

MUZYBAR
computer

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

PHASAK®

www.phasak.com

Seguridad y garantía, *no son una opción*

Fabricantes de Sistemas de Alimentación Ininterrumpida (SAI / UPS), Armarios Rack de 19", baterías, cableado y todo tipo accesorios relacionados.

Presente en mercados internacionales desde 1995, PHASAK apuesta por la calidad y la atención personalizada en cada uno de sus productos. Con más de 150 referencias en catálogo, ponemos a disposición de nuestros clientes soluciones integrales para entornos domésticos y empresariales.

30
Años de experiencia

Innovación y evolución

Atención personalizada

Distribución exclusiva para el canal mayorista
info@phasak.com

Sistemas de Alimentación Ininterrumpida

Los SAIS (**Sistemas de Seguridad Ininterrumpida**) o UPS protegen los equipos conectados frente a picos de tensión, generando su propia alimentación en caso de fallo o corte de suministro eléctrico.

PHASAK fabrica y distribuye una gran variedad de SAIS tanto con tecnología interactiva como online para instalaciones más complejas y críticas.

+ www.phasak.com

Armarios y murales Rack 19”

Phasak ofrece una amplia gama de armarios de suelo y murales en formato **Rack 19**” y una gran cantidad de accesorios y complementos que cubrirán todas las necesidades y personalización de los usuarios más exigentes.

Todos los armarios PHASAK incluyen **2 bandejas de 19" compatibles, regleta eléctrica de 19" compatible y juego de patas fijas.**

+ www.phasak.com/armarios-rack-19

Latiguillos

+ www.phasak.com/latiguillos

Bobinas de Cable

+ www.phasak.com/bobinas-de-cable

Baterías 12V

+ www.phasak.com/baterias

Descargue el catálogo completo en www.phasak.com

SAI / UPS Interactivos

Serie Basic
PH 9406 (600VA)
PH 9408 (800 VA)

Serie Ottima
PH 7266 (660 VA) · PH 7288 (860 VA)
PH 7210 (1060 VA)

Serie Esential
PH 9464 (600VA) · PH 9465 (650 VA)
PH 9485 (850 VA) · PH 9410 (1000VA)
PH 9420 (2000 VA)

Serie Kryptos
PH 9478 (800 VA)

Serie Sirius
PH 7312 (1260 VA) · PH 7315 (1560 VA)
PH 7322 (2260 VA)

Protekt Torre
PH 7610 (1060 VA) · PH 7621 (2160 VA)
PH 7631 (3160 VA)

Protekt Rack
PH 7512 (1260 VA) · PH 7521 (2160 VA)
PH 7530 (3060 VA)

SAI / UPS Online

Conqueror Pro
PH 8010 (1000 VA) · PH 8020 (2000 VA)
PH 8030 (3000 VA)

Smart Pro
PH 9210 (1000 VA) · PH 9220 (2000 VA)
PH 9230 (3000 VA)

Online Rack
PH 9315 (1500 VA)
PH 9330 (3000 VA)

Pro Rack
PH 9360 (6000 VA)
PH 9301 (10000 VA)

Gate Pro
PH 9260 (6000 VA)
PH 9270 (10000 VA)

Tempus 3P/3P
PH 9273 (10 Kva)
PH 9293 (20 Kva)
PH 9283 (30 Kva)
PH 9284 (40 Kva)

Dual Pro
PH 9286 (60 Kva)
Entradas duales

Distribución exclusiva para el canal mayorista
info@phasak.com

Baterías

Baterías selladas PHASAK de **plomo-ácido de 12V** disponibles en **7.2, 9 ó 12** Ah. Compatibles con los modelos de SAI/ UPS PHASAK que incorporen baterías de las mismas características.

Baterías **estándar compatibles** con cualquier producto que utilice baterías con características eléctricas similares.

PHB 1207
Voltaje: 12 V
Capacidad: 7.2 Ah

PHB 1209
Voltaje: 12 V
Capacidad: 9 Ah

PHB 1212
Voltaje: 12 V
Capacidad: 12 Ah

Bobinas de cable de red y latiguillos

Fabricadas en Categoría 6, la categoría más popular y la que ofrece una conexión más estable y de mayor fiabilidad, siendo la opción favorita de la mayoría de instaladores para tramos largos. Las bobinas PHASAK garantizan la compatibilidad con categorías anteriores.

Latiguillos de Red UTP fabricados por PHASAK con conectores RJ45 macho en sus dos extremos. Disponibles en **100% Cobre** o **CCA** en diferentes colores y medidas que van desde los 0.25 hasta los 30 metros.

Presentados en **bolsa retail** individual con cartoncillo y troquel, cumplirán con las expectativas de los usuarios más exigentes.

COBRE 100% SÓLIDO

PHR 652

Bobina de 305 metros de cable de red **Certificado UTP** sólido Eca LSZH en caja, de categoría 6 en Cobre

Soporta velocidades de transferencia de hasta 1 Gbps.

- ✔ Cu Sólido
- ✔ AWG24
- ✔ UTP + LSZH

PHR 660

Bobina de 305 metros de cable de red **Certificado S-FTP** sólido Eca LSZH en caja, de categoría 6A en Cobre

Soporta velocidades de transferencia de hasta 10 Gbps.

- ✔ Cu Sólido
- ✔ AWG23
- ✔ S-FTP + LSZH

CCA SÓLIDO

PHR 6302

Bobina de **305 metros** de cable de red UTP sólido en caja, de categoría 6 en CCA.

Soporta velocidades de transferencia de hasta 1 Gbps.

- ✔ CCA Sólido
- ✔ AWG23
- ✔ UTP

PHR 6301

Bobina de **305 metros** de cable de red UTP sólido LSZH en caja, de categoría 6 en CCA.

Soporta velocidades de transferencia de hasta 1 Gbps.

- ✔ CCA Sólido
- ✔ AWG23
- ✔ UTP + LSZH

PHR 6312

Bobina de **305 metros** de cable de red FTP sólido LSZH en caja, de categoría 6 en CCA.

Soporta velocidades de transferencia de hasta 1 Gbps.

- ✔ CCA Sólido
- ✔ AWG23
- ✔ FTP + LSZH

PHR 6100

Bobina de **100 metros** de cable de red UTP sólido en caja, de categoría 6 en CCA. Soporta velocidades de transferencia de hasta 1 Gbps.

✔ CCA Sólido ✔ AWG23 ✔ UTP

Contacto

www.phasak.com
info@phasak.com
980 53 94 99

Descargue el catálogo completo en www.phasak.com

Malinche saluda el nuevo formato del TD Synnex Explora

La gran carpa de Malinche fue uno de los puntos centrales de Explora donde, después de una bienvenida a cargo del equipo del mayorista, se explicó cómo ha sido la transición de la antigua Tech Data a TD Synnex, una compañía más potente, líder del mercado ibérico, situada en el centro del ecosistema de las colaboraciones tecnológicas, y que conecta a fabricantes y clientes con casos, recursos, datos, formación y conocimientos especializados.

EL MAYORISTA TD Synnex volvió a reunir a su canal de partners en un macroevento presencial tras cuatro años de sequía. El lugar escogido fue la carpa del Templo Canalla donde se celebra el musical "Malinche", el espectáculo concebido por Nacho Cano. "Ayer fue sin duda un día espectacular para TD Synnex y no podemos dejar de daros las gracias a cada uno de vosotros por ser parte fundamental de Explora", señalaba Marta Juderías, directora sénior de Marketing Iberia.

La primera edición de Explora, el evento que releva al recordado MeTIC de Tech Data durante ocho temporadas, ha sido un éxito total de asistencia y participación, colgando varias semanas antes el cartel de "No hay invitaciones" y reuniendo a una treintena de banderolas de expositores de los 52 que contribuyeron en gran medida a sufragar la puesta en escena.

"Conseguimos un ambiente vibrante y lleno de energía, y fue un verdadero placer teneros a todos como invitados en un momento tan significativo para TD Synnex", continuaba Marta Juderías. "Desde el momento en que abrimos las puertas de Explora, se podía sentir la emoción en el ambiente, el Templo Canalla estaba lleno de rostros sonrientes, conversaciones animadas y una ilusión que hizo que la experiencia fuera verdaderamente memorable. Cada uno de vosotros aportó su valioso conocimiento y perspectiva, lo cual fue fundamental para enriquecer nuestras discusiones y fortalecer nuestra red de contactos".

Doña Marina la Exploradora

2019 fue el último MeTIC en Barcelona, y desde entonces el mayorista y agregador de soluciones para el ecosistema de TI Tech Data ha pasado a llamarse TD Synnex, integrado en este conglomerado de capital principalmente norteamericano, y ahora vuelve a organizar su gran evento en España, con el que ha conseguido reunir en el Ifema de Madrid a más de mil partners y los principales fabricantes con los que trabaja.

Con el claim "Explora", que es el escogido para esta vuelta de TD Synnex a su encuentro anual con clientes y partners, se refleja la reconocida misión y filosofía del mayorista, que consiste en ayudar los clientes de la compañía a descubrir nuevas oportunidades de mercado mientras se les proporciona las mejores soluciones y las mejores herramientas para atender y apoyar sus necesidades de negocio.

Luis Pires, Marta Judarías y Pilar Martín de TD Synnex con el padre Olmedo (Nacha la Macha).

Los asistentes tuvieron la oportunidad de saludarse y charlar con sus principales fabricantes de su catálogo y conocer directamente sus propuestas tecnológicas y de servicio, todo ello de la mano de este mayorista reconocido por el mercado a través de Context ChannelWatch como "Mejor Distribuidor de España 2022" y "Mejor Distribuidor EMEA 2022" entre otros muchos galardones.

En un momento dado, ya todos aposentados en sus butacas del anfiteatro, sobre el escenario apareció una nao capitaneada por tres de los organizadores, que agradecieron la asistencia y presentaron las últimas novedades de la casa. "Recordad la última vez que pudimos reunirnos hace cuatro años. En 2020, diez días antes de celebrarse el MeTIC con todo ya listo hubo que cancelarlo por el confinamiento", rememoraba Marta Juderías. "Han pasado muchas cosas desde entonces, y hoy hemos venido a explorar y descubrir las nuevas necesidades del mercado y de nuestros clientes".

Ya con un pie en tierra, Luis Pires, VP Portugal y director de EndPoint Solutions Iberia, comenzó repasando las cifras de TD Synnex en la península: 650 empleados, 8.500 clientes, más de 200 fabricantes y cuatro oficinas en Madrid, Barcelona, Lisboa y Oporto. "Disponemos de un portfolio end-to-end con los mejores en sus categorías. Estamos especializados en dar servicios y ofrecer soluciones a todo tipo de necesidades contemplando todo el ciclo de vida a través de nuestra plataforma de agregación y orquestación que facilita el trabajo de nuestros partners. Somos por tanto un mayorista de valor añadido".

Otra de las novedades más destacada fue SMB Home, un espacio exclusivo que permite tener una visión detallada de la situación de negocio con TD Synnex, facilitando la gestión del día a día integrado dentro de Hola TD Synnex. "Apenas seis meses después del lanzamiento del espacio SMB Home de TD Synnex el pasado mes de junio de 2022, ya son más de 2.500 las empresas que lo utilizan de modo recurrente", señaló Pires.

Entre otros contenidos, que han alcanzado una alta valoración por los usuarios del espacio, se encuentran:

- Acceso y visibilidad detallada de las campañas promocionales vigentes, viendo en todo momento el nivel de consecución y evolución.
- Acceso a información sobre aspectos financieros como solicitud de crédito, actualización datos bancarios, certificados de revendedor, etc.
- Elementos operacionales para obtener información sobre actividad, evolución del negocio con TD Synnex, comparativas, análisis de oportunidades, etc.
- Eventos de TD Synnex y los fabricantes y acceso a los diferentes programas de canal de estos últimos.

"Como empresas, las pequeñas y medianas distribuidoras de tecnología y los proveedores de servicios gestionados se enfrentan a grandes retos. SMB Home es un espacio que pretende ser muy funcional, en el que se concentra

TD Synnex Iberia vuelve a organizar su gran evento anual en España, con el que ha conseguido reunir en el Ifema de Madrid a más de mil partners y los principales fabricantes con los que trabaja inspirándose en el espectáculo de Malinche

la información necesaria para nuestros clientes y con un acceso lo más sencillo posible, con el objetivo de ayudarlos, ponerlos en contacto con recursos, resolver problemas e incrementar su negocio", comentaba Pilar Martín, directora sénior de Ventas de TD Synnex España. "Estamos muy satisfechos con este hito que hemos alcanzado, pero no dejamos de trabajar en la mejora y ampliación de SMB Home. Estamos analizando la posibilidad de incorporar, en un breve plazo, toda una serie de mejoras, como notificaciones operacionales para nuestros clientes y nuevos programas de fidelización".

La jungla de los negocios

La parte formal del evento corrió a cargo de HP, HPE, Intel y Lenovo, que mostraron en breves intervenciones sus propuestas de mercado ante una audiencia de más de mil colaboradores, fabricantes, integradores y distribuidores. "Queremos expresar nuestra gratitud a nuestros ponentes y panelistas, cuyas presentaciones dejaron una profunda inspiración en todos los presentes. Sus conocimientos y experiencia compartida nos han brindado ideas valiosas y perspectivas frescas en el sector tecnológico".

Tras la inauguración del concepto Explora por parte de Luis, Marta y Pilar de TD Synnex, las Business Talks del primer día estuvieron a cargo de Melchor Sanz, *ceto* de HP, que contó con la ayuda del padre Olmedo (Nacha la Macha) para una divertida presentación con el tema de 'Mejorando la experiencia del trabajo híbrido'. Le siguió el turno de Fernando Hortal de HPE que describió el entorno Greenlake del core al extremo y la nube con 'Construye la nube que mejor se adapta a ti'. A continuación Elena del Campo Merino, EMEA CCG Sales Application Engineer de Intel, repasó los hitos de la compañía y el actual estado del arte con la 13ª generación de procesadores Intel Core. Finalmente, Carlos Serna, director de Canal y SMB Lenovo Iberia, sorprendió con una charla inspiracional que rompía muchos tabúes.

La segunda parte de Explora se articuló alrededor de tres grandes líneas de trabajo: presentaciones y conferencias por parte de TD Synnex y de destacados fabricantes; áreas o puntos de encuentro donde reunirse y trabajar junto con los principales proveedores; y un área de networking. En la convocatoria madrileña, los asistentes tuvieron la oportunidad de conocer de primera mano alguna de las propuestas tecnológicas y de servicio más innovadoras y avanzadas del momento.

"Explora ha sido una oportunidad única para conectar, aprender y disfrutar", dijo Pauli Amat, director general para Iberia de TD Synnex. "Hemos diseñado un espacio de trabajo, aprovechando el espectacular recinto donde se representa el musical de Nacho Cano 'Malinche', especialmente pensado para ampliar la red de contactos, aclarar dudas técnicas y hablar directamente con especialistas comerciales de los más importantes fabricantes. Y también queremos que sea un lugar de diversión y alegría. Tras cuatro años de parada, hemos vuelto a los eventos presenciales con más ganas y más ilusión que nunca, y queremos que sea algo inolvidable para todos. Queremos que Explora marque un antes y un después en nuestra relación con todos nuestros socios".

Concluido el espectáculo coreando algunas de las canciones más famosas de Mecano, todavía quedaba por delante la fiesta preparada en el Templo Canalla hasta altas horas de la noche. "No podríamos haber logrado este éxito sin el apoyo continuo de nuestros fabricantes patrocinadores. Su confianza en nosotros y su compromiso con nuestra visión son invaluables. Nos sentimos honrados de contar con su apoyo y esperamos seguir trabajando juntos en el futuro", concluye Marta Juderías. "Una vez más, queremos transmitir nuestro agradecimiento a todos por hacer de nuestro primer gran evento corporativo como TD Synnex un éxito rotundo. Vuestra participación y entusiasmo han dejado una huella imborrable en todos los que formamos nuestra empresa".

- **explora | Mejorando la Experiencia en el Trabajo Híbrido con HP**

Además de contar con su espacio que servía de punto de encuentro con los clientes en el evento corporativo de TD Synnex, como los otros 30 fabricantes, HP también formó parte de la plenaria de keynotes. En ella, Melchor Sanz, CTO de HP disertó sobre cómo mejorar la experiencia en el trabajo híbrido. "La pandemia de la covid-19 ha cambiado radicalmente la forma en que trabajamos y ha acelerado la adopción del trabajo remoto. Muchas empresas han adoptado modelos de trabajo híbrido que combinan el trabajo en la oficina con el trabajo desde casa o desde cualquier otra ubicación", señalaba Sanz. "Este nuevo modelo de trabajo presenta desafíos significativos para las empresas, especialmente en términos de la experiencia del usuario y la productividad. Los trabajadores necesitan dispositivos cómodos, seguros y gestionados de forma remota que les permitan trabajar de manera efectiva desde cualquier lugar".

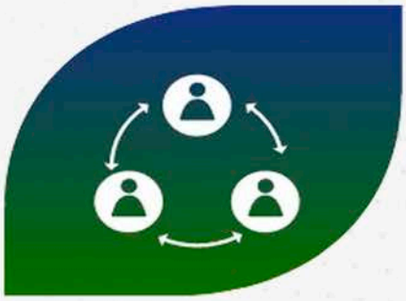
Es en este contexto, HP se presenta como una excelente oportunidad para que los asistentes de Explora pudieran conocer sus reflexiones y estrategias para mejorar la experiencia del usuario en el trabajo híbrido. Además de repasar las últimas tendencias y soluciones tecnológicas para el trabajo híbrido, HP mencionó mejores prácticas para garantizar que los trabajadores tengan una excelente experiencia de usuario, independientemente de su ubicación.

"En el tiempo en que se vendía a un cliente un ordenador -cinco o seis años- ahora puedes venderle casi doce móviles -uno cada seis meses-. Los ciclos han cambiado, y hemos tenido que ir abriendo el catálogo, de ahí la integración de compras como las de Poly (antes Plan-

inforpor

El Mayor referente en consumibles

Somos líderes del sector en España



Optimizamos la relación entre fabricantes y distribuidores

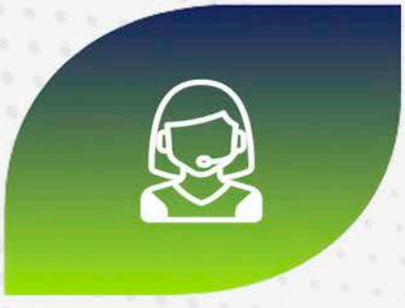
Ofrecemos diversidad de soluciones

Nuestro equipo humano, marca la diferencia

inforpor

Mayorista Global de Impresión

El catálogo más completo del mercado



Escuchar nos hace diferentes

La mejor apuesta por el Medio Ambiente

Servicios logísticos y financieros

tronics), con un amplio catálogo en periféricos y trabajo colaborativo".

- **explora | HPE GreenLake**

La plataforma HPE GreenLake Edge to Cloud Platform está diseñada para ofrecer una experiencia completa de la nube híbrida a cualquier tipo de empresa. De la mano de uno de sus consultores de tecnología, Fernando Hortal, se describió en el escenario como GreenLake permite gestionar las infraestructuras desde el extremo a la nube y ofrece la flexibilidad y facilidad de gestión necesarias para adaptarse a las necesidades del cliente. Además, se pueden integrar los servicios de los partners para enriquecer la experiencia de servicio en los clientes finales.

"La plataforma HPE GreenLake se puede personalizar para cada caso. Ofrecemos una experiencia completa de consumo de servicios en la nube, lo que permite que los clientes finales puedan acceder a los servicios que necesitan, independientemente de dónde se encuentren", señaló Hortal. "En un mundo donde la nube juega un papel cada vez más importante en la gestión de infraestructuras, HPE GreenLake se presenta como una solución completa y personalizable que se adapta a las necesidades de cada cliente".

- **explora | Intel y la 13ª generación de procesadores Intel Core**

Una de las charlas más esperadas en el evento corporativo de TD Synnex correspondía a la presentación de la 13ª generación de los procesadores Intel Core. Elena del Campo Merino, EMEA CCG Sales Application Engineer de Intel, expuso las características y tecnologías principales de la última generación de procesadores de Intel, que incluyen mejoras significativas en el rendimiento, la eficiencia energética y la conectividad. Además, se refirió a los diferentes productos que están equipados con esta arquitectura, desde portátiles y ordenadores de sobremesa hasta servidores y dispositivos de Internet de las cosas (IoT). "Intel es una empresa líder en tecnología de procesadores y ha estado a la vanguardia de la innovación en este campo durante muchos años", contaba Campo Merino. "Para tener una presencia ubicua y tender un puente entre los mundos físico y digital, hemos tenido que desarrollar cinco superpoderes: computación, conectividad persistente, infraestructura de la nube al extremo, inteligencia artificial, y sensorización".

- **explora | Lenovo, estrategia y supervivencia**

Cerraba el cuarteto de presentaciones la keynote de Carlos Serna, director de Canal y SMB Lenovo Iberia. En su charla, nos habló sobre los desafíos que enfrenta el sector y las estrategias clave para sobrevivir en un mercado altamente competitivo: "En un mundo en constante cambio y evolución, es esencial estar al tanto de los desafíos y las oportunidades que se presentan en el mercado para aprender sobre cómo navegar en un entorno empresarial competitivo y en constante cambio. Muchos de los factores a tenerse en cuenta para garantizar la supervivencia en el mundo empresarial actual están fuera de nuestro control, así que es mejor concentrarse en lo mejor que uno puede hacer y aportar guiado por la experiencia y el conocimiento".

Serna tiene claro las recetas: "Los PC cada vez tienen menos margen, y el precio es un gran determinante en la compra. Yo que soy muy cocinillas y me gusta el buen comer aplico un símil. La paella es la estrella de nuestra gastronomía, y no falta en cada casa, los ordenadores son lo que hoy nos da de comer. Pero hay que tener un ojo puesto en lo que se comerá mañana, e ir poniendo en remojo los garbanzos para estar preparados, por eso nuestra gran apuesta en infraestructuras de datacenter y en la movilidad con Motorola, que ya nos empieza a dar de comer muy bien. Y no debemos de olvidar de ir sembrando para estar listos con las cosechas que nos alimentarán en el futuro".

El director de Canal de Lenovo también se refirió a su negociado: "Tenemos que trabajar nuestras fortalezas, no potenciar las debilidades. Y nuestra fortaleza es que somos channel-first en todos los segmentos, 100% en ISG, 100% en telefonía, y solo en PC baja al 96% porque hay clientes tradicionales, normalmente con presencia en numerosos países, que prefieren tener una compra más centralizada. Pero para el resto de casos, incluida gran cuenta y administración pública, todo es 100% canal. Otros fabricantes tienen una proporción de 70/30, nosotros no, 100%. El canal es el que nos da de comer y no podemos molestar ni hacer nada contra el canal". Y después de una charla muy inspiradora, Serna terminaba con una reflexión: "No conozco a nadie que en su lecho de muerte se haya arrepentido de no haber trabajado más. Aprovechad la vida para disfrutar más de las cosas que os hacen felices, de las personas que queréis y os quieren".

TERMINALES PUNTO DE VENTA

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

POSBANK®

> APEXA
- > 15"/15.6"/19.5"/21.5".
- > Color Blanco o Negro.
- > Windows o Android.
- > Múltiples periféricos y configuraciones.

> MAZIC
- > Pantalla 15"/15.6".
- > Color Negro. Plegable.
- > Windows.
- > Múltiples periféricos y configuraciones.

> DCR
- > Pantalla 10".
- > Color Blanco o Negro.
- > Windows o Android.
- > Impresora 80mm.

> IMPREX PRIME
- > Pantalla 15"/17".
- > Color Blanco o Negro.
- > Windows.
- > Impresora 80mm..
- > Múltiples periféricos y configuraciones.

POSBANK TIENE UN ESTÁNDAR DE CALIDAD Y DISEÑO SUPERIOR.

CADA MODELO DISPONE DE VARIAS CONFIGURACIONES DE CPU: j3455, j6412, i3-G4, i5-G7 ...
SE PUEDEN INTEGRAR VISORES, LECTORES DE TARJETAS, MONITORES TRASEROS ...

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

> UNICO-W41N

- > Pantalla 15". 1024x768.
- > CPU 4125, 4+128GB.
- > Puede ir en pared.
- > Visor o LCD opcional.

> UNICO-W3N

- > Pantalla 15". 1024x768.
- > CPU i3-5005, 8+128GB.
- > Puede ir en pared.
- > Visor o LCD opcional.

> UNICO-W41NP

- > Pantalla 15.6". 1366x768.
- > CPU 4125, 4+128GB.
- > Puede ir en pared.
- > Visor o LCD opcional.

> UNICO-W5NP

- > Pantalla 15.6". 1366x768.
- > CPU i5-5200, 8+128GB.
- > Puede ir en pared.
- > Visor o LCD opcional.

> UNICO-WP5N

- > Pantalla 15.6". 1366x768.
- > CPU-i5-5200, 8+128GB.
- > Impresora Térmica 80mm.
- > Visor o LCD opcional.

> 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.

TERMINALES PUNTO DE VENTA ANDROID

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

SUNMI
Android POS Leader

> D2s

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

> D2s PLUS

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

> T2s LITE

- > Pantalla 15.6".
- > Opción 15.6" + 10"/15,6
- > Gama profesional.

> T2s

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

> D2 MINI

- > Pantalla 10.1".
- > Impresora 57mm.
- > Visor 4.3", NFC.
- > Gama económica.

> T2 MINI

- > Pantalla 11.6".
- > Impresora 80mm.
- > Visor, NFC, Lector QR.
- > 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 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.

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.


“Mi negocio vuela con las herramientas de gestión adecuadas”
sage.es
900 878 060
Sage
helping business flow