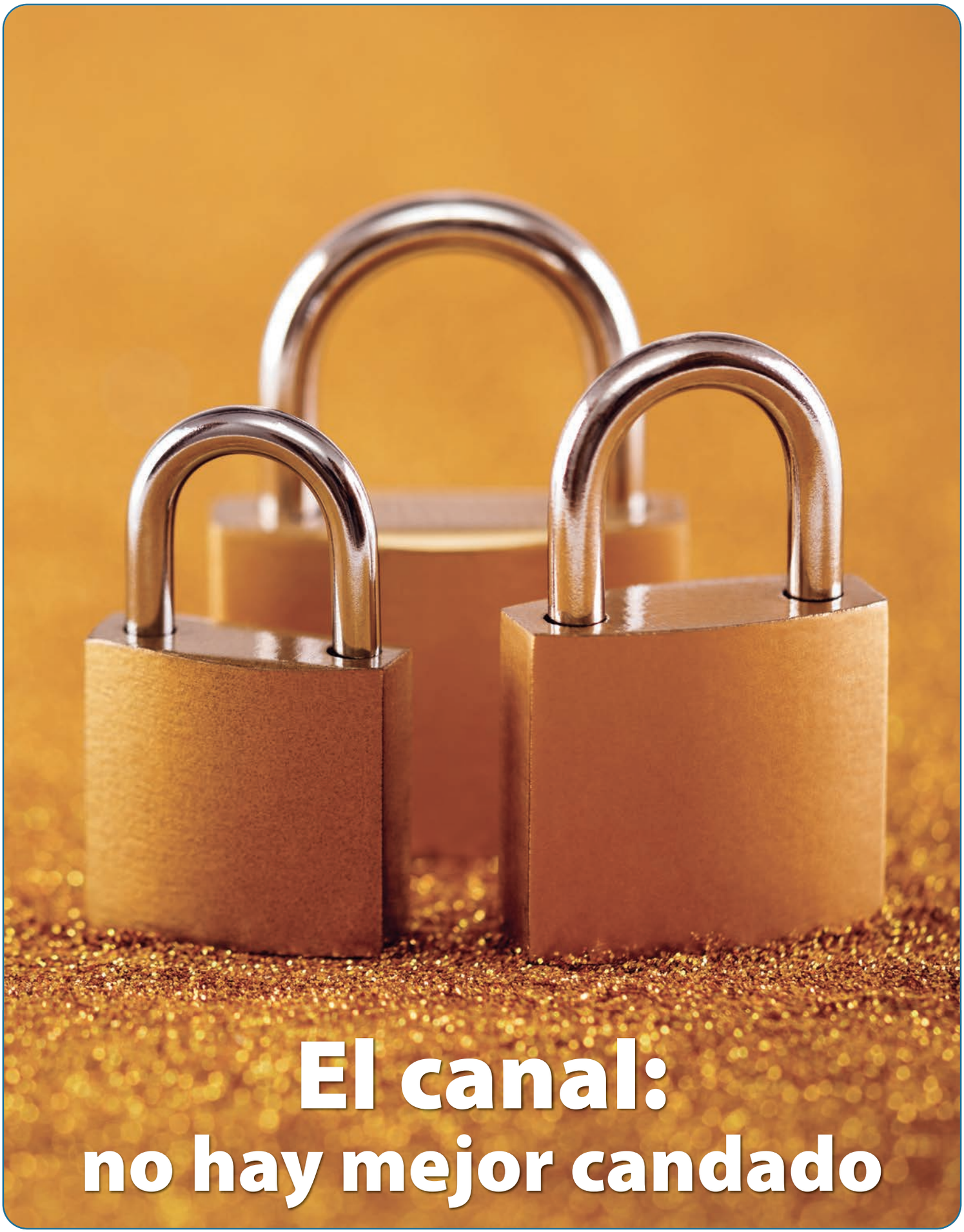

El canal: no hay mejor candado

Tendencias y oportunidades

del mercado de la ciberseguridad en España en 2023

El uso cada vez más creciente de los datos para la mejora de la experiencia de usuario y el avance hacia una organización conducida por datos *(data driven company)*, está condicionando la necesidad de abordar los retos asociados a la gestión de las herramientas y aplicativos de seguridad, así como facilitar el entorno de seguridad, de manera que se avance en la gestión de la privacidad y seguridad de los datos. En este contexto, los retos de desplegar, integrar, mantener y gestionar herramientas de seguridad dispares son una carga para los recursos finitos del equipo de seguridad, según afirman el 62 % de las organizaciones europeas.

El incremento exponencial de los datos de las organizaciones está favoreciendo que el número y sofisticación de las amenazas de seguridad crezca de igual forma, enfrentando a un escenario de seguridad fragmentado en las organizaciones y una situación de falta de habilidades de seguridad que se posicionan como los principales *drivers* de cambio en el mercado. Según datos de Proofpoint, el 68 % de las organizaciones europeas sufrió un ataque de *ransomware* que incluía robo de datos en 2022.

La irrupción de la inteligencia artificial en el campo de la seguridad está ayudando a mejorar las estrategias de defensa mediante la incorporación de esta en los sistemas de detección automática de las amenazas; no obstante, el uso de la tecnología "*deepfake*" requerirá incrementar la inversión en soluciones de gestión de la identidad para evitar ciberataques que aumenten el riesgo de fraude de identidad, engaño financiero y desinformación. En este sentido, si atendemos a aquellas asociadas con el uso ilegítimo de credenciales, veremos que el 48 % de las brechas de seguridad en 2021 (este tipo de amenazas está experimentando un crecimiento superior al 35 % en 2022, según datos de ForgeRock), está suponiendo unas pérdidas de más de 56.000 millones de euros, según datos de Protocol y Javelin, respectivamente.

El mercado de la seguridad en España muestra un crecimiento respecto del año pasado del 9,2 %, alcanzando los 2.130 millones de euros y para el año 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 %). Los segmentos de mayor crecimiento son los relativos a los servicios gestionados de seguridad, los servicios de integración y los servicios de red.

Por ello, se requiere cada vez más una mayor diversificación de las defensas. Las organizaciones buscan mejorar la seguridad de su infraestructura de red y recibir servicios avanzados de asesoramiento para proteger adecuadamente sus organizaciones.

En este sentido, la ciberresiliencia se configura como un objetivo prioritario a incorporar en las organizaciones. No se trata solo con el valor de la empresa y la reducción del riesgo empresarial, sino también con la seguridad económica nacional. Las organizaciones deben demostrar una ciberresiliencia satisfactoria frente a un entorno de riesgo digital más amplio.

Los datos de IDC apuntan a que para 2024 hasta el 60 % de las empresas europeas incrementarán en un 20% su presupuesto en ciberresiliencia para proteger sus inversiones digitales contra el ciberriesgo, lo que supondrá un gasto adicional de 5.900 millones de euros en seguridad en 2024. En 2023 las prioridades de inversión en materia de ciberseguridad pasarán por la racionalización de los *frameworks* de seguridad con el objetivo de disponer de una visión global de la misma en la organización. En concreto, la automatización y la racionalización de entornos de herramientas de seguridad es clave, así como que la automatización y orquestación de la seguridad está llevando a que el 39 % de las empresas españolas establezca como prioridad la incorporación de soluciones de automatización y orquestación de seguridad, así como la búsqueda de una racionalización o integración de entornos de herramientas de seguridad, como reconocen el 32 % de las empresas españolas.

José Antonio Cano
Director de análisis de IDC

YOU DESERVE THE BEST SECURITY

Only the best security can protect you from today's complex cyber threats. Large scale, multi-vector attacks now threaten the fabric of organizations around the globe.

Check Point fully protects you against these Gen V attacks. Our transformative product innovations protect better than all other options.

In a world where threats are ever growing, you deserve the best security. Check Point.

Quantum
Deep Learning & AI Driven Network Security

CloudGuard
Fully Automated Cloud Native Security from Code to Cloud

Harmony
Highest Level of Security for Remote Users

Horizon
Prevention-First Security Operations

www.checkpoint.com/es

CHECK POINT™

En el último lustro el crecimiento del negocio ibérico ha sido entre dos y tres veces mayor que el mundial

"Check Point Software asegura un 99 % de protección. Cuando detectamos una vulnerabilidad, la resolvemos en un día"

No resulta sencillo el panorama que se pinta en el mercado de la seguridad. Aunque crece la inversión, también lo hacen las amenazas. Sin embargo, no todos los fabricantes ofrecen el mismo nivel de protección. Mario García, director general de Check Point Software en España y Portugal, defiende su propuesta, que reposa en una plataforma que cumple con tres "ces": completa, consolidada y colaborativa; arropada por una estrategia en la que, cualquier vulnerabilidad que se detecta en ella, se resuelve, como máximo, en un día. "Para ofrecer seguridad es esencial que la plataforma sea lo más segura posible. Y, si algo nos distingue, es que contamos con los productos más seguros".

Marilés de Pedro

Una estrategia que tiene su reflejo en el crecimiento consolidado del negocio en los últimos años. En la región ibérica, incluso, con muy altos ratios, ya que en el último lustro el crecimiento acumulado ha sido entre dos y tres veces mayor que el experimentado a nivel mundial.

Estrategia diferencial

A semejanza de la mayoría de las empresas, la estrategia de Check Point Software reposa en una plataforma que ofrece una seguridad completa. Mario García explica que uno de sus rasgos diferenciales es la capacidad de integración que permite que las herramientas sean capaces de colaborar. Otro rasgo es su nivel de seguridad. "Tenemos que tener los productos más seguros del mercado ya que si sufrimos alguna vulnerabilidad los clientes se ven también afectados", recuerda. Por ello, explica que su ratio de vulnerabilidades es muy inferior al que tienen otros fabricantes. También su capacidad de detectarlas y, en un tiempo mínimo, subsanarlas. Exactamente, un día. "Hay fabricantes que han estado durante 180 días con vulnerabilidades sin subsanar, lo que supone un enorme riesgo para sus clientes", asegura. Otros manejan plazos de 50 o 60 días para solucionar estas brechas. La última diferencia es su capacidad, no solo de detectar y avisar de un ataque, sino también de pararlo. "Garantizamos un 99 % de protección", desvela. En el complejo entorno de la nube, en el que los grandes proveedores *cloud* también ofrecen sus propias herramientas de seguridad, algunos responsables de seguridad aseguran que la protección que ofrecen estos hiperescalares es mayor que la que dan los fabricantes especializados o, al menos, más que suficiente. Mario García asegura que no es así. "Nosotros, los proveedores de seguridad, contamos con herramientas con un nivel de protección muy alto y sumamos muchos años de experiencia", recuerda. "Somos capaces de aportar algo que falta muchísimo en el mercado: el conocimiento real de la seguridad". No cree que las herramientas de los hiperescalares sean malas, solo que "no están al mismo nivel que las nuestras". En muchas ocasiones las empresas diseñan un proyecto en la nube sin haber hecho un análisis real de cuál es su nivel de seguridad. "Los CISO necesitan herramientas que les permitan gozar de visibilidad, respaldadas con un equipo de seguridad especializado".

El canal de seguridad, el más preparado

Observado el complejo panorama del mercado de la seguridad Mario García cree que la formación y la especialización que se le exige al canal que se encarga de desplegarla es enorme. "La seguridad es un tema amplísimo y la barrera de entrada que se exige es muy alta". Check Point Software cuenta con un ecosistema de canal en el que conviven dos tipos de *partners*: unos, con un tamaño mayor, encargados de cubrir la parte más alta del mercado, conviven con compañías con un tamaño más reducido que se encargan de desplegar proyectos en empresas más pequeñas. La marca cuenta con equipos diferenciados para desarrollar ambos segmentos. Con las compañías encargadas de los mercados más altos, el objetivo es desplegar soluciones más completas en los clientes, con mayor capacidad de colaboración, para elevar el nivel de protección.

Informe anual

El pasado mes de marzo Check Point Software presentaba su tradicional informe de amenazas en el que, entre otras destacadas conclusiones, se desvelaba que en 2022 los ciberataques se incrementaron un 38 %, registrándose una media de 1.168 ataques semanales por organización. Se calculaba que en 2025 los daños superarán los 10.000 millones de dólares. "El cibercrimen es un negocio y cuanto más dinero consiguen los *hackers,* más actividad van a desarrollar y más van a atacar", explica, con aplastante lógica, Mario García. Los ataques, por tanto, seguirán incrementándose este año. "Hay mucho dinero en juego para el cibercrimen".

Por su parte, el crecimiento que ha experimentado la marca en el mercado mediano es espectacular. Un mercado para el que la marca acaba de presentar una solución integral, Infinity Spark. "Estamos creciendo muchísimo y muy rápido, tanto en el volumen de negocio como en el número de *partners* que se dedican a desarrollarlo", reconoce. Unos resultados que han situado a la región ibérica como una de las zonas que más crece en Europa. La vía ha sido la creación de soluciones más sencillas, más fáciles de implantar y de gestionar, pero completas. Un mercado que también exige máximo conocimiento a los distribuidores. "Sigue siendo un canal especializado".

Mario García,
director general de **Check Point Software** en España y Portugal

"Hay fabricantes que han estado durante 180 días con vulnerabilidades sin subsanar, lo que supone un enorme riesgo para sus clientes. En nuestro caso, el plazo máximo es un día"

Clave también para el canal es el despliegue del modelo de seguridad gestionada, que supone en torno al 30 % del negocio de Check Point Software. García asegura que cuentan con *partners* con capacidad de desplegar servicios de SOC, con profesionales formados. "Cada vez hacemos más negocio con este tipo de empresas, que implantan soluciones cada vez más completas, lo que nos hace avanzar más, y de manera más rápida". Sin embargo, reconoce que no todo su canal cuenta con estas capacidades pero insiste en que todos "más pronto o más tarde tendrán que desplegar estos modelos".

Check Point Software
checkpoint.com/es/

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

https://newsbook.es/reportajes/check-point-software-asegura-un-99-de-proteccion-cuando-detectamos-una-vulnerabilidad-la-resolvemos-en-un-dia-20230429101827.htm

El área de la seguridad gestionada crece a doble dígito en WatchGuard

"Nuestros MSSP tienen una gran oportunidad de ofrecer sus servicios fuera de España"

Un ecosistema en el que la directiva observa una enorme oportunidad más allá de las fronteras españolas. "Vamos a ayudar a la internacionalización de los MSSP españoles", desvela. "Tienen una gran oportunidad de ofrecer sus servicios fuera de nuestras fronteras. Desde WatchGuard tratamos de ayudarles en ese proceso, de simplificarlo, y de que traten de aprovechar su conocimiento", explica. A su juicio, España exhibe una posición muy competitiva para proveer de estos servicios a otras regiones. "Tenemos una enorme potencialidad por madurez, por competitividad y por talento". Un atractivo que también han observado algunos proveedores de servicios de seguridad foráneos que están tratando de acceder a España para implantar sus servicios.

Elena García-Mascaraque,
directora multinacional de proveedores de servicios de seguridad de **WatchGuard**

"Nuestro reto es hacer sencillo lo complicado"

Cuatro áreas de valor

La propuesta de valor de WatchGuard reposa en cuatro pilares. La tecnología es pilar básico. "Nuestro reto es hacer sencillo lo complicado", recuerda. Una tecnología que se reparte en cuatro áreas de soluciones: la seguridad en el *endpoint*, el área de autenticación multifactor (MFA), la protección de los entornos inalámbricos y la seguridad de red. "Es muy importante centrarnos en qué manera podemos mejorar los procesos

A doble dígito galopa el negocio de WatchGuard identificado con la seguridad gestionada. Elena García-Mascaraque, directora multinacional de proveedores de servicios de seguridad del fabricante, desvela que 2022 fue un año espectacular, creciendo, incluso, por encima de lo que señaló el mercado. Unos resultados que espera que continúen a lo largo de este ejercicio. "Es un mercado estratégico", insiste. "Nuestro éxito es el de los proveedores de seguridad gestionada. Y el suyo es el nuestro". Un éxito, explica, que reposa en el crecimiento conjunto. "Tenemos que seguir evolucionando nuestra tecnología, nuestras capacidades y nuestros modelos de suscripción para que nuestro ecosistema de proveedores de servicio gestionado siga teniendo un negocio exitoso en el mercado".

Marilés de Pedro

de los SOC y hacer que sean más eficientes trabajando con nuestras plataformas tecnológicas". La reducción de costes señala otro pilar de desarrollo. "Hay que trabajar también en una mejora en la eficiencia de los costes de los servicios gestionados para que el acceso de las empresas a ellos sea mucho más fácil". Por último, ofrecer a los SOC un modelo de negocio adaptativo y predecible; con una fórmula de suscripción absolutamente adaptada a lo que necesiten. "Se trata de que el proveedor de seguridad no tenga que adaptarse a nosotros, sino que WatchGuard se adapte a su modelo de negocio".

Pilar fundamental de este modelo es Unified Security Platform, la plataforma de seguridad unificada en la que se integran los diferentes componentes tecnológicos que dan respuesta a su visión. "Consideramos la seguridad como una plataforma de servicios", insiste.

En Unified Security Platform se integran los diferentes *stack* tecnológicos en los que se reparte la oferta: *endpoint*, MFA, *wifi* y red. Cuenta con elementos comunes de gestión alrededor de WatchGuard Cloud, que permiten una gestión integrada de estas áreas tecnológicas, con capacidades de XDR para detectar y responder a las diferentes amenazas.

Ecosistema

En el ecosistema de canal de WatchGuard conviven todo tipo de proveedores de servicios de seguridad, lo que incluye a los proveedores de servicios gestionados (MSP), los proveedores de servicios de seguridad gestionada (MSSP) y de detección y respuesta gestionada (MDR). A nivel mundial la marca cuenta con alrededor de 16.000 *partners*. García-Mascaraque diferencia entre aquellas compañías que cuentan con SOC internos, otras que disponen de capacidades para ofrecer servicios de externalización y otras, también capaces de ofrecer servicios, pero con un nivel más básico. Por último, observa que la dinámica de consolidación que se observa en otros segmentos "también ha alcanzado a este apartado de los proveedores de seguridad gestionada".

Cualquier mercado

Para García-Mascaraque el negocio de la seguridad gestionada alcanza cualquier segmento de mercado: la pyme, el área de las grandes empresas y todos y cada uno de los segmentos verticales en los que se reparte el mercado.

> "Consideramos la seguridad como una plataforma de servicios"

En el área de la pyme, al ser un entorno donde se hace más evidente la escasez de recursos y la complejidad del ecosistema de ciberseguridad, este modelo se torna muy necesario. "No debemos olvidar que el 48 % de los ataques está siendo dirigido a empresas con recursos limitados en ciberseguridad. Además, el incremento de ataques está siendo de un 68 % año tras año; lo que hace efectivamente que una de las áreas de más preocupación sea la pyme y la empresa que no disponga de esos recursos dentro de su organización. Y, por supuesto, externalizar ese tipo de conocimiento, ese manejo de la complejidad, es muy importante a la hora de plantear la seguridad como servicio".

Enorme oportunidad

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.

"Es una realidad", opina. Una fórmula que están adoptando tanto las grandes corporaciones como las pequeñas y medianas empresas "con diferentes niveles de consideración de cuál es su postura de seguridad y de los servicios que necesitan".

García-Mascaraque señala el concepto de Zero Trust como la clave para responder, no solo al panorama de múltiples amenazas, sino también para cumplir con la regulación. "Zero Trust abarca la protección del puesto de trabajo y la identidad, gestionando quién accede al dato. Y las capas de servicio que nos permiten monitorizar, detectar y responder a las diferentes amenazas. Todo ello está incluido en nuestra plataforma Unified Security Platform".

WatchGuard
watchguard.es

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

https://newsbook.es/canal/nuestros-mssp-tienen-una-gran-oportunidad-de-ofrecer-sus-servicios-fuera-de-espana-20230428101794.htm

Para este 2023 la compañía busca crecer en las áreas en las que su mensaje es diferenciador y consolidarse en la parte de *backup*

"Con un solo sabor, el de Hornetsecurity, los *partners* cubren la prevención, detección y recuperación"

Félix de la Fuente,
country manager de **Hornetsecurity** en España, Italia y América Latina

La nube y la seguridad como servicio gestionado son dos de las tendencias que mayor protagonismo están acaparando en los últimos tiempos y que están marcando el presente y futuro del mercado de la ciberseguridad. No en balde ambas tendencias están ganando terreno y cada vez son más las empresas que migran sus procesos y servicios al *cloud* o que deciden dejar su seguridad en manos de expertos externalizando estos servicios. Unas tendencias cuya adopción depende, según Félix de la Fuente, *country manager* de Hornetsecurity en España, Italia y América Latina, del tamaño de las empresas y sus necesidades.

Olga Romero

De la Fuente, que recuerda que "la nube como concepto no es más que el hardware deslocalizado que las empresas tenían en sus *data centers* o CPD", explica que para los pequeños negocios la migración a la nube responde a la necesidad de buscar, por un lado, el servicio y, por otro lado, la facilidad de llegar a un entorno de aplicaciones al que no podrían acceder por sus propios medios, ya que carecen de los recursos necesarios. Mientras que en el caso de las grandes empresas lo que buscan es el servicio y desvincularse del hardware.

En cuanto a las brechas de seguridad a las que las organizaciones deben hacer frente en el *cloud*, el responsable del negocio de Hornetsecurity en España, Italia y América Latina señala el factor humano como el elemento más sensible de la cadena. "La concienciación es fundamental y las empresas están prestando especial atención a este aspecto, de hecho, están empezando a invertir bastante", afirma.

> "Hemos particularizado los mensajes en función de las capacidades y el público al que se dirigen los diferentes *partners*"

Además, de la Fuente cree que es imprescindible "rodear de tecnología a los trabajadores" y filtrar los accesos para conseguir que comentan los menores errores posibles. Un filtrado que, junto con la formación, se enmarca en la prevención, el primero de los tres pilares en los que Hornetsecurity tiene puesto el foco. Las otras dos patas de la propuesta de la compañía son la detección y la recuperación de los datos.

Sobre la seguridad como servicio gestionado,

"El 94 % de los clientes, independientemente del tamaño, que prueban nuestros servicios se quedan con ellos"

modelo que, según previsiones de Gartner, en 2025 ya habrá implementado el 50 % de las empresas, el directivo cree que "el mercado español está evolucionado" y señala la búsqueda de un servicio fácil que les proteja y les garantice, en caso de ser atacados, la recuperación de los datos la razón por la que las pymes se decantan por este modelo. Mientras que las grandes corporaciones buscan el servicio para dar continuidad al plan diseñado por el director de ciberseguridad y desvincularse así del hardware.

Partners, figura clave

Para Hornetsecurity su red de *partners* tiene un papel fundamental. "Son nuestras manos, lo que llega al cliente y quien firma el contrato con el cliente final", asegura de la Fuente. Por ello la estrategia de canal de la compañía está centrada en "hacerles competitivos" y con esta finalidad el acompañamiento, la formación, "para que cuenten con personal preparado dentro de su organización", y proporcionar una plataforma *cloud* sencilla son los pilares en los que se apoya el plan de canal de Hornetsecurity.

Además, el fabricante, en su incansable búsqueda por ofrecer la mejor solución a sus socios, ha particularizado los mensajes en función de las capacidades y el público al que se dirigen sus diferentes *partners*. "Nos adaptamos a sus necesidades para que sean competitivos, confíen en la solución que les presentan a sus clientes y, en definitiva, sigan haciendo negocio con nosotros", apunta.

Más que una plataforma *cloud*

Hornetsecurity ofrece una solución sencilla, estructurada, intuitiva y estable. Todo esto se aglutina en su plataforma *cloud* que, además de las ventajas que aporta al ser una herramienta en la nube, incluye tecnología de inteligencia artificial, la cual se emplea para conocer el nivel de concienciación de los empleados. "Parece complicado, pero es tan sencillo como hacer *clic* y dejarlo funcionar para que nuestra IA personalice a cada empleado", explica de la Fuente. De esta manera, la formación que reciban los trabajadores en materia de concienciación será totalmente personalizada según sus capacidades.

Otra de las ventajas de la plataforma en la nube de Hornetsecurity se encuentra en la parte de *backup*, el cual incluye almacenamiento. "Nosotros disponemos de nuestros propios centros de datos, uno de ellos está en España, y esto nos garantiza independencia, es decir, no dependemos del comportamiento que puedan tener en precios los *hyperscalers*. Lo que se traduce en una política sostenible, estable y previsible", explica.

Asimismo, la sencillez de la plataforma está permitiendo a Hornetsecurity llegar de una manera más sencilla al mercado de la pyme porque, como destaca el directivo, al ser un servicio de "*clic* y me olvido" a la pyme le sorprende su facilidad de uso. "Las pymes son, precisamente, las que más disfrutan de estos servicios porque no tienen recursos dedicados y lo que quieren es proteger y, en caso de problemas, recuperar la información para seguir trabajando", afirma.

Por último, cabe destacar la autonomía que la plataforma ofrece a los *partners*. Una autonomía que se traduce en que los socios puedan hacer todas las pruebas de concepto que requieran sin necesidad de avisar a Hornetsecurity. Para ello los *partners*, desde el momento en el que inician su actividad con el fabricante, disponen de un entorno de pruebas porque, como indica de la Fuente, "lo que no pruebas no puedes explicarlo". Una apuesta que parece triunfar entre los *partners* ya que "más del 94 % de los clientes que prueban nuestros servicios se quedan con ellos", asegura el directivo.

Con esta sólida propuesta, basada en la prevención, detección y recuperación y apoyada en su plataforma *cloud*, Hornetsecurity espera, en este 20233, "seguir creciendo en las áreas en las que tenemos un mensaje muy particular y diferenciador". El fabricante también espera consolidar su presencia en otros ámbitos como en el de *backup*.

Hornetsecurity
hornetsecurity.es

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

https://newsbook.es/videos/con-un-solo-sabor-el-de-hornetsecurity-los-partners-cubren-la-prevencion-deteccion-y-recuperacion-20230428101807.htm

El reto de la seguridad total: reforzar el cortafuegos humano

Es fundamental contar con las soluciones más avanzadas en materia de seguridad, desde la prevención hasta la respuesta y recuperación, pasando por la protección. Se puede conseguir que la actividad comercial siga adelante sin interrupciones, que los ataques se encuentren con una rápida defensa y, en caso necesario, que todos los sistemas, archivos y datos puedan ser recuperados con celeridad.

Sin embargo, si bien es crucial garantizar que se apliquen las normas de ciberseguridad, los atacantes suelen apuntar a la presa más fácil. Con demasiada frecuencia, organizaciones con enormes presupuestos de seguridad son vulneradas por algo tan simple como un *email* de *phishing*. Un ataque realizado con éxito puede suponer graves daños económicos para las empresas afectadas y una pérdida de confianza entre sus clientes y proveedores. Como ejemplo, en correos electrónicos que se hacen pasar por auténticos, los estafadores simulan ser directivos de la propia empresa, compañeros de trabajo o *partners* para persuadir a los empleados de que revelen datos muy sensibles o para que abran enlaces o archivos adjuntos maliciosos que pueden servir como puerta de entrada a toda la red de la empresa. Y todo esto, además, acrecentado por los riesgos que aportan el aumento del teletrabajo o el uso de dispositivos privados para fines empresariales.

Incluso bajo la creencia de que la organización tiene cubiertos los aspectos básicos, es importante revisarlos constantemente y adoptar una cultura de "seguridad sostenible". La mayor parte de los ciberataques siguen centrándose en el "punto débil humano", al fin y al cabo, hasta los sistemas y herramientas más seguros desde el punto de vista técnico son sólo tan seguros como la prudencia

con la que los manejan los usuarios.

Cualquier estrategia de ciberseguridad debe cubrir los 360º e integrar el factor humano en su propia solución de seguridad, incorporándolo activamente en el ciclo de seguridad informática. La capacitación en seguridad continua prepara sistemáticamente a los empleados ante los riesgos cibernéticos, que son cada vez más frecuentes. Con el transcurso del tiempo aprenden a reconocer y repeler de manera efectiva incluso los ataques más sofisticados, dominando las medidas necesarias para impedir graves incidentes de seguridad y para que en todo momento esté asegurada la continuidad del negocio.

Por esta razón, cada vez más organizaciones están recurriendo a la concienciación en seguridad del usuario final de manera que les permita capacitarles para detectar potenciales ciberataques. No se puede subestimar la importancia de formar a los usuarios para que sean conscientes de estos ataques y conseguir así una cultura de seguridad sostenible que prevenga en la mayor medida posible la exposición a los riesgos cibernéticos.

Para llevarlo a cabo, Hornetsecurity ha desarrollado una solución integral basada en inteligencia artificial que combina formatos de aprendizaje innovadores y gamificación, con una de las simulaciones de *phishing* más avanzadas. A través del uso de una combinación de *elearning* interactivo, vídeos cortos y cuestionarios, los participantes reciben información importante sobre los crecientes riesgos cibernéticos, reforzando su concienciación sobre las amenazas en ciberseguridad.

Security Awareness Service de Hornetsecurity funciona de forma totalmente automatizada y mide continuamente el comportamiento de seguridad de los empleados, lo que significa que la formación y las simulaciones de *phishing* se adaptan a las necesidades individuales de cada usuario, sin que los administradores o responsables de seguridad informática tengan que intervenir.

El resultado es una cultura proactiva de la seguridad y unos empleados formados que reconocen los ciberataques y los rechazan con eficacia y, de esta manera, conocen y tienen en cuenta su responsabilidad con la empresa.

Félix de la Fuente
Country manager de **Hornetsecurity**
en España, Italia y América Latina

La seguridad como garantía de éxito del trabajo híbrido

El teletrabajo es ya una realidad. No obstante, en muchas compañías se ha optado por tomar lo mejor de ambos mundos, es decir un modelo mixto que combina el trabajo en la oficina y en remoto. La unión de ambos escenarios permite al empleado realizar su labor de la mejor forma posible, ofreciéndole flexibilidad y favoreciendo a su conciliación laboral; pero ¿se lleva a cabo el trabajo híbrido de una manera óptima y segura? A esta pregunta, responde el estudio que hemos elaborado recientemente en Canon, "Instantánea híbrida: impacto en los empleados y en la experiencia de TI", que revela que un 81 % de las empresas españolas se enfrenta a dificultades para garantizar la seguridad en esta modalidad de trabajo híbrido.

En este escenario híbrido es aún más importante mantener una estrategia de ciberseguridad que blinde a la empresa de cualquier posible riesgo, con independencia de dónde trabaje su equipo. El acceso a los sistemas y datos de la empresa desde ubicaciones remotas puede aumentar el riesgo de ciberataques e infracciones de la seguridad de la información. Se trata de un aspecto que preocupa a las organizaciones españolas y europeas, concretamente a un 85 % les inquieta que los empleados no sigan los procedimientos de seguridad cuando están fuera de las instalaciones físicas. La falta de seguridad en el trabajo híbrido puede exponer a la organización a riesgos significativos, como la pérdida de datos, el robo de información confidencial o incluso la interrupción de las operaciones comerciales, con las pérdidas económicas que esto supone.

Además, para abordar este desafío, se deben implementar medidas de seguridad que garanticen que el empleado pueda desempeñar exactamente las mismas funciones, ya sea trabajando desde cualquier lugar o en la oficina, y sobre todo hacerlo con la misma garantía de seguridad. Por

ejemplo, en una tarea habitual como puede ser la de imprimir documentos confidenciales o trabajar con ellos fuera de la oficina, no debe suponer, a priori, ningún problema. No obstante, lo cierto es que, según revela el citado informe, el 75 % de los profesionales de TI en Europa tiene dificultades para establecer los ajustes necesarios de seguridad en las impresoras y escáneres para su actividad en remoto. A esto se le une que solamente el 26 % de las empresas de España es capaz de tener un seguimiento completo del ciclo de vida de un documento, desde que se accede a él hasta que se comparte, imprime, archiva y elimina, contribuyendo a aumentar la vulnerabilidad de los datos frente a posibles ataques.

Ante estos desafíos, la buena noticia es que existe tecnología y soluciones para garantizar la seguridad en la gestión de documento, incluido su impresión y escaneo en remoto. Las compañías deben acometer las inversiones oportunas para abordar la digitalización de sus procesos de trabajo y para ello, la mejor solución es confiar en un socio experto que les ayude a abordarlo. El problema al que se enfrentan en muchas ocasiones las organizaciones es a la falta de conocimiento o al erróneo pensamiento de que un cambio de este tipo puede suponer grandes inversiones o periodos de adaptación muy largos. Por ello, recomendamos contar con un socio de confianza que le acompañe en todos los pasos.

En definitiva, la protección de los documentos y, en especial, la de la información sensible que se maneja fuera de las instalaciones, debe ser prioritaria para cualquier compañía. Solo asegurando cada elemento, se podrá garantizar un trabajo híbrido sin fisuras. Y es que, si no se garantiza esta modalidad de trabajo, las compañías tienen el riesgo de no ser competitivas, porque el trabajo híbrido ha llegado para quedarse.

Eva Sánchez,
head of Solutions de **Canon** España