linkedin
twitter
newsbook.es

>> La revista del distribuidor informático

Newsbook

Tai editorial

Año XXIX Nº 305 Junio 2023 0,01 Euros

La seguridad: bolsa de rentabilidad para el canal

La oportunidad del mercado de la seguridad se mantiene: IDC asegura que el ritmo de crecimiento es del 9,2 % este año

Seguridad en el canal: exigencia, formación y eterna oportunidad

Mucho se le exige al canal que se encarga de desplegar protección en España a todo tipo de empresas, de cualquier tamaño y condición. El carácter crítico del área de la ciberseguridad, con un panorama que, al mismo ritmo que crecen las amenazas, se carga de una mayor complejidad para desplegar la seguridad requerida para detectarlas y paralizarla a tiempo. A cambio, es un canal que disfruta de un enorme caudal de negocio ya que la seguridad es área de inversión prioritaria. Un canal en el que los mayoristas, como es el caso de Arrow, Exclusive Networks y V-Valley se han asentado como figuras imprescindibles.

Marilés de Pedro

Panorama complejo

Según los datos del Instituto Nacional de Ciberseguridad de España (INCIBE), en 2022 se detectaron, desde su Centro de Respuesta a Incidentes de Seguridad (INCIBE-CERT), 118.820 incidentes, un 9 % más respecto al año anterior. En el análisis que hace el instituto, 1 de cada 3 incidentes son una filtración de datos (sensibles, protegidos o confidenciales que son robados por una persona no autorizada); y 2 de cada 5 son vulnerabilidades de sistemas tecnológicos (debilidad de un sistema que puede poner en riesgo su seguridad). Un panorama que no parece contar con demasiado espacio para la mejora en este 2023. "El número

"El conocimiento que se le exige al *partner* que se dedica a desplegar la seguridad es muchísimo mayor que en cualquier otro sector"

Ángel García
director del área de Seguridad en **Arrow**

de amenazas sigue aumentando año tras año", recuerda Ángel García, director del área de Seguridad en Arrow. "Los ataques son cada vez más sofisticados con el objetivo, evidente, del fin económico". En la lista de amenazas, a la cabeza, el *malware*, que se incrementa vía ataques a los dispositivos de IoT. "Han aumentado las amenazas encriptadas destinadas a comprometer el puesto de trabajo. También es especialmente preocupante el robo de identidades y los accesos privilegiados", analiza.

David Gasca, *sales & marketing manager cibersecurity* de V-Valley, apunta la gravedad en torno a las credenciales; un asunto que ratifica Gartner que predice que el 50 % de las brechas de seguridad en este 2023 apuntarán a ellas. "Es un tema muy grave", analiza. "Ya nos movemos en múltiples entornos (nube, *onpremise*, entornos híbridos, el uso de múltiples aplicaciones, etc.), lo que provoca un mayor número de errores por una mala gestión de las credenciales", relata. Su gestión, de una manera segura y unificada, va a ser esencial. Junto a este crítico tema, Gasca recuerda el protagonismo de tecnologías como SASE y SSE (Security Services Edge). "Se trata, en definitiva, de lograr que las empresas disfruten de una seguridad extremo a extremo".

El *ransomware*, ¿en la cumbre?

Después de un 2021 récord, los ataques de *ransomware* siguieron en 2022. Según el informe de amenazas de Sonicwall, durante los nueve primeros meses del pasado año aumentaron en EMEA un 38 %. Es más fácil que nunca realizar ataques de *ransomware*. Con las ofertas de *ransomware as a service* (RaaS), incluso los ciberdelincuentes menos técnicos pueden comprar kits de *ransomware* en la *dark web* y apuntar a organizaciones con experiencia mínima.

"Es un enorme negocio", recuerda José Manuel Medina, director de Desarrollo de Negocio de Exclusive Networks Iberia. El *ransomware* mueve unos 40.000 millones de dólares en el mundo. "Es un negocio enormemente lucrativo y, por tanto, va a seguir siendo una de las amenazas más importantes".

No es fácil protegerse del *ransomware*. "Muy pocas empresas tienen una seguridad bien planteada", valora David Gasca. A la falta de presupuesto para adquirir y diseñar un buen sistema de protección, hay que unir la necesidad de contar con un conocimiento profundo para configurarlo de manera adecuada. "El *ransomware* es más avanzado cada vez. Se basa en la intervención del usuario, que muchas veces tiene más privilegios de los que debería", continúa. Un complejo panorama al que se une la "perfección" que alcanza el *phishing*, la técnica más habitual. "Son cada vez más sofisticados: ya no cuentan con faltas de ortografía, son coherentes, están bien escritos. Vamos a sufrir una oleada de *ransomware* creado, en ocasiones, con herramientas que cuentan con una lógica de conversaciones tan profunda que van a engañar aún más al usuario".

Ante esta avalancha de *phishing*, los representantes de los mayoristas aseguran que se ha notado un incremento de la inversión de las empresas en herramientas de concienciación y de formación para sus empleados. "El eslabón débil sigue siendo el usuario", recuerda Ángel García.

Entorno *cloud* en peligro

A medida que las empresas siguen incorporándose a la nube se encuentran con el reto de gestionar la complejidad de la protección de sus infraestructuras a través de múltiples plataformas. Según un informe de Check Point Software, los incidentes relacionados con la protección de la nube aumentaron un 10 %. "Es la mayor oportunidad para el canal", asegura David Gasca, quien pinta un panorama, curioso, en el que los *partners* dedicados al desarrollo del *cloud* no despliegan soluciones de seguridad y, por el contrario, las compañías que ofrecen protección no incluyen el entorno del *cloud* en su oferta. "La oportunidad,
por tanto,

José Manuel Medina
director de Desarrollo de Negocio de **Exclusive Networks Iberia**

"El canal tiene que seguir prescribiendo. Y una vez que realice esta prescripción, ofrecer unos servicios gestionados potentes que permitan que todo funcione correctamente"

se abre en ambos mundos. Las compañías cuyo negocio está en la nube, y aunque la seguridad en este entorno ha mejorado muchísimo en los últimos años, no está integrada con la protección tradicional que está desplegada en el resto de las áreas (oficinas, *endpoint*, dispositivos móviles, etc.). Sin lugar a dudas, hay muy pocos *partners* que sean capaces de dar servicio a los dos mundos".

Ángel García suma la complejidad del entorno *multicloud*, que exige una compleja gestión. "El distribuidor que sea capaz de acompañar al cliente hacia la nube incrementará su negocio. Y, en esta transición, ese cliente final sigue confiando en que su *partner* de seguridad tradicional le ofrezca la solución completa". Un panorama en el que los hiperescalares ya cuentan con su propia oferta de soluciones de seguridad para protegerlo. "Van a aparecer fabricantes de seguridad con su propia *cloud*", completa el responsable de Seguridad de Arrow.

José Manuel Medina recuerda que el *partner* de *cloud* no tiene conocimientos de la seguridad tradicional. "Está focalizado en una determinada nube (Microsoft Azure, AWS o Google) y aplica la seguridad que ésta ofrece pero no conoce las herramienta de las otras *cloud* porque es muy complicado tener un conocimiento de todas las nubes. Sin embargo, los *partners* más tradicionales del mercado de la seguridad sí tienen una visión mucho más horizontal. Y son ellos a los que llaman sus clientes para que les ayuden a proteger sus cargas en la nube". Y todo desde un único punto. "En el *cloud* no podemos crear islas independientes, con sistemas de protección independientes. Hay que gestionar la seguridad desde un punto único".

Ángel García suma también el área del centro de datos. "Para armar un discurso completo de protección de las cargas en el *cloud*, el *partner* centrado en el entorno de la seguridad tiene que comprender también el centro de datos", alerta. "Hablamos, por tanto, de un "súper" *partner*, protagonista de las transiciones al *cloud*, con un conocimiento global. Se trata de un entorno muy complejo".

La eterna protección del puesto de trabajo

El espacio de trabajo sigue siendo principal campo de ataque. Un entorno que tras la expansión que ha experimentado el teletrabajo ha aumentado aún más su criticidad debido a que la intensidad de los ciberataques se ha incrementado, exponiendo a las compañías a nuevas vulnerabilidades. La protección del puesto de trabajo, que sigue siendo una pieza clave en el negocio de seguridad de los mayoristas, está creciendo muy rápido y de forma muy potente.

Un entorno en el que la progresiva introducción de las soluciones EDR (detección y respuesta) y XDR (detección y respuesta extendidas) ha exigido al canal un mayor conocimiento. "El canal tiene que seguir prescribiendo. Y una vez que realice esta prescripción, ofrecer unos servicios gestionados potentes que permitan que todo funcione correctamente e integrar en esta propuesta soluciones complementarias", recomienda José Manuel Medina. No olvida la visibilidad. "Es importantísima. Y no solo la del *endpoint*, también hay que observar la red y la nube".

Recuerda David Gasca que el conocimiento que tiene el canal del cliente final es insustituible. "Es su mayor valor". Y para sacar un buen provecho, tiene que estar suficientemente capacitado. "Son los distribuidores los que van a dar realmente un servicio adecuado y bien ajustado a lo que requiere su cliente. Esta relación es su salvoconducto para que no le sustituyan por un servicio paquetizado".

La oportunidad del OT

La protección de los entornos OT sigue creciendo. Un entorno, complejo, en el que prima, como recuerda José Manuel Medina, la disponibilidad. "Existen soluciones muy potentes para asegurar estos entornos", comenta. "Es esencial

Habilite las medidas de Seguridad, en cualquier lugar

Proteja los intereses y las posibilidades de su negocio sin limitar a empleados, clientes o proveedores.

arrow.com/globalecs/es

ARROW

David Gasca
sales & marketing manager cibersecurity de **V-Valley**

> "La protección de la nube es la mayor oportunidad para el canal"

que las empresas disfruten de una visibilidad: qué está pasando, cómo está pasando, qué protocolos se utilizan (son protocolos completamente diferentes) y cómo protegerlo". Un entorno, amenazado, y que exige un incremento de los niveles de protección. El informe global sobre el estado de la tecnología operacional y la ciberseguridad 2022 de Fortinet desveló que los entornos de control industrial siguen siendo un objetivo para los ciberdelincuentes, con el 93 % de los entornos OT experimentando una intrusión en los últimos 12 meses. Como resultado de estas intrusiones, casi el 50 % de las organizaciones sufrieron una interrupción de las operaciones que afectó a la productividad. Un tercio de los encuestados declaró que estas intrusiones de seguridad afectaron a sus ingresos, a la pérdida de datos, al cumplimiento de la normativa y al valor de la marca.

En España hay una enorme oportunidad ya que el sector industrial es enorme. Y más allá, alcanza a sectores como la agricultura, el eólico o el segmento cerámico, entre muchos otros. "Se trata de dispositivos que están conectados a la red, monitorizados, y que deben estar protegidos. Son susceptibles de ser atacados y, naturalmente, son más vulnerables.

Retener el talento

El sector TIC es uno de los grandes empleadores en España. Según los últimos datos del INE en 2020 la cifra de profesionales superaba ampliamente el medio millón de puestos. Un volumen, alto, que sin embargo sigue siendo escaso en algunos sectores como es el de la ciberseguridad que presentan mayor oferta que demanda. Los altos conocimientos que exige su desempeño y el carácter crítico de la ciberseguridad así lo han marcado. Según el Observatorio Nacional de Tecnología y Seguridad (ONTSI), la demanda de talento en ciberseguridad doblará a la oferta, requiriendo a más de 83.000 profesionales de este ámbito en 2024. Para Innovery, especialista en soluciones que blindan las tecnologías de las empresas, el experto en ciberseguridad es el perfil profesional de más futuro y su demanda será aún mayor en los próximos años.

A nivel mundial el panorama es similar: un estudio del organismo industrial ISACA, que recoge la opinión de más de 2.000 profesionales de la ciberseguridad en todo el mundo, concluye que el 63% de las empresas tiene puestos de seguridad sin cubrir y el 62 % considera que sus equipos carecen de personal en temas de ciberseguridad. Por otro lado, una quinta parte de los encuestados afirma que tarda más de medio año en encontrar candidatos cualificados para los puestos vacantes. Además, el 60 % afirma tener problemas para retener a su personal actual.

Según ISC, el déficit de competencias en ciberseguridad a nivel mundial asciende a 2,7 millones de trabajadores en todo el mundo, incluidos casi 200.000 en Europa.

El mercado mayorista no es ajeno a esta realidad y las fórmulas para formar y retener el talento no son sencillas de aplicar. Medina recuerda que hay que formar al talento joven. "Hay que ofrecer un proyecto de empresa atractivo y una formación de carrera".

La demanda de talento, como recuerda Ángel García, es enorme. "Se necesitan muchos profesionales y cada vez más". También apuesta por construir perfiles junior e ir haciéndoles crecer. "Debemos crear una cultura de compañía con los empleados, que incluya conocer sus necesidades para retener ese talento. También la conciliación entre su vida personal y profesional, y que puedan desarrollar un plan de carrera, poniendo a su disposición herramientas para que siga creciendo a nivel profesional".

En esta formación del talento joven todas las empresas se enfrentan a un reto idéntico: se trata de un perfil muy "proclive" al cambio y a ser contratado, una vez formado, por empresas con mayores salarios. "En un mercado como el de la ciberseguridad, en el que un profesional con cuatro años o cinco años de experiencia ya cuenta con un excelente nivel de formación, es muy complicado retener el talento", asegura David Gasca, que recuerda un elemento fundamental: la constitución de los mejores equipos exige todo tipo de perfiles. "Aprecio mucho la adaptación de aquellos profesionales que ya han superado la fase de ansiedad de crecimiento exponencial; esas personas senior, con ganas de adaptarse y que buscan la estabilidad que te da un entorno laboral donde van a poder seguir desarrollándose".

V-Valley
enhancing your business

ESPECIALISTAS EN ADVANCED SOLUTIONS

Mayor rentabilidad y valor en tus proyectos de Ciberseguridad Corporativa

Acompañamos a los clientes a potenciar, aún más, sus proyectos de transformación digital dirigidos a clientes finales y Administraciones Públicas.

BARCELONA | BILBAO | MADRID | LISBOA | SEVILLA | ZARAGOZA

Amplia gama de tecnologías que se ofrecen en modelos on-premise o como servicio

Organización altamente especializada

Extenso conjunto de servicios a disposición de los players del sector

Network | Cloud | Workplace | Aplicación | Dato | Gestión

A10 BACKBOX BROADCOM CHECK POINT CLOUDFLARE CounterCraft CyberRes ENTRUST JUNIPER NETWORKS

kaspersky McAfee MICRO FOCUS ravenloop Skyhigh Security SONICWALL Trellix TREND MICRO VU WatchGuard

www.v-valley.es

seguridad@v-valley.com

El espectro que se abre al sumar esos dos mundos, el mundo tradicional y el mundo del OT, es crítico". Unos entornos en los que la visibilidad y el control son esenciales. "Las empresas ya contaban con herramientas de control y visibilidad en el área TI, y ahora hay que sumar soluciones similares en el área OT", recuerda Ángel García.

La presencia de fabricantes en este mercado no deja de aumentar: a la lista de fabricantes específicos, focalizados en este negocio, se están sumando fabricantes tradicionales de seguridad que están lanzando líneas específicas de producto para el entorno OT. En España es un mercado que está creciendo a una enorme velocidad.

Gasca alerta de las conexiones a las que están sujetos los dispositivos. "Están conectados a redes 5G públicas o privadas, lo que les hace estar más expuestos todavía. El 5G no está pensado para ser seguro. Su base de conocimiento es ser rápido y estar disponible, pero no la seguridad. Las redes 5G diseñadas por cualquier empresa, con sus antenas y puntos de acceso, es una zona de ataque para los maleantes".

La movilidad, siempre pendiente

Una de las áreas con mayor recorrido sigue siendo la protección de los dispositivos móviles. Según Proofpoint, a principios del pasado año se había detectado un aumento del 500 % en los intentos de envío de *malware* para móviles en Europa. "Sigue siendo un área sin protección porque a los usuarios empresariales todavía les cuesta aceptar el control de la seguridad en su dispositivo", afirma Medina.

Como bien recuerda David Gasca, los departamentos TI de las grandes empresas establecen políticas de seguridad en los dispositivos que cuentan con un doble entorno, el personal y el profesional. "En el momento en el que se desciende en la pirámide empresarial, nadie obliga a establecer medidas de seguridad; a lo que se une que la seguridad es incómoda. Muchas pymes solo toman medidas cuando han sufrido un ataque".

El número de ataques de *phishing* al móvil se incrementa año tras año. "El dispositivo móvil es un "ordenador" con informaciones críticas que se comparten y se almacenan en la nube", recuerda Ángel García, a quien le parece llamativo que no sea "lo que primero se protege". Conscientes de este reto, el responsable de seguridad de Arrow explica que cada vez más los fabricantes sacan líneas de negocio específicas para este entorno.

Mucha inversión

Según la consultora IDC, el mercado de la seguridad en España está mostrando este año un crecimiento respecto del año pasado del 9,2 %, alcanzando los 2.130 millones de euros. Para 2026 podría superar la barrera de los 2.995 millones de euros, manteniendo ritmos de crecimiento similares que se acercan al doble dígito (9,9 %).

Ángel García apunta la enorme inversión que se ha desplegado en el área de la protección del *endpoint*, SDWAN y SASE. "También hemos notado un aumento de la seguridad en los entornos IT y OT, en los modelos de transición hacia la *cloud* y en las herramientas para formar y concienciar al usuario", completa.

Una lista a la que José Manuel Medina suma la gestión de cuentas privilegiada (PAN) y Gasca el CDN (red de distribución de contenidos) y WAF en la nube, lo que habla del carácter crítico de la disponibilidad en la nube y de la protec-

Seguridad gestionada

Según Gartner, en 2025 el 50 % de las empresas disfrutará de la seguridad como un servicio gestionado. Un modelo que se espera que galope a un crecimiento de entre el 17 y el 20 % en los próximos años, muy por encima del crecimiento orgánico del sector. Aunque los mayoristas señalan que esta fórmula marca la tendencia del segmento, no observan una transición tan radical. "Es una grandísima oportunidad", observa David Gasca. A su juicio, si los *partners* que se encargan de desplegar la seguridad, decidieran dar el paso a la nube, deberán ofrecer un modelo como servicio; que es la fórmula imperante en estos entornos.

Ángel García repasa las dos vertientes que ofrece este modelo. En el área corporativa, por la complejidad del entorno, la exigencia de responder de manera inmediata y el uso de un mayor número de aplicaciones, muchas empresas optan por combinar su seguridad con este tipo de servicios. "Es imposible gestionar y disfrutar de un control total". También en las pymes. "La flexibilidad de este modelo les permite ir introduciendo capas de seguridad, abonando cada mes una cantidad por la protección del *endpoint*, el *firewall*, etc. Se trata de un gasto, creciente o decreciente, en función de sus necesidades; que se adapta al negocio", recuerda el directivo de Arrow.

José Manuel Medina distingue en el canal entre los grandes *partners*, que además de desplegar su conocimiento en el área de los sistemas, ya han incluido la seguridad; y los *partners* especializados en este apartado, con una enorme experiencia, que cuentan con un SOC y ofrecen una cartera de servicios.

David Gasca recuerda que, aunque el negocio que hacen todavía es pequeño, ya existen fabricantes que han sido capaces de desplegar un modelo "puro" de MSP. "Es una fórmula en la que todos los fabricantes quieren estar y, más o menos rápido, todos están empezando a desplegar sus propuestas".

La ciberseguridad *cloud*, el camino hacia la transformación digital

A medida que aumenta el consumo de productos y servicios creados en torno al cloud, las empresas son más conscientes de la importancia de proteger no sólo sus datos y los de sus clientes, sino también su propia infraestructura.

La creciente dependencia de las tecnologías de la nube está generando una mayor presión. Por ello, establecer una correcta estrategia de gestión y protección de estos entornos es ahora una prioridad, máxime cuando los episodios de ataques de ciberseguridad, filtraciones de datos y accesos no autorizados no paran de crecer, aprovechando que la inmensa mayoría de las provisiones y cargas en el *cloud*, ya sean en modo SaaS, IaaS o PaaS, se encuentran aún en un proceso de adición de mecanismos de seguridad adecuados.

> "Con X-OD el canal puede transformar su modelo de negocio, liberar sus flujos de caja y mantener un beneficio estable"

Las organizaciones tienen que asumir que el *stack* de seguridad tradicional no es suficiente cuando los usuarios pueden estar en cualquier lugar y accediendo con cualquier dispositivo a recursos de la compañía, ya estén alojados en un *datacenter* propio, en *cloud* pública o en entornos SaaS, y por ello, la mejor aproximación de seguridad es la protección total, desde el *endpoint* hasta el dato, sin importar dónde se encuentre este.

Los cibercriminales han avanzado mucho en los últimos años, desarrollando fórmulas de ataque adaptadas a los nuevos usos y costumbres, además de técnicas de camuflaje para eludir los sistemas de detección. Así, siguen dándose amenazas de *ramsomware*, campañas de *phishing* y descargas de *malware* (troyanos, *phishing*...), impulsadas estas últimas por el incremento de las técnicas de ingeniería social y de funcionalidades maliciosas. Tampoco podemos olvidarnos de los ataques internos, lo que está llevando a las empresas a desarrollar renovadas estrategias de control orientada a este tipo de amenazas.

Exclusive Networks, el socio de confianza

Ante tal proliferación de ataques, son cada vez más las empresas que deciden establecer una estrategia que les permita mitigar e intentar detener estos ataques masivos, y deseosas de encontrar una solución eficiente, más allá de las propuestas tradicionales.

Como mayorista especializado en ciberseguridad, Exclusive Networks posee una completa oferta de soluciones de seguridad dirigidas a comprender y proteger estos entornos. Desde el perímetro y el bastionado del puesto de trabajo, hasta la propia gestión de la infraestructura. También si se trata del más puro enfoque *cloud* público, desde el mero Cloud Security Posture Management (CSPM), Cloud Workload Protection (CWPP), *serverless* o la microsegmentación, a soluciones de protección de secretos y accesos, que nos garanticen la disponibilidad y continuidad de nuestro negocio.

Para los entornos híbridos, Exclusive aborda estos desafíos mediante una combinación de soluciones de seguridad basadas en la prevención, detección y mitigación de amenazas y que cubren múltiples vectores de amenazas (*email*, *endpoint*, *cloud*, web...), independientemente de la tipología de acceso y usuarios, y de la localización de los datos y de las aplicaciones.

Para facilitar el acceso a su canal de distribución a estas tecnologías, Exclusive cuenta con X-OD, Exclusive On Demand, su servicio de suscripción para el consumo de tecnología, que incluye tanto hardware como software y que permite personalizar las soluciones de ciberseguridad contratadas. Con X-OD los integradores y *resellers* pueden transformar su modelo de negocio, liberar sus flujos de caja y mantener un beneficio estable en los proyectos.

José Manuel Medina,
director de desarrollo de negocio de
Exclusive Networks

ción de aplicaciones. "Tras la pandemia, las empresas han puesto en manos de los usuarios muchas más herramientas digitales. El comercio electrónico ha crecido muchísimo, se consumen más servicios a través de Internet y los ciudadanos, en el espectro público, utilizan mucho más los portales de la Administración", relata el responsable de marketing y ventas del área de seguridad en V-Valley.

Respecto a los mercados, sigue persistiendo la brecha económica entre el mercado de la pyme y el área *enterprise*. La primera, aunque ha aumentado su capacidad de inversión, sigue siendo el segmento de mercado que más debe invertir. "Hay que ayudarla con buenos servicios. Son los *partners* más pequeños los que están más cerca de este tipo de empresas. Hay que crear paquetes, fáciles de implementar y que integren unos servicios mínimos", explica José Manuel Medina.

La Administración Pública fue el motor del segmento de la ciberseguridad en 2022, con mercados como la sanidad, la defensa y la educación como sectores claves. En este 2023, y a pesar de que muchos ministerios ya tienen adjudicados sus presupuestos, las licitaciones se están retrasando, lo que apunta a una cierta ralentización en la segunda parte del año. Sin embargo, los fondos NextGenerationEU van a seguir tirando de este segmento y serán un revulsivo para los próximos años.

El canal de seguridad, crítico

El carácter crítico del mercado de la ciberseguridad exige al canal encargado de desarrollarlo un enorme conocimiento. "Por la diversidad, enorme, de soluciones y la complejidad del mercado el *partner* que se dedica a este apartado es el que más conocimiento y formación requiere", señala el responsable de desarrollo de negocio de Exclusive Networks.

La evolución, siempre rápida en el mercado de la tecnología, es aún más acelerada en el área de la ciberseguridad y exige expertos en todos los segmentos. "Desde técnicos especializados en SIEM, en respuesta a incidentes o en protección del *endpoint* hasta profesionales expertos en tareas de orquestación, en el despliegue de *firewalls*, etc.", enumera Gasca.

"El conocimiento que se le exige al *partner* que se dedica a desplegar la seguridad es muchísimo mayor que en cualquier otro sector", ratifica Ángel García. Es un mercado que se mueve muy rápido, con unos crecimientos enormes, casi siempre a doble dígito, en el que cada vez hay más entornos que proteger. "Cualquier empresa puede ser atacada y el ataque es crítico ya que afecta directamente al negocio y al servicio que se ofrece; por tanto, es infinitamente más problemático que otros asuntos".