El **desarrollo** de los **negocios** de **valor, cima** en **V-Valley**

Alrededor de 80 profesionales reunió V-Valley en su III Encuentro Cataluña Summit que celebró en Baqueira Beret los días 7 y 8 de marzo, congregando a fabricantes y clientes. Dos jornadas que contaron con la celebración de tres mesas redondas en torno a las oportunidades que se le abren a su ecosistema en torno a la ciberseguridad, la nube, la infraestructura, las redes o la eficiencia energética.

A10 Networks, Acronis, Adobe, Allied Telesis, APC by Schneider Electric, Backbox, Check Point Software, Cloudflare, CyberArk, Dell Technologies, ExaGrid, Hitachi Vantara, Kaspersky, Salicru, Sailpoint, Trellix y Zyxel fueron los fabricantes presentes en el evento.

El Grupo Esprinet, en el que está incluida esta unidad consagrada al área del valor, es el mayorista líder en el sur de Europa. Un liderazgo que el pasado año se asentó en una facturación de 4.900 millones de euros y en la que V-Valley ya genera, en volumen, el 23 % de la compañía, con una participación de más del 50 % del EBITDA. Hugo Fernández, administrador delegado de V-Valley, insistió en la enorme solidez financiera que enarbola el mayorista gracias al despliegue de las operaciones en España, Italia, Portugal y el norte de África. Una cobertura que "nos concede mucha cercanía con el ecosistema de clientes, al que atendemos todas las necesidades". Un ecosistema de clientes, "que es nuestra fortaleza".

David Gasca, *sales & marketing manager cibersecurity* de V-Valley, defendió la enorme diversidad que exhibe la unidad de valor. "Contamos con equipos especializados para cada mercado. Somos flexibles y ofrecemos soporte, formación y consultoría para desarrollar cualquier negocio". El reto es ayudar a los *partners* a desplegar su negocio más allá de las áreas de las que tradicionalmente se han ocupado.

La regencia del dato

Perdido el perímetro de seguridad tradicional, el nuevo foco se pone en los datos y en la gestión de las identidades bajo un modelo de Confianza Cero, o *Zero Trust*, que garantiza que solo la entidad correcta puede acceder a los recursos necesarios. La gestión de datos; por tanto, va unida inexorablemente a la gestión de quién y cómo se accede a ellos. Son dos áreas con una gran oportunidad: el almacenamiento del dato, su gobernanza y

gestión; y la perfecta gestión de las identidades para acceder a él. Backbox, CyberArk, Dell Technologies, Exagrid, Hitachi Vantara y Sailpoint son fabricantes que arman su negocio en torno a este crítico activo.

Mar García, responsable de desarrollo de canal de Dell Technologies, recordó que todas las empresas quieren incrementar la productividad, obtener mejores rendimientos y conseguir una mejor optimización y capitalización de sus datos. "Fabricantes y *partners* debemos incrementar aún más nuestra especialización para saber responder a estas necesidades; si no, nos quedaremos atrás". En este abanico de necesidades, García recordó el papel, clave, que va a tener la inteligencia artificial como fuente de oportunidad o los retos, enormes, que se abren en los entornos *multicloud*. "Cuanto antes entendamos dónde está el dato y dónde se almacena, mejor. Los datos son cada vez más valiosos. Hay que saber manejar la complejidad y ayudar a las empresas a capitalizarlos".

> "Los datos son cada vez más valiosos. Hay que saber manejar la complejidad y ayudar a las empresas a capitalizarlos"
>
> **(Mar García. Dell Technologies)**

Eduard Alegre, *territory business developer* de la división Enterprise Security en V-Valley, que representaba a Backbox, recordó que en los últimos años "hemos pasado de defender castillos a defender lo más valioso, que es el dato". Backbox, como fabricante especializado en procesos de automatización, abarca todo tipo de tareas: desde *backups* de las configuraciones hasta la gestión de contraseñas. También la actualización permanente de todos los dispositivos; algo clave, "ya que los datos residen en ellos".

Valentín Pinuaga, director general de Hitachi Vantara en Iberia, cree que el canal está muy pendiente de cómo evoluciona el mercado; lo que sitúa al concepto del "*data driven*" como área esencial. "Dónde está el dato, cómo se protege y gestiona, cómo se almacena y se replica, es una de las máximas preocupaciones de las empresas". Pinuaga recuerda que la ciberseguridad es la puerta que abre el negocio en cualquier empresa. "Los clientes siempre te escuchan".

En este círculo alrededor del dato, la gestión de identidades se torna esencial. Juan Antonio de la Viña, preventa, consultoría y *product manager* en VValley en representación de Cyberark y Sailpoint, recuerda que ya no solo se trata de protegerlo y almacenarlo, sino de prevenir los robos de información y la suplantación de identidades. "Con la extensión del teletrabajo, el campo de actuación se ha ampliado y los usuarios pueden acceder desde cualquier lugar, a través de una conexión no segura, a los datos de la compañía", alerta.

"Es muy importante controlar y proteger a quién acceda, de qué manera lo hace y des-

> "La ciberseguridad es la puerta que abre el negocio en cualquier empresa"
>
> **(Valentín Pinuaga. Hitachi Vantara)**

de dónde. Sin olvidar que el dato siempre debe quedar auditado", enumera.

Tampoco se olvidan las enormes oportunidades que abre la tecnología de *backup*. David Blanqué, responsable de ventas en Iberia de Exagrid, recuerda que siempre existió pero que en los últimos años ha reforzado su valor. "Es la tecnología que permite recuperar el dato, susceptible de ser perdido, con el enorme impacto que puede tener esto en el negocio". Ahora bien, hay que reflexionar sobre lo que realmente es el *backup*. "No se trata de comercializar un producto", alerta. Atañe a una complejidad "que abarca desde la gestión de identidades hasta la prevención o la protección de red". Se trata de "hacer una venta cruzada; no solo es vender un producto, sino comercializar todo lo necesario para protegerse en todas las fases de un ataque".

Eduard Alegre recuerda que, dentro de los procesos de automatización de Backbox, está incluida la automatización del *backup*, capital. "Es absolutamente necesario que las empresas conozcan qué dispositivos tienen, en qué versiones trabajan y cuáles son sus vulnerabilidades, para mantenerlos completamente actualizados", explica. Automatizar procesos, incluido el *backup*, "ahorra tiempo a los equipos y evita errores".

Blanqué recuerda el complejo panorama de amenazas al que se deben enfrentar las empresas. "Hay una amenaza cibernética, que cada vez crece más, y que es mucho más latente y más potente", explica. Un panorama al que se suma el obligado cumplimiento de una legislación estricta en la gobernanza y la gestión de los datos. Para dar cumplida cuenta de todos estos retos, el directivo de Exagrid apela a los *partners*. "Deben entender qué es lo que se está exigiendo y cuál es la amenaza a la que se enfrentan las empresas. Para ello, tienen que dotarse de las capacidades consultivas necesarias para ser capaces de cartografiar los servicios, saber identificar qué es crítico y, en el caso de un ataque, ayudar a priorizar". Unas tareas que alcanzan hasta la auditoría. "Deben ayudar a ver qué grado de cumplimiento tienen sus clientes de las directivas". Se trata, por tanto, de unos proyectos que van mucho más allá de la venta de infraestructura. "Los CIO y CISO buscan un *partner* que les asesore y que les ayude a implementar una estrategia de ciberseguridad; acompañándoles en todo el proceso", insiste.

> "Automatizar procesos ahorra tiempo a los equipos y evita errores"
>
> **(Eduard Alegre. V-Valley en representación de Backbox)**

> "Los CIO y CISO buscan un *partner* que les asesore y que les ayude a implementar una estrategia de ciberseguridad"
>
> **(David Blanqué. Exagrid)**

En el área de las oportunidades, la ciberseguridad está en cabeza. Un área a la que están accediendo, incluso, los fabricantes dedicados a la gestión del dato. Para Valentín Pinuaga tiene todo el sentido. "Cuando tu negocio principal gira alrededor del dato y se observa que la seguridad es elemento de preocupación, desde los departamentos de ingeniería se busca complementar que, junto a la custodia y la disponibilidad del dato, se garantice su protección". Desde la perspectiva del *partner*, es aún más evidente. "Los clientes no están interesados en un producto para resolver un problema concreto, sino en alguien que les asesore desde un punto de vista global. La problemática de la seguridad no se puede abordar desde la parcialidad del almacenamiento del hardware, de la gestión del acceso, de la protección del dato o del *backup*. Hay que abordarla con un enfoque global".

Un horizonte de oportunidades en el que los modelos de infraestructura como servicio van a ocupar un gran espacio. Mar García apela al cambio que se está operando en la manera en la que las empresas consumen la tecnología. "Esta es costosa, incluye diferentes capas, con una complejidad creciente". A su juicio, estos modelos van calando poco a poco. "Requieren un proceso de evangelización. Son modelos que permiten abordar todas las necesidades de una empresa en un

> "Es muy importante controlar y proteger a quién acceda, de qué manera lo hace y desde dónde"
>
> **(Juan Antonio de la Viña. V-Valley en representación de CyberArk y Sailpoint)**

único proyecto; con la posibilidad de incluir a varios fabricantes y disfrutar de una facturación estable". El *partner* "logra una fidelización de su cliente y puede ofrecerle nuevos proyectos".

También la gestión de identidades ofrece un excelente panorama de negocio. Hay grandes ataques a las identidades, siendo el *phishing* la fórmula preferida por los *hackers* para suplantar identidades y usurpar cuentas para acceder a los datos. Un problema que afecta, por igual, a grandes o pequeñas empresas. "El eslabón más débil de la cadena es el usuario", recuerda Juan Antonio de la Viña. "Es muy importante la integración entre las soluciones y cómo nos hablamos con ellas", alerta. Es esencial establecer una serie de controles e, incluso, en el caso de que se consiga un usuario y una contraseña, el daño pueda ser minimizado. De la Viña apela al ciclo de vida de la identidad. "Hay profesionales que cambiaron de compañía o que fueron despedidos, y que mantienen su usuario, lo que supone un enorme riesgo. El cliente tiene que saber quién se conecta y establecer medidas proactivas para controlar si esa persona es realmente quien dice ser".

Seguridad "integral"

Si bien la nube ofrece numerosas ventajas, como la escalabilidad, la flexibilidad y la reducción de costes, también introduce nuevos riesgos de seguridad que deben ser cuidadosamente considerados. Una protección que debe ser integral, alcanzando aplicaciones, la red y, por supuesto, el puesto de trabajo. A esta seguridad "integral" se dedicó

> "La pyme está siendo consciente de la necesidad de estar protegida y es el canal el que tiene que encargarse de su protección"
>
> **(Gonzalo Echeverría. Zyxel)**

la mesa en la que participaron Check Point Software, Kaspersky, Trellix y Zyxel.

Una seguridad que sigue siendo un segmento "bendecido" por la oportunidad. Según la consultora IDC, el mercado de la seguridad en España mostró el pasado año un crecimiento respecto a 2022 del 9,2 %.

Un ritmo de inversión que no hace disminuir el número de amenazas que consiguen hacer diana en las empresas. Reconoce Gonzalo Echeverría, director general de Zyxel en España y Portugal, que a los "*hackers* nunca

> "Son claves soluciones que permitan proteger al usuario a través de sistemas de autenticación y con estrategias de confianza cero"
>
> **(Nicola Carparelli. Trellix)**

se les va a alcanzar. Nunca podremos cerrar la brecha, pero la oportunidad es enorme". Una brecha que es más crítica en la pyme, foco de negocio prioritario de la marca. "Es la eterna olvidada. Aunque ha incrementado su inversión en los últimos años, aún queda muchísimo camino por recorrer".

Nicola Carparelli, *channel & sales account manager* de España e Italia de Trellix, recordó el complicado panorama al que tienen que enfrentase las empresas, con ataques dirigidos incluso por determinados gobiernos, que se han recrudecido con las guerras. "Son claves tecnologías como el EDR que permiten una mayor visibilidad y soluciones que permitan proteger al usuario a través de sistemas de autenticación y con estrategias de confianza cero".

"La brecha se reduce invirtiendo más dinero", resume José Antonio Morcillo, director de canal de Kaspersky en España y Portugal. En el caso de la pyme, la clave está en externalizar la seguridad. "Es el *partner* el que tiene que ofrecer servicios especializados: el cliente jamás va a conseguir su nivel de calidad". Invertir en un producto, continúa, es un error. "Se entra en una competencia que maltrata los márgenes, tanto del fabricante como del *partner*. La clave es dar un servicio especializado sobre un producto de calidad".

El grado de profesionalización que ha alcanzado el cibercrimen es otro de los factores que explica el adelanto de los *hackers*. Sebastien Loisy, responsable de cuentas nominadas en Check Point Software, recuerda, para completar este complejo panorama, el concurso de la inteligencia artificial. "Su uso por parte de los ciberdelincuentes es, al menos, tan intenso como el que hacemos los fabricantes de seguridad". A su juicio, reducir la brecha implica poner barreras. "Hay un problema enorme de falta de recursos en todos los clientes", alerta. La oportunidad, por tanto, para los *partners* es enorme. "Ellos pueden desplegar la seguridad que necesitan con un servicio de prevención y respuesta".

España, país de pymes

El 98 % del mercado español empresarial son pymes. Unas empresas que exigen soluciones sencillas y adaptadas a sus necesidades y presupuestos; pero que cuenten con idéntica fiabilidad que las grandes. Gonzalo Echeverría asegura que ha mejorado su inversión. "La pyme está siendo consciente de la necesidad de estar protegida y es el canal el que

tiene que encargarse de su protección, con una labor de asesoramiento". Para ello, apela, una vez más, al concepto de *Zero Trust*, que "sigue siendo la base". Una oportunidad que también se extiende a la red. "La velocidad, medida en gigas, ya no es suficiente; hay que dar acceso a la pyme a wifi7 y a la disponibilidad de *switches* multigiga. La oportunidad, por tanto, va más allá de la ciberseguridad, alcanzando a la actualización de la red".

El principal problema de estas empresas es la falta de conocimientos y de recursos. Morcillo desvela que algunas instalan tecnologías como un EDR, porque así se lo exigen por el área de negocio en la que se mueven, y apenas sacan partido de todas sus funcionalidades. "Ya no basta con instalar una herramienta; hay que conocer las tendencias del mercado, qué es lo que está pasando y qué se está haciendo. En definitiva, hay que aportar inteligencia a estos servicios". ¿La solución? Una vez más, dejar su protección en manos del canal. "Nuestro MDR no es competencia para el *partner*", reivindica. Se trata de un servicio en el que el canal aprovecha la capa de inteligencia del fabricante para ofrecer protección y prevención. "Es el futuro".

> "Es el *partner* el que tiene que ofrecer servicios especializados: el cliente jamás va a conseguir su nivel de calidad"
>
> **(José Antonio Morcillo. Kaspersky)**

Nube y puesto de trabajo

El *cloud* es uno de los principales caballos de batalla porque hay que exigirle la misma ciberseguridad que se tiene dentro de la

red corporativa. Según un estudio de Check Point Software, el 76 % de las compañías españolas mostraba su preocupación ante el aumento de los ataques a las redes basadas en el *cloud*. Junto a este dato, al 59 % le preocupaban los errores de configuración de la infraestructura *cloud*. "Los clientes reconocen que hay un mayor riesgo ya que su LAN es la nube", recuerda Sebastien Loisy. El *multicloud* es una realidad, un entorno complejo de proteger porque las empresas no cuentan con especialistas en todas y cada una de las nubes. El directivo recuerda que hay herramientas de gestión del riesgo que permiten detectar y prevenir las brechas. "La seguridad debe observarse desde el principio. Integrarla al final cuando ya está todo montado abre muchos más riesgos. Para el *partner*, por tanto, la oportunidad está en integrarla al principio, con una estrategia que proteja el código".

> "Hay un problema enorme de falta de recursos en todos los clientes"
>
> **(Sebastien Loisy. Check Point Sofware)**

> "Es clave seguir acompañando a los clientes en su viaje hacia los entornos en la nube"
>
> **(Juan Muñoz. A10 Networks)**

Por último, el puesto de trabajo sigue siendo área esencial. Aunque las empresas han mejorado la protección en estos entornos el aumento de la zona de exposición abre nuevas vías de vulnerabilidad. Nicola Carparelli reconoce que los riesgos han aumentado. "El problema de la cadena es el usuario", advierte. A su juicio, es esencial que las empresas desarrollen una seguridad con una visión amplia que abarque "el correo electrónico, la red y la nube". El canal, a su juicio, "debe proporcionar valor añadido, especialmente en el segmento de mercado de las pymes".

Redes, gestión energética y continuidad de negocio

En el mundo actual, donde las empresas dependen cada vez más de las redes para sus operaciones diarias, la continuidad de negocio se ha convertido en un tema crucial. En este contexto, la red juega un papel fundamental al proporcionar la infraestructura necesaria para mantener las operaciones funcionando incluso en caso de interrupciones o desastres. Una red, segura, en un entorno en el que la gestión y la eficiencia energética son esenciales.

Según la consultora Context, el mercado de valor fue el segmento con mejor comportamiento el pasado año en España en el canal, con un crecimiento del 12 %. Un entorno en el que se ubican los negocios vinculados con el centro de dato, que creció un 29 %, la se-

> "Se trata de conseguir una seguridad *end to end*"
>
> **(Luis González. Allied Telesis)**

guridad y las redes, que se elevaron un 17 %. Juan Muñoz, director general de A10 Networks, asegura que las perspectivas son positivas para este 2024. "Es clave seguir acompañando a los clientes en su viaje hacia los entornos en la nube, con una transición cada vez más clara hacia el sabor híbrido", explica. Unos clientes que, cada vez, demandan más servicios y más conocimiento al canal.

Para Luis González, director de ventas de Allied Telesis, 2024 es un año de asentamiento. El fabricante, con muy buenos resultados en los últimos años, prevé volver a crecer. "Hemos aprovechado muchas sinergias que se han producido en estos ejercicios y ahora toca asentar tecnología y ver realmente qué es lo que está ocurriendo".

Un excelente panorama que se extiende al área de las aplicaciones, claves en el ámbito de la empresa. Son la base en el mundo digital y, por ello, siguen siendo en gran medida inseguras, siendo una de las dianas preferidas de los *hackers*. Juan Molina, *Network and Security Sales Engineer* de Cloudflare, asegura que el mercado crece a un gran ritmo brutal, sobre todo con la expansión del trabajo híbrido que ha provocado un completo cambio de paradigma. "El uso de la red se ha intensificado por el incremento de los servicios que se requieren, con lo cual la proliferación de aplicaciones en la web ha crecido exponencialmente". Un mayor uso que exige de más servicios de ciberseguridad para proteger las aplicaciones. "No se trata solo del tráfico web, sino el tráfico API que hay entre los sistemas. Hay un tráfico inmenso y la demanda ha crecido exponencialmente".

También se suman al optimismo fabricantes como Schneider Electric o Salicru vinculados al centro de datos y a las soluciones relacionadas con la continuidad de negocio y la eficiencia energética, Víctor Gago, *IT & ET Channel Sales Manager* de la división de Secure Power en Schneider Electric Iberia, recuerda que la digitalización está provocando que exista una enorme inversión en infraestructura y, específicamente, en tecnología vinculada con los centros de datos. La zona ibérica, y especialmente España, "está atrayendo muchas inversiones por motivos geográficos, de estabilidad jurídica y, por supuesto, por nuestro acceso a las energías renovables". Asegura que solo se está viendo la punta del iceberg. "Se estima que la base instalada en energía consumida en el centro de datos es de unos 180 megavatios y

> "La proliferación de aplicaciones en la web ha crecido exponencialmente"
>
> **(Juan Molina. Cloudflare)**

la previsión es que antes de 2030 podremos alcanzar los 1.100 megavatios; lo que señala un enorme crecimiento. Sin lugar a dudas, el área del centro de datos va a traer grandes crecimientos en los próximos años".

Tecnologías emergentes como el *big data*, el IoT, la inteligencia artificial, el *cloud* o la implementación del 5G van a impulsar, "tanto la demanda en torno al centro de datos tradicional como al *edge computing*, cada vez más valorado por la cercanía y por la rapidez de acceso a los datos", explica Alex Castellvi, responsable de desarrollo de negocio en la pyme de Salicru. En 2023, el negocio de los centros de datos movió a nivel mundial en torno a 11.000 millones de dólares. "La previsión es que en 2033 alcance los 60.000 millones de dólares". Ambos fabricantes han desplegado una poderosa estrategia en torno a uno de los conceptos con más valor en estos momentos, sobre todo en su acercamiento al *edge* y al centro de datos: la sostenibilidad. Incluso V-Valley este año va a conformar una división centrada en el desarrollo de la tecnología vinculada con la energía y la eficiencia energética. "La sostenibilidad ya no es una opción, es un mandato", asegura Víctor Gago. Un concepto más interiorizado en las grandes compañías que lo han asimilado en su estrategia corporativa "porque les da acce-

> "La sostenibilidad ya no es una opción, es un mandato"
>
> **(Víctor Gago. Schneider Electric)**

so a más financiación y a más reputación, en definitiva, a más valor en el mercado". Y, a su juicio, se trata de un concepto que cada vez cala más. "Nos hemos convertido en un asesor del canal en este camino hacia la sostenibilidad gracias a nuestro propio compromiso con ella". Una labor de asesoramiento que alcanza su relación con el cliente, para ayudarle a definir un plan de sostenibilidad y a medir sus resultados. También soporte en su propia estrategia sostenible y, por último, la reducción de la huella de carbono gracias al diseño de soluciones que permiten disfrutar de una visibilidad de esta huella y del impacto en los planes de sostenibilidad.

Alex Castellvi reconoce el incremento de la concienciación, a nivel individual, sobre estos temas y el compromiso del fabricante con el diseño de equipos más sostenibles. Aunque tiene claro que el canal sí ha aumentado su compromiso por este asunto, duda si es un factor clave en las decisiones de compra de las empresas. "Tanto los fabricantes como el canal somos conscientes de que hay que ir hacia la sostenibilidad plena. Dudo, sin embargo, si una solución más eficiente tiene más peso en la decisión del cliente".

Seguridad y red

Un área de clara sinergia para el canal es el que protagonizan las redes y la seguridad. Los *partners* especializados en una u otra área han sabido dar el salto hacia el despli-

> "Va a aumentar la demanda tanto del centro de datos tradicional como del *edge computing*"
>
> **(Alex Castellvi. Salicru)**

gue de proyectos globales. Luis González recuerda que estas sinergias también se observan en la oferta y que se buscan elementos de integración entre diferentes fabricantes. "Se trata de conseguir una seguridad *end to end*". Es el caso del fabricante, en sus propias instalaciones, con equipos propios y controladores capaces de entenderse con los *firewalls* o con sistemas de seguridad de terceros, para advertir de posibles problemas para actuar en el área de las redes. El director de ventas de Allied Telesis defiende el compromiso de la marca con la sostenibilidad, con una estrategia que incluye sus procesos de fabricación. Un compromiso que, advierte, "no es percibido por todas las empresas; algunas siguen priorizando otros conceptos como el precio".

Juan Muñoz recuerda la evolución de A10 desde los entornos de la infraestructura hasta la seguridad. "Una transición que también la está haciendo el canal y que supone una ampliación de los interlocutores con los que

Los servicios financieros, claves

El soporte financiero es una de las áreas más importantes en un mayorista. Desde hace años, Esprinet ha desplegado diferentes opciones, como el *renting*, el préstamo o la venta a plazos, por ejemplo, a las que se ha unido, recientemente, una solución propia de *renting*. Ana Martínez, responsable del departamento de Soluciones Financieras del Grupo Esprinet, recordó que la manera en la que las empresas adquieren la tecnología ha cambiado. "El avance digital tan rápido que estamos viviendo ha llevado a las empresas a demandar nuevos modelos de adquisición", completó.

La modalidad de alquiler propia de Esprinet cuenta con el respaldo financiero del mayorista. Martínez señala su flexibilidad, adaptándose a las necesidades del negocio de cada *partner*. "Se elimina la burocracia contractual, simplificándola, aunando todo en una misma cuota". Además de ser multiproducto, incluye servicios vinculados, por ejemplo, con la protección del dispositivo, la gestión de incidencias bajo la garantía de los fabricantes, la sustitución temporal del dispositivo, el borrado de datos a la finalización del alquiler o la recogida. "Se trata de proporcionar, además del dispositivo, un pago por un uso de servicios". No se olvida la apuesta por la sostenibilidad ya que a la finalización del alquiler hay una renovación tecnológica ya que al dispositivo se le da una segunda vida.

Javier de la Cruz, *account manager de device as a service* (DaaS), recordó que los ciclos de vida de los dispositivos o de la propia tecnología se han acortado. "Nuestro reto es proporcionar la solución financiera que mejor se adapta a cada uno de nuestros clientes".

hablan en las empresas: junto al responsable de seguridad, que define la estrategia de protección, está el que se encarga de gestionar la infraestructura; lo que exige una versatilidad en el integrador".

En el ámbito de las aplicaciones, las empresas deben gestionar tanto las aplicaciones instaladas en los entornos *onpremise*, como las nativas en la nube. Juan Molina recuerda que las primeras exigen contar con una persona experta en su gestión y protección. "Sin embargo, la misma aplicación, en la nube, disfruta de la protección que ofrece el servicio en la nube, lo que no requiere personal dedicado. Un servicio que aprende continuamente gracias a la información que recibe de todos los ataques que se producen a nivel mundial", especifica. El responsable de Cloudflare asegura que, tarde o temprano, "se producirá una migración de todas las aplicaciones al *cloud*".