it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Abril 2022 - nº 51

SSE vs SASE,
¿qué hay de nuevo?

‘En general, no se aprovecha todo el potencial que ofrece la tecnología que has implantado’ Gustavo Lozano, ING

‘La colaboración con terceros es fundamental en el mundo de la ciberseguridad’ Juan Luis Garijo, Crowdstrike

La Seguridad en la nueva era de SD-WAN

#DesayunosITDS. Protección de aplicaciones web y APIs

Guarda esta revista en tu equipo y ábrela con Adobe Acrobat Reader para aprovechar al máximo sus opciones de interactividad

Directora Rosalía Arroyo
rosalia.arroyo@itdmgroup.es

Colaboradores Hilda Gómez, Arantxa Herranz, Reyes Alonso, Ricardo Gómez

Diseño revistas digitales Contracorriente

Producción audiovisual Miss Wallace, Alberto Varet

Fotografía Ania Lewandowska

Director General
Juan Ramón Melara juanramon.melara@itdmgroup.es

Director de Contenidos
Miguel Ángel Gómez miguelangel.gomez@itdmgroup.es

Directora IT Televisión y Lead Gen
Arancha Asenjo arancha.asenjo@itdmgroup.es

Directora División Web
Bárbara Madariaga barbara.madariaga@itdmgroup.es

Director de Operaciones
Ángel Porras angel.porras@itdmgroup.es

Clara del Rey, 36 1º A · 28002 Madrid · Tel. 91 601 52 92

Secure Service Edge, el nuevo cuadrante

Dos años después de definir SASE, un modelo para diseñar la arquitectura de seguridad y redes en un mundo en el que el uso de aplicaciones en la nube es omnipresente en las empresas, los analistas de Gartner estrenaron el término SSE (Secure Service Edge), que hace referencia a un conjunto de capacidades necesarias para lograr la seguridad que SASE describe, centrándose en los requisitos medulares de la plataforma, incluyendo el agente de seguridad de acceso a la nube (CASB), el gateway de seguridad web (SWG) y el acceso a la red basado en confianza cero (ZTNA). De ello hablamos en este número de IT Digital Security.

Además, en #ITDSAbril entrevistamos a Gustavo Lozano, CISO de ING, para quien no se aprovecha todo el potencial de la tecnología que las empresas implantan; y a Juan Luis Garijo, Director de Crowdstrike, quien destaca las capacidades de visibilidad, ciberinteligencia y Threat Hunting de la plataforma Falcon de la compañía.

Os resumimos el evento Netskope Barcelona Summit 2022 celebrado hace unas semanas, así como un nuevo #DesayunoITDS centrado en la seguridad de las aplicaciones y las APIs en el que han participado Daniel Howe, Senior Sales Engineer de Fastly; Nuno Silveiro, Principal Sales Specialist de Citrix Iberia; Francisco Lahoz, Ingeniero Preventa de F5 Networks; José Juan Díaz, Iberia Senior SE de Barracuda; y Eusebio Nieva, Director Técnico de Check Point.

También podéis leer las principales conclusiones de un debate en torno a SD-WAN que reunió a Fernando Cócaro, Senior Security Architect de Clariant Ibérica; Carlos Asún, CISO de Food Delivery Brands; Ángel Uruñuela, CISO de Fluidra; Elena García Díez, CISO de Indra; e Iker del Fresno, Country Manager de Aruba, a Hewlett Packard Enterprise Company.

La actualidad llega también de la mano de CATO Networks, un jugador del mercado SASE que está en proceso de abrir oficina en España; y de Vicarius, una empresa israelí representada por Ingecom que ofrece una plataforma autónoma para la gestión y remediación de vulnerabilidades.

¿Te interesa la seguridad? Entonces seguro que te gusta este número de IT Digital Security.

itds

Sumario

Actualidad

Encuentros ITDS

Monográfico

Webinars

Entrevistas

Desayunos ITDS

No solo IT

Índice de anunciantes

ARMIS®

Fortalece la seguridad de tus pacientes obteniendo visibilidad completa de todos tus dispositivos

Armis ofrece visibilidad completa e información precisa sobre todos los dispositivos administrados y no autorizados de tu red.

Descubre nuestra solución en
www.armis.com/medical-device-security/

Netskope Barcelona Summit 2022

“Es el momento de Netskope”

Durante el mes de marzo celebró Netskope un evento en Barcelona que reunió a más de 80 personas entre partner y clientes y donde se quiso dejar claro que este es el momento de Netskope, y lo es por derecho, y porque el nuevo cuadrante SSE de Gartner valida la trayectoria de una compañía que nació como CASB y ha evolucionado para desplegar una oferta completa de seguridad cloud basada en NewEdge, la infraestructura cloud de la compañía, que tiene como objetivo mantener una conectividad rápida y fiable con todas las regiones del mundo sin comprometer la seguridad.

Durante el mes de marzo celebró Netskope un evento en Barcelona que reunió a más de 80 personas entre partner y clientes y donde se quiso dejar claro que este es el momento de Netskope, y lo es por derecho, y porque el nuevo cuadrante SSE de Gartner valida la trayectoria de una compañía que nació como CASB y ha evolucionado para desplegar una oferta completa de seguridad cloud basada en NewEdge, la infraestructura cloud de la compañía, que tiene como objetivo mantener una conectividad rápida y fiable con todas las regiones del mundo sin comprometer la seguridad.

"Si importante es tener un cloud propio, igual de importante es entender las aplicaciones cloud"

David Macià,
Regional Sales Manager, Netskope

Miguel Ángel Martos, country manager de Netskope para la región de iberia, inauguraba el encuentro para decir que el momento de Netskope es ahora. La compañía, que sin estar cotizando en bolsa ya tiene una capitalización de mercado de 7.500 millones de dólares, trabaja con más de cien clientes en España, incluidas el 30% de las empresas del IBEX.

La transformación digital en la que se ven envueltas las empresas implica llevar datos a la nube, "y esto supone la transformación de la red, lo que conlleva la transformación de la seguridad", decía Martos, quien aseguraba además que el crecimiento de Netskope se basa en tres pilares: la tecnología, el capital humano y el ecosistema de partnes.

"Clientes y partners están respondiendo a la necesidad de cambiar la seguridad", decía durante su intervención David Macià, Regional Sales Manager - Eastern Iberia, de la compañía. Explicaba

“La estrategia de la compañía es continuar invirtiendo en NewEdge”

(David Macià, Regional Netskope)

Año y medio llevan David Maciá, Regional Sales Manager, e Ignacio Franzoni, senior Sales Engineer, trabajando la región este de España, con un crecimiento “muy grande” que les ha llevado a multiplicar por tres los ingresos y sumar 23 nuevos clientes a la compañía.

El reto, asegura, es de evangelización y explicar cómo se securiza la nube. La compañía, que empezó en el mundo CASB, aprovechó la oleada del SASE y triunfa en el nuevo cuadrante SSE, está en su mejor momento. Sobre SSE, dice David Macià que no cambia tanto las cosas, que se trata de la traslación de la arquitectura SASE anunciada hace unos años por Gartner, que hablaba de red como servicio y seguridad como servicio; “SSE (Secure Service Edge) coge la parte de seguridad y lo traslada a producto, donde ya no es pensar en un proxy, un CASB o un DLP en la nube sino en una plataforma de servicios de seguridad en la nube donde hay una serie de fabricantes, y Gartner nos ha reconocido como líderes” explica Macià añadiendo que este reconocimiento es una validación de una estrategia que, como comentábamos, se inició en el CASB.

Si importante es tener un cloud propio, igual de importante es entender las aplicaciones cloud, nos cuenta David Macià. Teniendo en cuenta que el 70% del tráfico de Internet son aplicaciones cloud, saber qué pasa dentro de estas aplicaciones, poder profundizar en el dato, es clave y es uno de los elementos diferenciadores de la oferta de Netskope; es el valor de haber nacido CASB.

Mirando hacia un futuro que pasa, de manera más o menos inminente, por una salida a Bolsa, la estrategia de la compañía es “continuar invirtiendo en NewEdge, nuestra propia infraestructura cloud, porque es clave poder decir que la latencia que se puedan encontrar los usuarios al pasar por nuestros servicios de seguridad es la mejor, la más óptima”. Y esta estrategia de continuar ampliando la infraestructura sirve “para soportar esta demanda creciente de usuarios”.

Además, se continuará invirtiendo en Data Protection, “e innovando en, sin necesidad de pre-clasificar la información poder hacer machine learning para proteger la información, independientemente de dónde esté el usuario o el dato”.

Juan Manuel Pascual Escribá, CEO de Open3S

David Martin Lindström, Head of Network & Data Security Products en Telefónica Tech

Eloi Sarsanedas, CEO de Madcoms

Antonio Cañada, Responsable de Preventa Zona Este en Exclusive Networks

el directivo que “SASE es el framework y SSE el conjunto de productos consumidos como servicio de seguridad”; que gracias a NewEdge “somos extremadamente rápidos”; y que, entendiendo que no están solos en el mundo, la compañía ha desplegado una estrategia de alianzas que le permite, gracias a su integración con SOAR, EDRs o SIEMs, “poder proteger el dato allí donde esté”.

Yaroslav Rosomakho, Field CTO de Netskope, dedicó su ponencia a hablar de cómo proteger a personas y datos, “los activos más importantes de las empresas”. Sobre las personas comentó que las empresas deben garantizar una buena experiencia de usuario, y que sean más ágiles y productivos y, al mismo tiempo, garantizar que no comentan errores que pongan en riesgo a los negocios. “Los datos son un elemento estratégico que tiene que ver con los procesos”, decía, señalado que la estructura de los datos está

"Es clave encontrar el equilibrio entre la agilidad, los costes y el riesgo"

Ilona Simpson, CIO EMEA, Netskope

cambiando, que los datos se almacenan en cualquier parte y que no deben olvidarse presiones con el compliance.

Antes de asegurar que "Zero Trust es ineficiente", Rosomakho mencionó algunos de los pilares de la propuestas Netskope Intelligent SSE (FWaaS, CASB, SWG, ZTNA, CPSM…) y explicó que la confianza "debe ser adaptativa en función de una serie de elementos", que van desde las aplicaciones que se utilizan, qué es lo que está haciendo el usuario, el riesgo del dispositivo, etc.

Durante su presentación Ilona Simpson, CIO para la región de EMEA de Netskope, mencionó la ciberseguridad y las interrupciones de la cadena de suministro como los dos factores que, según un estudio de Deloitte, llevarían a los CEOs a cambiar su estrategia en los próximos cuatro meses. La cadena de suministro es un ecosistema muy vivo que tiene diferentes elementos sobre los que actuar. Según el mismo estudio, los CEOs encuestados identificaron una serie de acciones que tendrían mayor impacto dentro de esa cadena de suministro, como es la adopción de nuevos modelos comerciales, nuevos socios, nuevas iniciativas, el cambio de la oferta de productos o una adquisición o integración en un vertical.

Como es lógico, los CIOs se enfrentan a una realidad diferente en la que el aumento del teletrabajo, las regulaciones, el incremento de los datos, dispositivos y aplicaciones se unen al famoso Shadow IT o la aparición de nuevas tecnologías. "¿Cómo gestionamos este caos?", se preguntaba Ilona Simpson parea después añadir que la experiencia del usuario y la resiliencia son la base del negocio y que deben incluirse en la 'Business Agility Agenda' de los CIOs para avanzar de la modernización a la transformación y habilitar el negocio.

Terminaba su intervención la directiva mencionando cómo es clave encontrar el equilibrio entre la agilidad, los costes y el riesgo.

Premios al canal

Al finalizar el evento, en el que también se pudo disfrutar de una demo, se realizó la entrega de los 2021 Iberia Partners Awards.

Antonio Cañada, Responsable de Preventa Zona Este en Exclusive Networks, destacaba durante la recogida de uno de los galardones que "Netskope despierta una gran motivación entre usuario final y

"Datos y empleados son los activos más importantes de las empresas"

Yaroslav Rosomakho, Field CTO, Netskope

equipo técnico" y que trabajar con la compañía no sólo escala el negocio, sino "el valor que el partner puede dar a los clientes".

Juan Manuel Pascual Escribá, CEO de Open3S, quien trabaja con Netskope desde 2016, destacó que la del fabricante "nos sigue pareciendo una solución innovadora".

Eloi Sarsanedas, CEO de Madcoms, resaltó la confianza de los clientes en la solución de Netskope, en su catálogo desde "mucho antes de que hubiera alguien de Netskope en España".

En el momento de recoger el premio, David Martin Lindström, Head of Network & Data Security Products en Telefónica Tech, comentó que es un privilegio poder trabajar con Netskope y llevar sus soluciones al mercado; "están funcionando muy bien y esperamos que siga así en el futuro". it

Enlaces de interés...

- Netskope continúa la expansión de su nube privada de seguridad NewEdge
- Netskope: "Vamos a acelerar la inversión en Iberia"
- La presión del CISO en el desempeño de su trabajo, un factor a tener en cuenta para su salud mental

Compartir en RRSS

"La transformación digital implica llevar datos a la nube, y esto supone la transformación de la red y de la seguridad"

Miguel Ángel Martos,
Country Manager, Netskope

IBERLAYER

Cloud Email Security

9 de cada 10 incidentes de
ciberseguridad empiezan por email

¿Cuánto le preocupa la seguridad del suyo?

WWW.IBERLAYER.COM

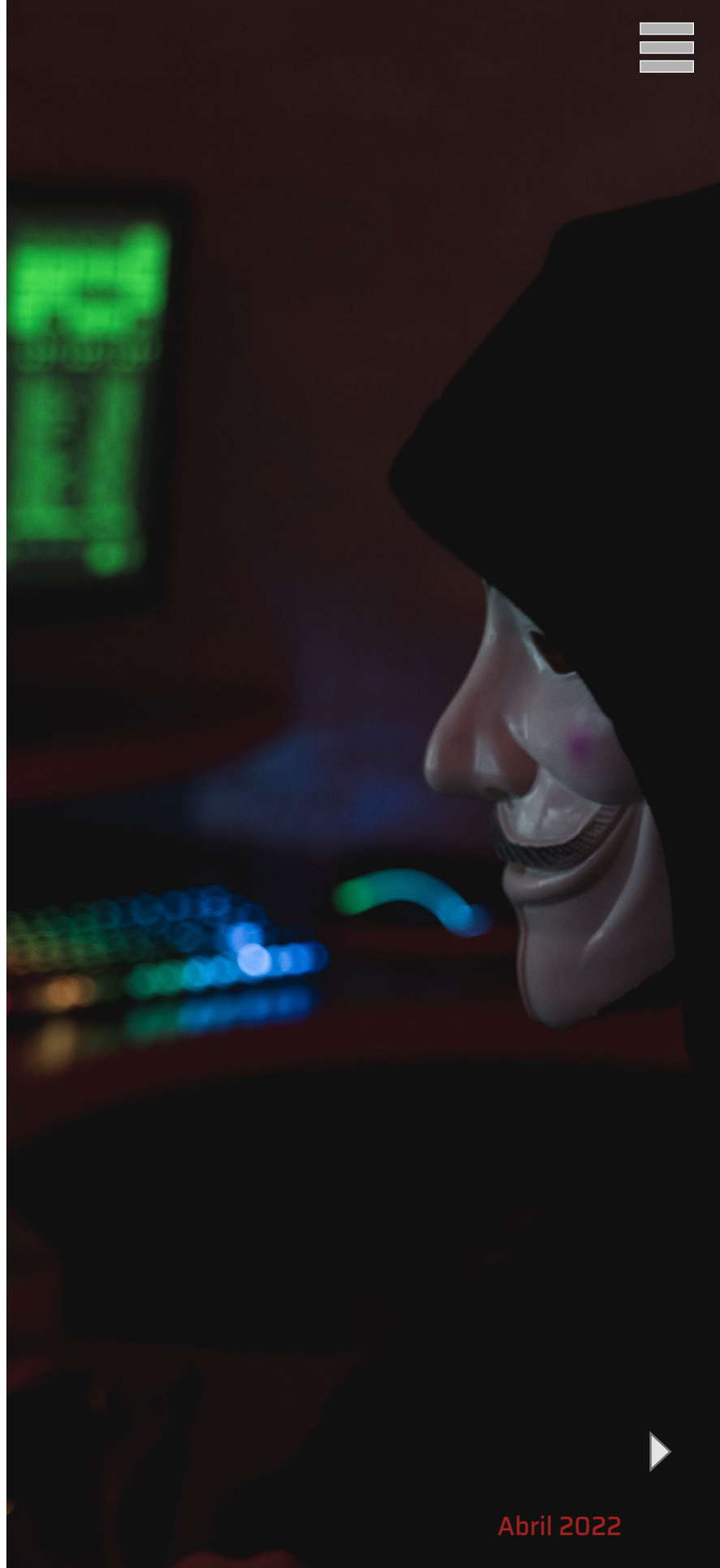
Protección total contra Spam, Phishing, Ransomware, Malware,
APTs, Scam, Fraudes de CEO, Fraudes Bancarios ...

Vicarius trae a España su plataforma TOPIA para la gestión y remediación de vulnerabilidades

Fundada por tres expertos en seguridad, Michael Assraf, Yossi Ze'evi y Roi Cohen, Vicarius equipa a los equipos de TI y seguridad con una plataforma totalmente automatizada y consolidada, TOPIA, para evaluar, priorizar y remediar vulnerabilidades en aplicaciones, activos y sistemas operativos. Las herramientas tradicionales basadas en redes y escaneo se enfocan exclusivamente en el descubrimiento de vulnerabilidades o la administración de parches y no pueden adaptarse a la cambiante infraestructura híbrida. Vicarius proporciona una solución integrada que da prioridad a la nube y que cierra el ciclo desde el descubrimiento hasta la remediación para el cambio actual hacia el trabajo remoto y las aplicaciones basadas en la nube.

Hablamos con Michael Assraf, CEO y cofundador de Vicarius, que llega a España de la mano de Ingecom y que según Crunchabase ha recaudado 29,2 millones de dólares en cinco rondas de financiación, la última -una SerieA, en febrero de este año por valor de 24 millones.

Vicarius comienza identificando las debilidades dentro del entorno digital de los clientes utilizando una metodología de análisis de código binario patentada. Luego prioriza estas vulnerabilidades, creando un mapa de amenazas en tiempo real de la infraestructura de la organización utilizando el análisis de contexto de activos. Por último, se implementa una capa de corrección para proteger el software de las vulnerabilidades identificadas al limitar el acceso a su código explotable en tiempo real.



"Al consolidar el proceso de remediación de vulnerabilidades en una sola plataforma y eliminar la complejidad asociada con los productos aislados y los canales de comunicación cerrados, estamos reuniendo a los equipos de seguridad y TI bajo un mismo techo para tomar medidas y reducir el riesgo"

Michael Assraf, CEO y cofundador, Vicarius

Michael Assraf, CEO y cofundador de Vicarius

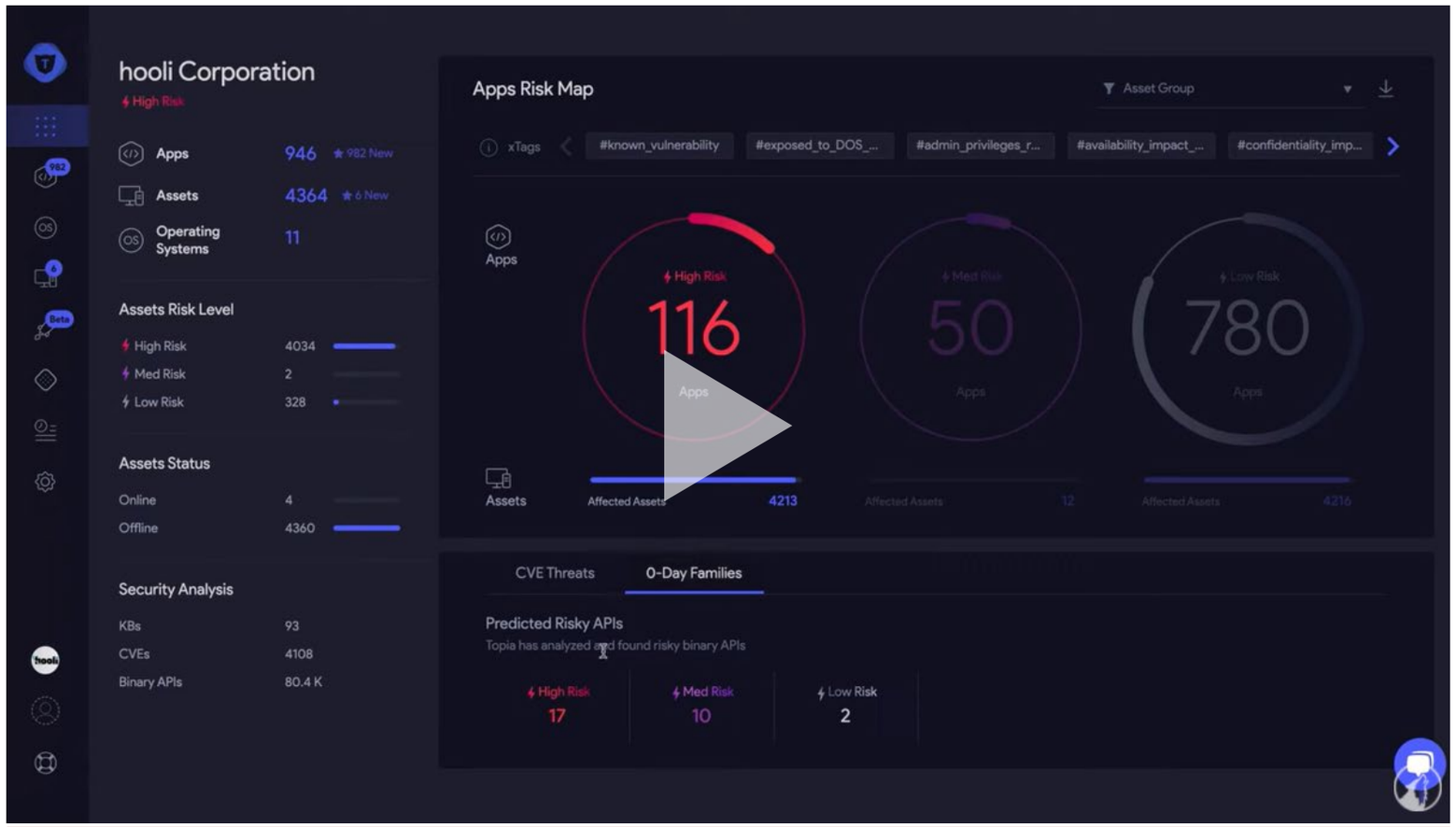
"La tecnología permite a las empresas proteger el software que tienen, incluso si sus proveedores aún no han emitido una corrección o una solución de seguridad", asegura Michael Assraf. Define el directivo la oferta de la compañía, que se ofrece bajo un modelo SaaS, como una plataforma autónoma de remediación de vulnerabilidades, "lo que significa que realiza todas las actividades para la remediación de vulnerabilidades de infraestructura, dispositivos, servidores… lo que sea". La plataforma permite también predecir vulnerabilidades a partir del análisis de código binario y priorizarlas en función del análisis contextual, de forma que "podemos decirles a los clientes cuáles de sus aplicaciones vulnerables se usan más, cuáles se ejecutan con cuentas privilegiadas sólidas, cuáles se comunican con Internet externo, etcétera. Y luego podemos adaptar la probabilidad de explotación".

Topia propone formas de arreglar esos fallos y si se da el caso de que un cliente no puede implementar una actualización "porque temen el tiempo de inactividad y cosas por el estilo, también podemos permitirles usar nuestra protección de parches, que es otra herramienta que los equipos de seguridad pueden usar cuando realmente no pueden implementar el parche de seguridad". ¿Se trata de un herramienta de Virtual Patching? "No exactamente". Cuando el parche de un proveedor no está disponible, TOPIA aplica de forma autónoma Patchless Protection, una tecnología de protección en memoria que permite a las empresas proteger las aplicaciones sin actualizaciones de software. Mediante el mapeo exclusivo del ADN del software y el aprendizaje de su estructura, TOPIA detecta archivos de software anormales para evitar ataques a la cadena de suministro.

Ventajas de Vicarius

Preguntamos a Michael Assraf por la diferenciación de la propuesta de Vicarius. Comenta que una de las ventajas de la plataforma Topia es que consolida las diferentes partes y capacidades de remediación de vulnerabilidades, sin tener que saltar de una herramienta a otra;

Explica que el proceso de corrección de vulnerabilidades se divide entre dos departamentos. Por un lado, el de seguridad, que identifica y prioriza las vulnerabilidades, y por otro el de IT, que las repara.



TOPIA **CLICAR PARA VER EL VÍDEO**

Los equipos de seguridad están comprometidos a reducir el riesgo introducido por la tecnología, mientras que los equipos de TI desean que las operaciones funcionen sin problemas y de manera eficiente con una interrupción o un tiempo de inactividad mínimos. Esto crea un conflicto de intereses inherente, que se ve exacerbado por la falta de integración de productos, uno de los mayores obstáculos en la remediación de vulnerabilidades en la actualidad. “Al consolidar el proceso de remediación de vulnerabilidades en una sola plataforma y eliminar la complejidad asociada con los productos aislados y los canales de comunicación cerrados, estamos reuniendo a los equipos de seguridad y TI bajo un mismo techo para tomar medidas y reducir el riesgo”, asegura el directivo, añadiendo que “tenemos nuestro propio motor para el seguimiento de CVE, tenemos nuestras propias capacidades de administración de parches. Nuestra plataforma permite a las empresas comprender primero dónde son

"Nuestra estrategia es movernos más rápido, y por ello lanzamos funciones semanalmente"

Michael Assraf,
CEO y cofundador, Vicarius

Vicarius proporciona información sobre amenazas, así como amplias capacidades de aplicación de parches y priorización

Roi Cohen, Michael Assraf y Yossi Ze'evi, fundadores de Vicarius

vulnerables, incluso antes de que esté disponible públicamente utilizando nuestra predicción de vulnerabilidad". Además, incluso si ya se sabe que hay una nueva vulnerabilidad, en lugar de ir a la plataforma y tener que manipularla "simplemente puede configurar una determinada política que la remediará automáticamente en todo su entorno".

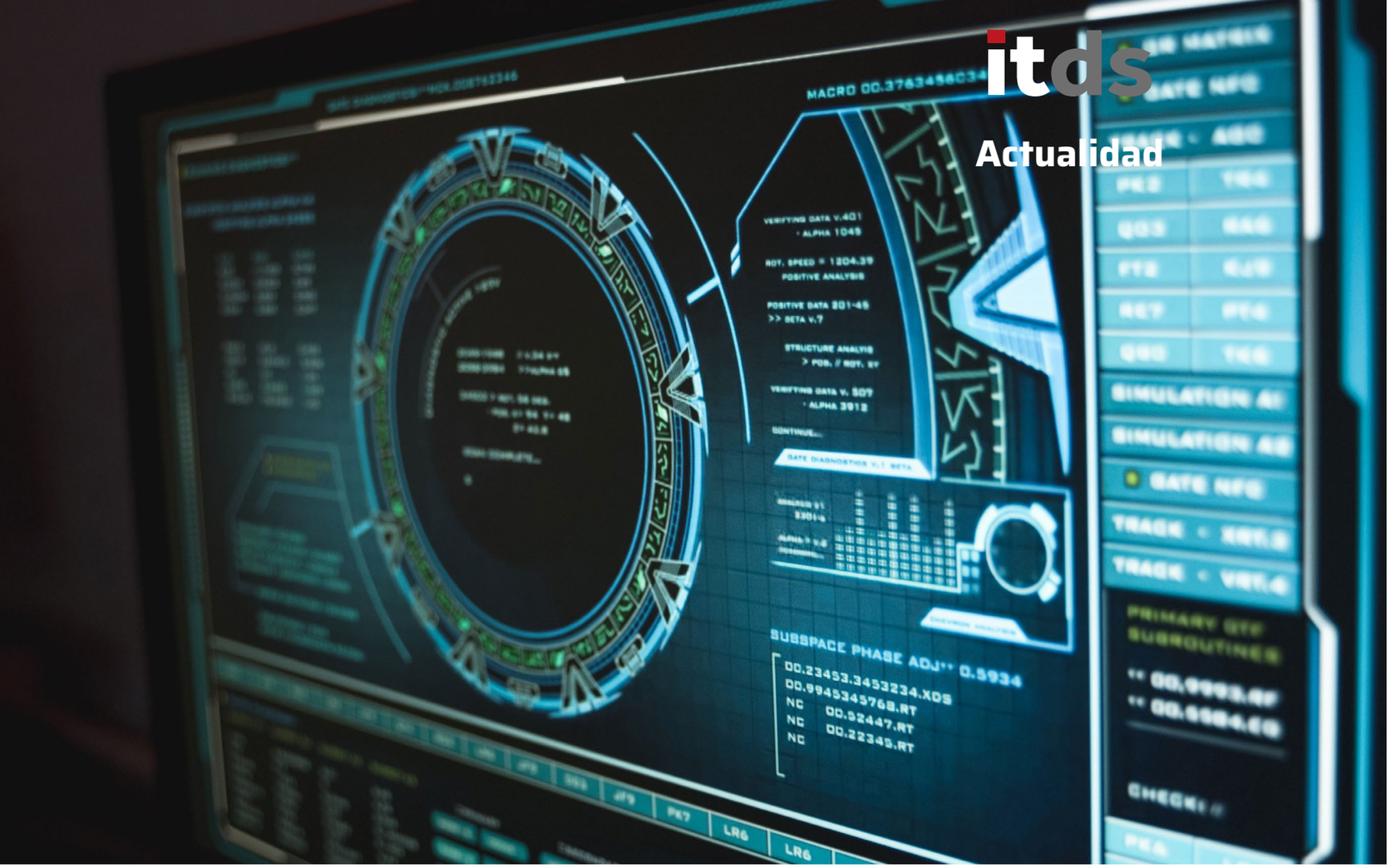
Sobre lo que la compañía quiere hacer con los 24 millones de dólares conseguidos en la última ronda de financiación, explica el CEO de Vicarius que hay dos objetivos, por un lado, mejorar el producto. Explica que entre los planes hay una plataforma social "para que los ingenieros de seguridad colaboren y compartan información sobre cómo solucionar vulnerabilidades". Además, la compañía está ampliando su soporte para dispositivos IoT y dispositivos no administrados que pueden escanearse con un agente; "pronto podremos admitir cualquier tipo de dispositivo en nuestra infraestructura", asegura Michael Assraf. La compañía, además, quiere ampliar el equipo de marketing y ventas y está en proceso de externalización.

En el corto plazo, prevé la compañía dos grandes lanzamientos. Por un lado, los usuarios de Nmap ("Network Mapper"), una utilidad gratuita y de código abierto para el descubrimiento de redes y la auditoría de seguridad, podrán llevar su escaneo a la plataforma de Vicarius de forma gratuita (se lanzará más información en breve). Además, se lanzará una plataforma social en la que encontrar ayuda para sobre cómo resolver una vulnerabilidad, "estamos construyendo una plataforma en la que todos, podrán sugerir la solución correcta. Así que será una colaboración de todos los ingenieros de seguridad del mundo. Podrán intercambiar opiniones y será completamente abierto".

Vicarius en España

Respecto a los planes concretos para el mercado español, "un mercado muy importante para nosotros y donde tenemos una parte bastante significativa de nuestro negocio", asegura el directivo que se está reforzando la presencia de la compañía a través de Ingecom, además de localizando los materiales y propuesta.

En todo caso, no llega Vicarius a un mercado yermo. Además de empresas muy conocidas en el mercado de gestión de vulnerabilidades, como pueden ser Trend Micro o Qualys, otras muchas están integrando herramientas de este tipo en sus propuestas de seguridad, como es el caso de Palo



Enlaces de interés...

- Detectados una media de 31.000 fallos de seguridad en cada organización
- El 47% de los ataques al sector industrial en 2021 se debieron a vulnerabilidades

El proceso desde la divulgación de la vulnerabilidad hasta el lanzamiento del parche, la implementación y las pruebas tarda en promedio de cuatro a seis meses

Alto… ¿Cuáles son los planes de Vicarius para competir con otras compañías que están mejor establecidas en nuestro en el mercado español? “Sabemos que estamos compitiendo con empresas muy grandes y buenas. Nuestra estrategia es movernos más rápido, y por ello lanzamos funciones semanalmente. Estamos extremadamente enfocados en el cliente, lo que significa que los clientes, incluso si acuden a un partner, siempre pueden comunicarse con nosotros. Además, estratégicamente decidimos que los socios locales saben mejor que nosotros cómo comunicar nuestra oferta a los mercados locales de todo el mundo, no solo en España. También proporcionan soporte local para la zona horaria correspondiente en el idioma correspondiente”.

Respecto a los planes de la compañía para este año, nos cuenta el CEO de Vicarius que, alcanzados los 150 clientes, “queremos triplicar la cifra y tener entre 400 y 500 clientes a finales de año”. También se prevé lanzar un portal de partners y mejorar los incentivos de los mismos.

Compartir en RRSS

La educación, uno de los sectores más afectados por el ransomware.

Sophos Endpoint

Intercept X

Bloquee los ataques de ransomware antes de que causen estragos en su entorno con tecnología antiransomware que detecta procesos de cifrado malicioso y los neutraliza antes de que puedan propagarse por la red.

sophos.com/es-es/endpoint

SOPHOS
Cybersecurity evolved.

21-09-20 ES(DD)

CATO Networks, el jugador SASE/SSE con red propia que busca abrirse hueco en España

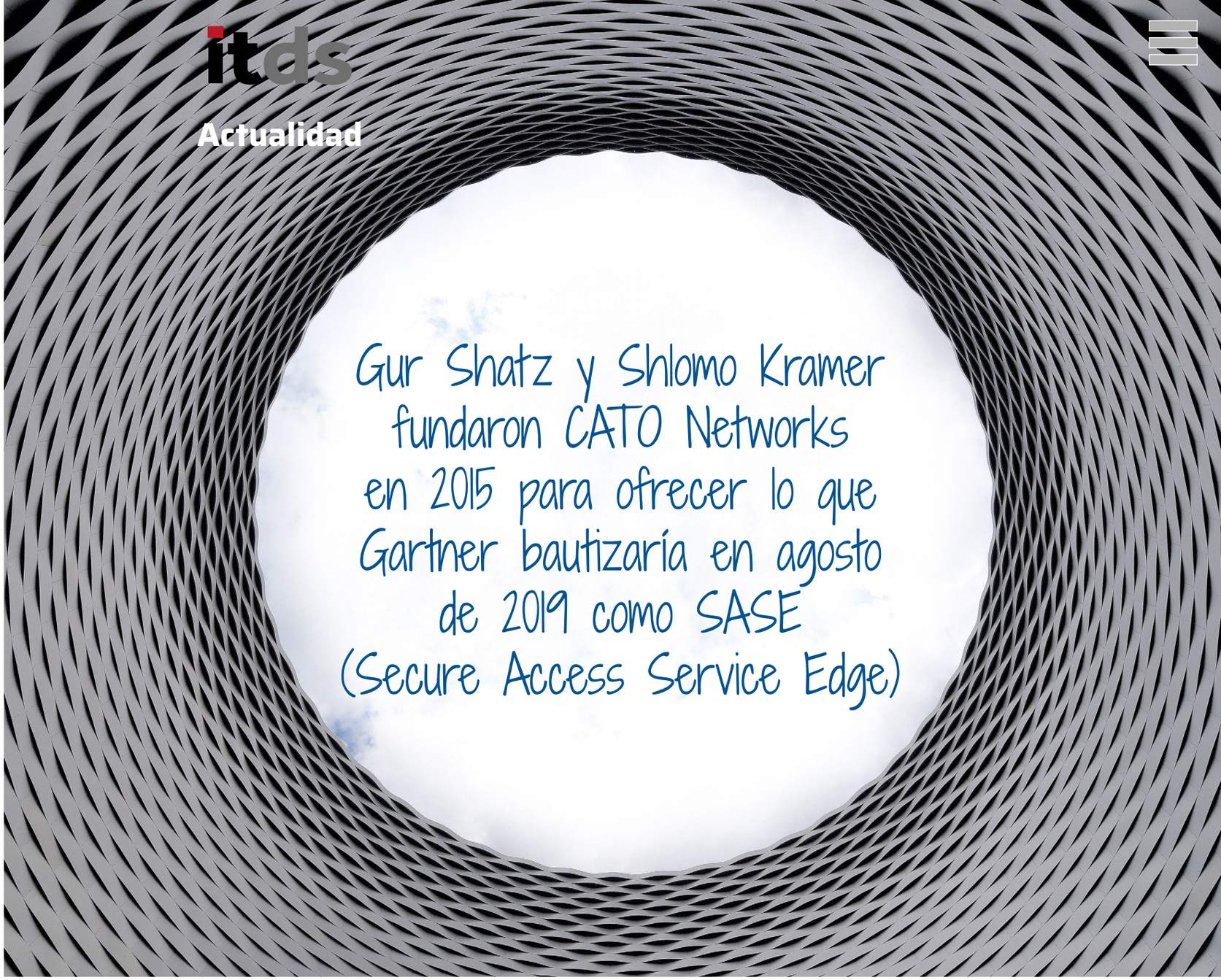
Mientras el mercado sigue empujando la adopción de SASE (Secure Access Service Edge) y Gartner decide crear otro cuadrante, SSE (Secure Service Edge), CATO Networks inicia sus operaciones en España. Su gran ventaja: contar con su propio backbone, su propia red troncal; su estrategia para competir en un mercado con jugadores relevantes: el canal.

Cuando los fundadores de tu compañía son los mismos que años atrás fundaron Check Point o Imperva lo cuentas. Y lo haces porque es relevante. Y eso es lo que hizo Christophe Lopez-Castel, responsable de canal para el sur de Europa de CATO Networks cuando nos encontramos hace unas semanas. Un encuentro casi fortuito ya que tras contactar a través de la página web del fabricante para saber qué planes había para el mercado

español, estaba programada una visita a Madrid tan sólo una semana después para, casualidades de la vida, mantener varias reuniones que llevarán a la apertura de una oficina de la compañía en los próximos meses.

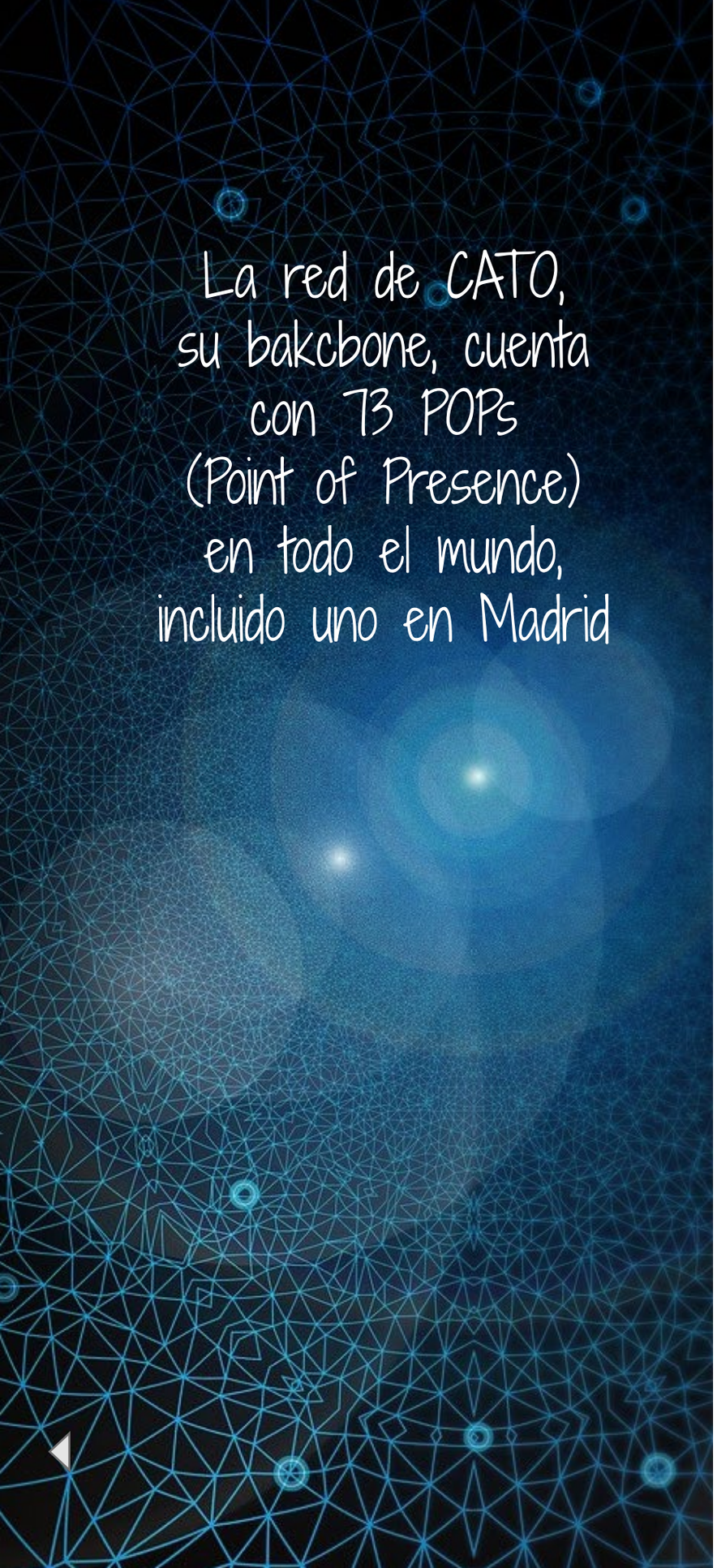
Gur Shatz y Shlomo Kramer fundaron CATO Networks en 2015 para ofrecer lo que Gartner bautizaría en agosto de 2019 como SASE (Secure Access Service Edge). Asegura Christophe Lopez-Castel que la compañía es capaz de conectar todos los edges, que el directivo identifica como recursos y que pueden ser desde un servidor en Azure como el móvil de un usuario, una oficina remota; “somos capaces de conectar cualquier tipo de recurso con CATO SASE Cloud para después securizar cualquier tipo de tráfico entre los diferentes recursos, así como entre internet, la nube o una aplicación SaaS y el recurso. Y después proporcionar a los clientes o partners una única consola para gestionarlo todo de forma que puedes conectar todos tus recursos, asegurar todo el tráfico y utilizar una sola consola para monitorizar, gestionar y configurar todo. Esta es la propuesta de valor de CATO Networks”, dice Christophe Lopez-Castel.

La compañía, que tiene su sede en Tel Aviv, se expandió primero a Estados Unidos para después ampliar mercado en las regiones de APAC y EMEA. CATO Networks abrió oficina en Francia en Septiembre de 2019, casi al mismo tiempo que en Italia, países en los que, donde según Christophe Lopez-Castel, ya tienen más de 30 clientes



en producción, de los más de 1.100 que tienen en todo el mundo. Asegura también el directivo que la compañía “necesita continuar con nuestro crecimiento y nuestro desarrollo en Europa”, y España es su nuevo destino.

Sobre la decisión de Gartner de crear un nuevo cuadrante llamado SSE (Secure Service Edge), explica el responsable de canal para el sur de Europa de CATO Networks, que la principal diferencia entre SSE y SASE es la “A” de Access, y por lo tanto es el backbone. En sus comienzo CATO decidió construir un backbone, que es “uno de los principales diferenciadores ahora mismo en el mercado”, asegura, añadiendo que son muchas las empresas que reclaman estar haciendo SASE, pero que, si nos fijamos en lo que dice Gartner, hay cuatro pilares “que no son negociables: el primero es que tienes que ser nube; el segundo es



WHAT IS SASE?
THE BENEFITS OF SECURE ACCESS SERVICE EDGE

CLICAR PARA VER EL VÍDEO

que tienes que ser global; el tercero es que tienes que converger la red y la seguridad; y el último es que tienes que dar servicios para todos los Edge". Explica el directivo que SSE no incluye el acceso y eso hace que salgan de la ecuación muchos fabricantes que no son capaces de ofrecer un backbone porque "supone una inversión de cientos de millones de dólares". La red de CATO, su bakcbone, cuenta con 73 POPs (Point of Presence) en todo el mundo, incluido uno en Madrid.

Ese backbone es lo que permite a la compañía conectar una oficina en París y un site en Madrid, "y lo importante, el valor para el cliente, es converger en una nube, una aplicación y una plataforma con todos los servicios relacionados con la red, incluido el acceso y la seguridad".

No siendo un completo desconocido, CATO llega a un mercado, el español, donde ya hay jugadores de SASE bien establecidos (Netskope, Zscaler, Palo Alto, Cisco, Forcepoint…). ¿Cómo

"Somos capaces de conectar cualquier tipo de recurso con CATO SASE Cloud para después securizar cualquier tipo de tráfico"

Christophe Lopez-Castel, South EMEA Channel Manager, CATO Networks

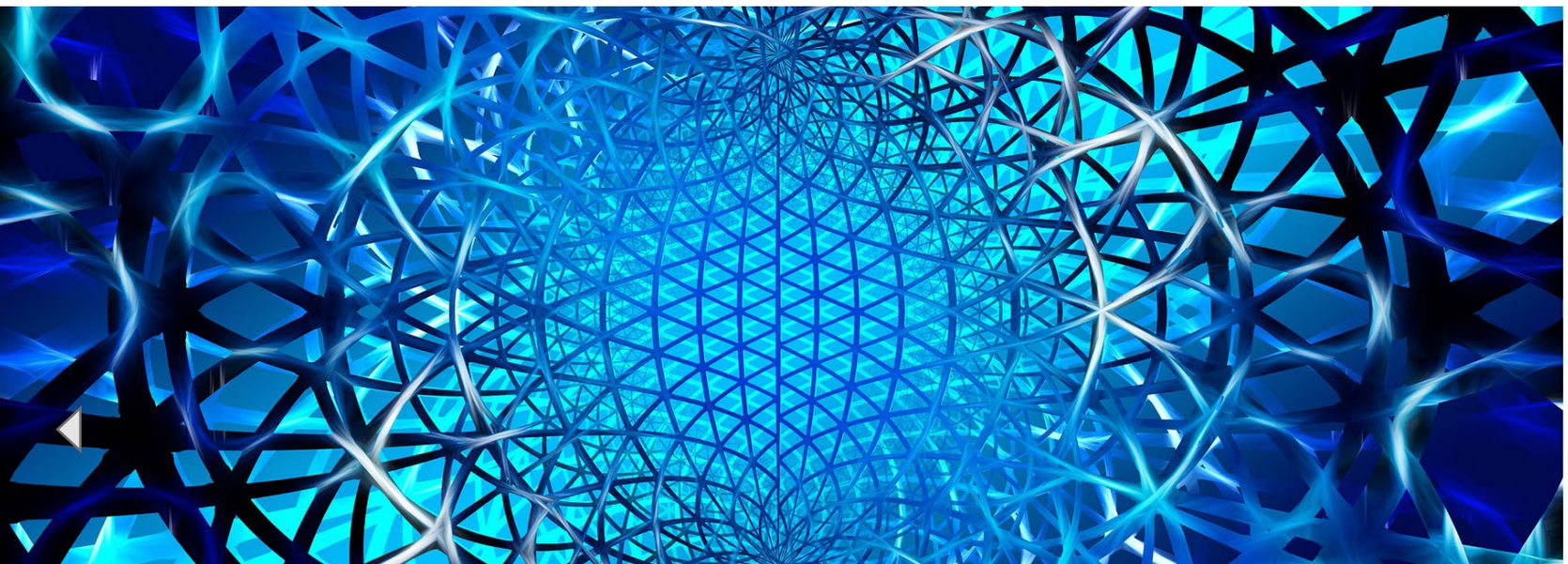
Enlaces de interés...

- Canal de YouTube de CATO Networks

quieren competir? Dice Christophe Lopez-Castel que ya se vivió la misma situación en Francia y en Italia y que la estrategia será la misma: "somos una compañía de canal y vamos a crear un modelo Tier2. Vamos a empezar con un acuerdo con un distribuidor de valor, que es Nuvias y después reclutaremos partners para crear un ecosistema de canal que entienda las necesidades del cliente", explica el directivo añadiendo que se contratarán recursos porque, como ya ha ocurrido en el resto de países, "cuando tienes recursos propios, los clientes pueden comprender el valor de nuestro modelo".

Asegura también el responsable de canal de CATO para el sur de Europa, que se necesita tener el socio adecuado que crea en tu propuesta de valor, "y parece que con más de 1.100 clientes en el mundo nuestra propuesta parece importante".

Preguntamos también a Christophe Lopez-Castel por el cliente tipo de CATO Networks. Dice que puede tener tanto presencia nacional como internacional; "en Francia o Italia, el 50% de nuestros clientes son empresa nacionales, o utiliza CATO a nivel nacional, y el 50% son empresa internacionales". Además, el en 50% de los casos son empresas privadas. En cuanto al tamaño, habal de midmarket, empresas con entre 50 y 5.000 empleados, "pero lo importante es un cliente con una estrategia multicloud". En todo caso, asegura también, el valor del backbone de CATO es enorme.



Compartir en RRSS

STORMSHIELD

La opción europea en ciberseguridad

El partner de confianza
para
securizar sus
infraestructuras operacionales y sensibles

www.stormshield.com

‘Invertimos muchísimo esfuerzo, tiempo y campañas de concienciación en diferentes medios para que el cliente sea nuestro principal aliado’

(Gustavo Lozano, ING)

Texto: Rosalía Arroyo • Fotos: Ania Lewandowska

CISO de ING desde hace más de tres años, Gustavo Lozano asegura que quien no tenga la seguridad como una prioridad no va a subsistir; ve la regulación como una oportunidad para innovar; cree que para ser un buen CISO hay que tener una base sólida de conocimientos de gestión; que están por llegar muchas más soluciones que exploten la ingente cantidad de información que se maneja en seguridad para ofrecer algo más específico y que el reto para evitar el fraude es que replicar en el mundo digital lo que no se hace en el mundo físico.

Antes de elegir carrera ya le gustaba la informática. Y antes de terminarla ya le llamó la atención la seguridad informática. Entre sus profesores dos conocidos del sector: Alfonso Mur y Luis Carro, ambos gerentes de Arthur Andersen. “Quizá fuera la manera de explicarlo, o el entusiasmo que transmitían, pero fue en ese momento, en segundo de carrera”, cuando la seguridad y el control IT le atrajo, y llevó a Gustavo Lozano, hoy CISO de ING, a seguir a sus dos profesores para realizar auditorías y consultorías

"No se debe perder ninguna característica de seguridad por el hecho de ir a la nube"

de seguridad. Años después, en SIA, se adentró definitivamente al mundo de la seguridad aprendiendo a realizar planes directores de seguridad, análisis de riesgos… El camino natural fue saltar al otro lado, a convertirse en responsable de seguridad en DIA, creando el área de seguridad informática dentro de la organización, y, finalmente, en CISO, cargo que ocuparía durante 13 años hasta que decidió "cambiar de sector y seguir aprendiendo". Hace más de tres años que es el CISO de ING, una empresa que contempla la seguridad de una manera integral, en la que los departamentos de seguridad lógica o la cyber y seguridad física, están unidos además de otras funciones relevantes como la continuidad de negocio, arquitectura de seguridad, seguridad de aplicaciones y gestión de identidades.

Cuando le preguntamos por las cualidades que debe tener un buen CISO habla Gustavo Lozano de "mucha profundidad técnica, mucho conocimiento". No cree que haya que ser un especialista a nivel hacker, "pero sí conocer técnicas, vectores de ataque, soluciones, amenazas, y algo muy importante: tener una base sólida de conocimientos de gestión". Tener resiliencia personal y profesional es, en opinión de este directivo, otra cualidad necesaria para un CISO, "una figura a la que cada se ha ido concentrando mucha responsabilidad y complejidad". Añade el tener capacidad de comunicación "si quieres crear cultura de seguridad", además de "tener visión del sector en el que estás como negocio, aprenderlo, porque es la forma de aportar más desde el diseño".

Amenazas que quitan el sueño

ING es un banco digital con presencia en 40 países. Asegura Gustavo Lozano que la seguridad y el cumplimiento son prioridad absoluta, y no sólo parea el área de seguridad, sino en todo el banco ya que está embebida en procesos e incluida en objetivos. Cuando le preguntamos qué amenazas le preocupan más dice que "nuestra máxima prioridad es mantener el banco seguro y disponible", por lo que todo lo que tenga que ver con amenazas contra la disponibilidad (DDoS) es clave. Se busca que el banco sea resiliente desde un punto de vista de infraestructura frente a un ataque de denegación de servicio, además de ser capaces de prevenir, detectar y reaccionar, para lo que es fundamental "tener una buena infraestructura, procesos engrasados en cuanto a detección y alertado, y gente muy preparada y entrenada para mitigarlo".

Cualquier amenaza que pueda afectar a datos, tanto de los clientes como de los propios procesos internos de la compañía, es también prioridad para Gustavo Lozano. "Cualquier tipo de intento de intrusión es otro vector de ataque que nos preocupa porque de ahí se podría derivar un ransomware", explica, para después añadir un tercer vector de ataque sobre el que se mantiene alerta:

"La identidad, tanto del empleado como del cliente, se va a poner en el centro"

la protección Web y de App, “ya no sólo desde un punto de disponibilidad, sino de acceso, para prevenir el fraude”.

¿Ser un banco digital hace que vuestros clientes estén mejor preparados para tratar con la tecnología y de alguna forma sean más precavidos? Dice Gustavo Lozano que, sin saber en detalle lo que sucede en otras entidades, “lo que sí sé es que invertimos muchísimo esfuerzo y tiempo en campañas de concienciación en diferentes medios para que el cliente sea nuestro principal aliado”. ING, además, ha trabajado en mejorar la página de seguridad de la web, se lanzan mensajes personalizados en cada canal, o cuando se piden segundas validaciones en transacciones se incluyen mensajes específicos.

Por supuesto, desde ING la colaboración en el sector y hacia Fuerzas y Cuerpos de Seguridad del Estado es total para luchar contra la ciberdelincuencia.

El reto para evitar el fraude, explica el directivo, es replicar en el mundo digital lo que no se hace en el mundo físico, como es no dar nuestra documentación o las llaves de nuestro coche o nuestra casa al primero que pasa por la calle; “eso es lo que sucede en el mundo digital y eso es lo que tratamos de evitar”. Añade que también se hace un esfuerzo importante en el ámbito interno ya que los empleados de la compañía, independientemente del departamento, “están preparados para detectar un phishing o un mensaje sospechoso. Además, las áreas que están en contacto directo con el cliente están preparados para gestionar alertas, pudiendo llegar a parar en tiempo real un ataque”. El uso de determinadas herramientas y procesos lleva a Gustavo Lozano a asegurar: “hemos conseguido reducir el fraude a la mínima expresión”.

Cuando le preguntamos si la seguridad se ha convertido en una prioridad para la empresa española, dice que “para ING es una prioridad absoluta. Está en el ADN de la compañía y se tiene en cuenta desde el diseño”. Además de la seguridad, la privacidad es también prioritaria, y respecto a los datos, se trabaja estrechamente con el DPO para crear cultura de seguridad.

Como profesional del sector, añade Gustavo Lozano que hay sectores en los que todavía queda mucho por hacer a pesar de que “quien no tenga

hoy en día la seguridad como un pilar, como una prioridad, no va a subsistir. Es un factor clave en la existencia de una empresa, independientemente del sector".

Cómo escoger

En un mercado saturado de fabricantes, soluciones y propuestas, ¿cómo se escoge la herramienta de seguridad adecuada? Explica Gustavo Lozano que al estar dentro de una multinacional "tratamos de que las soluciones sean las mismas". Dice que, dependiendo del análisis de riesgos, necesidades y plan de seguridad aprobado, se va al mercado y, a la hora de escoger, se tienen en cuenta informes donde se compara la tecnología, "pero lo fundamental es que invertimos mucho tiempo y dinero en pruebas. Es decir, se eligen con diferentes criterios ciertos fabricantes, y después se hacen pruebas específicas de rendimiento, efectividad, etc."; las pruebas se reparten entre diferentes países para ponerlas en conjunto en un grupo de trabajo, y si es un producto que va más allá de lo nacional, que se quiere implantar en todos los países, ya se hace el contacto a nivel global".

"Más que pensar que hay muchos fabricantes, a mí siempre me preocupa saber quién va a ser el integrador"

En todo caso lo importante es quién lo va a implantar; "más que pensar que hay muchos fabricantes, a mí siempre me preocupa saber quién va a ser el integrador, porque todo se basa en las personas". Añade además Gustavo Lozano que "en la ecuación cliente-fabricante-integrador, la parte de integrador es la que más peso tiene para el éxito del proyecto".

Sobre el cloud dice que "ING apuesta por la innovación y estamos en pleno proceso de transición hacia la nube privada", dice el directivo. Explica que desde el punto de vista de la seguridad "el factor principal es conocer cuál es tu arquitectura de seguridad. Da igual que sea on-premise o que sea en cloud. La base sigue siendo ese análisis de riesgos, tener una arquitectura de seguridad sólida y, a nivel de requisitos, se deben mantener independientemente de si estás on- premise o en cloud. No se debe perder ninguna característica de seguridad por el hecho de ir a la nube".

"Sí, tenemos servicios de seguridad gestionados, pero apostamos por la internalización, al menos en todo lo que son procesos críticos" responde Gustavo Lozano cuando le preguntamos por los servicios gestionados de seguridad.

Regulación

El sector de banca y seguros es uno de los más maduros a nivel tecnológico y de ciberseguridad. Es también uno de los más regulados, con normativas

más estrictas a nivel de protección de activos. ¿Cómo impacta esa alta regulación en el mercado bancario? “Yo creo que hay que utilizarlo como una oportunidad. La regulación pretende proteger al ciudadano, proteger al cliente, y en ING lo vemos como una oportunidad para ofrecer aplicaciones y servicios más seguros”.

Además de como una oportunidad, ve Gustavo Lozano la regulación como un reto “porque es cambiante, hay que adaptarse y los nuevos requisitos también abren la puerta a innovar en cuanto a soluciones de seguridad”.

Tecnologías a futuro

Hablando sobre tecnologías imprescindibles y las que habrán de serlo en los próximos años, nos cuenta Gustavo Lozano que en ING ya hay prácticamente de todo en las diferentes capas de protección. Menciona como fundamental la protección del endpoint, puesto de trabajo, herramientas de colaboración, correo electrónico, anti spam o navegación de usuario. Añade un segundo pilar de protección en torno a la infraestructura, y menciona los firewalls, herramientas de detección de amenazas avanzadas, IPS, y todo lo que tiene que ver con la segmentación de la red, tanto en infraestructura on-premise como en cloud.

Dice que todo el mundo dispone de firewalls, módulos de filtrado de diferentes capas y que le parece fundamental la evolución de esas tecnologías y mantenerlas actualizadas porque, “en general, no se aprovecha todo el potencial que ofrece la tecnología que has implantado” y porque “no sólo es tener más presupuesto para buscar nuevas cosas, sino mirar lo que tienes, explotarlo, evolucionarlo, hacer un fine-tunning de las herramientas e invertir en el equipo, en su formación y certificación para que puedan explotar esas tecnologías”.

Asegura que la tercera palanca a tener en cuenta es todo lo que tiene que ver con monitorización e integración entre consolas, porque “de nada vale tener diez consolas si no correlas los incidentes de seguridad”. Añade que a futuro cobrarán más importancia las tecnologías que exploten mejor la

"Hay una oportunidad muy buena que en cuanto a unir la gestión de la seguridad con la gestión del dato"

"En general, no se aprovecha todo el potencial que ofrece la tecnología que has implantado"

información, las alertas, que las correlen y agreguen patrones de comportamiento; "además, hay una oportunidad muy buena en cuanto a unir la gestión de la seguridad con la gestión del dato, de la información. Yo creo que tienen que venir muchas más soluciones de cómo explotar esos volúmenes tan ingentes de información que manejamos en seguridad en cuanto a alertas para ofrecer algo más específico".

También mirando hacia el futuro asegura Gustavo Lozano que la identidad, tanto del empleado como del cliente, se va a poner en el centro, que las empresas están evolucionando sus modelos de gestión de identidad, haciéndolos más conectados para evitar que haya diferentes islas de autenticación, "porque de ahí dependen todos los procesos de detección de amenazas que vienen detrás. Las herramientas están basadas en la identidad y esa correlación de identidad de empleado cliente, hacia dónde se mueve, cómo opera, cuál es su comportamiento, o lo tienes bien armado o el resto de las herramientas que están en la parte de detección y de reacción no van a funcionar correctamente".

Respecto a la situación actual, y a lo que queda de este año, pone sobre la mesa Gustavo Lozano la gestión de riesgos de terceros; "todos estamos haciendo esfuerzos importantes por asegurar la resiliencia de los terceros, ayudar y colaborar para evitar que se vean impactados por ciberataques, y que ese impacto nos afecte a nosotros".

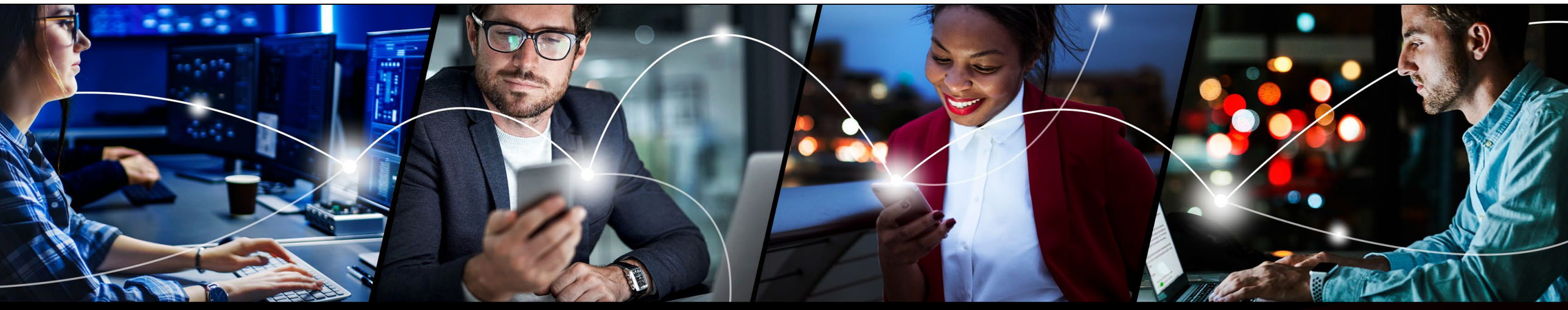
En este aspecto la compañía cuenta con un framework a nivel internacional para asegurar la cadena de suministro que está construido en base a tipología de acceso a la información y la criticidad de proceso.

Enlaces de interés...

- 'La seguridad se convertirá en una ventaja competitiva de las empresas' (Pablo Masaguer, CISO, Sociedad Textil Lonia)
- 'Lo importante, y más en el ámbito de la seguridad, no es tanto la solución o producto que vayas a seleccionar, sino el proveedor' (Roberto González, Grupo Primavera)
- "Resisten los que se adaptan" (Belén Pérez, CISO, Grupo Nueva Pescanova)
- 'Identificar los roles críticos en la organización, que no necesariamente son los del comité de dirección, es fundamental' (Gabriel Moliné, Leroy Merlín)
- 'En los próximos años la tendencia en ciberseguridad será el análisis de comportamiento' (Mario Andrés, Mercadona)
- 'Identificar los roles críticos en la organización, que no necesariamente son los del comité de dirección, es fundamental' (Gabriel Moliné, Leroy Merlín)

Compartir en RRSS

Seguridad unificada para un mundo RECONECTADO



SEGURIDAD DE RED

AUTENTICACIÓN MULTIFACTOR

NUBE SEGURA WI-FI

SEGURIDAD ENDPOINT

Unified Security Platform™

CLARIDAD Y CONTROL | **SEGURIDAD INTEGRAL** | **CONOCIMIENTO COMPARTIDO** | **ALINEACIÓN OPERATIVA** | **AUTOMATIZACIÓN**

Contacto: +34 917 932 531

Email: spain@watchguard.com

www.watchguard.com

‘La colaboración con terceros es fundamental en el mundo de la ciberseguridad’

(Juan Luis Garijo, Crowdstrike)

Desde su fundación en 2011 como uno de los primeros visionarios en un mercado de seguridad endpoint que fue bautizado como EDR (Endpoint Detection and Response), Crowdstrike acumuló 481 millones de dólares en cuatro rondas de inversión, ha realizado cuatro adquisiciones, salido a Bolsa y pasado a proteger no sólo los puntos finales de las empresas, sino los datos, las identidades y el cloud.

Rosalía Arroyo

Tras casi seis años en Palo Alto, Juan Luis Garijo es, desde hace año y medio, el responsable de Crowdstrike en la región de Iberia, que es donde la compañía ha decidido establecer el heaquarter europeo, concretamente en Barcelona. De forma que, si al ocupar su puesto, la compañía estaba compuesta por tres personas en España, “ahora dirijo un equipo de 20” y además en la región se pagan más de 85 nóminas.

Nos cuenta Juan Luis Garijo que cuando George Kurtz, ex CTO de McAfee, fundó Crowdstrike en 2011 es porque ya previó un aumento exponencial de ataques, y estableció dos casuísticas: la respuesta ante incidentes y la ciberinteligencia. Explica que para hacer una buena respuesta ante

incidentes hace falta entender cómo trabajan los ciberdelincuentes, lo que llevó a la compañía, ya en 2011, a hacer un trabajo exhaustivo de cualificar quiénes son los cieberdelincuentes, qué tipos de crimen organizado hay, con qué objetivo realizan un ciberataque, qué tipo de técnicas utilizan, qué tipo de extorsión, o si son ataques estado nación, o de cadena de suministro o si lo que quieren es recaudar dinero, exfiltrar información, etc., “porque una vez consigues entender el problema de facto, eres capaz de resolver esa respuesta”.

Entre 2011 y 2015 “utilizábamos herramientas de terceros para hacer ese ejercicio de respuesta de incidencias”, pero sabiendo qué herramientas y técnicas harían falta para hacer esa respuesta de manera más eficientes, decidieron desarrollar las suyas propias, “y así nace la plataforma Falcon”, que actualmente tiene 23 módulos y se espera que tenga hasta 30 en los próximos seis meses.

En julio de 2019 y ya con 5.000 empleados, la compañía sale a Bolsa con una capitalización de mercado de 43.000 millones de dólares, el doble que Telefónica. Se ha convertido, además, en la segunda compañía que más rápido ha pasado de facturar un dólar a superar el billón de dólares de facturación, por detrás de Salesforce, “

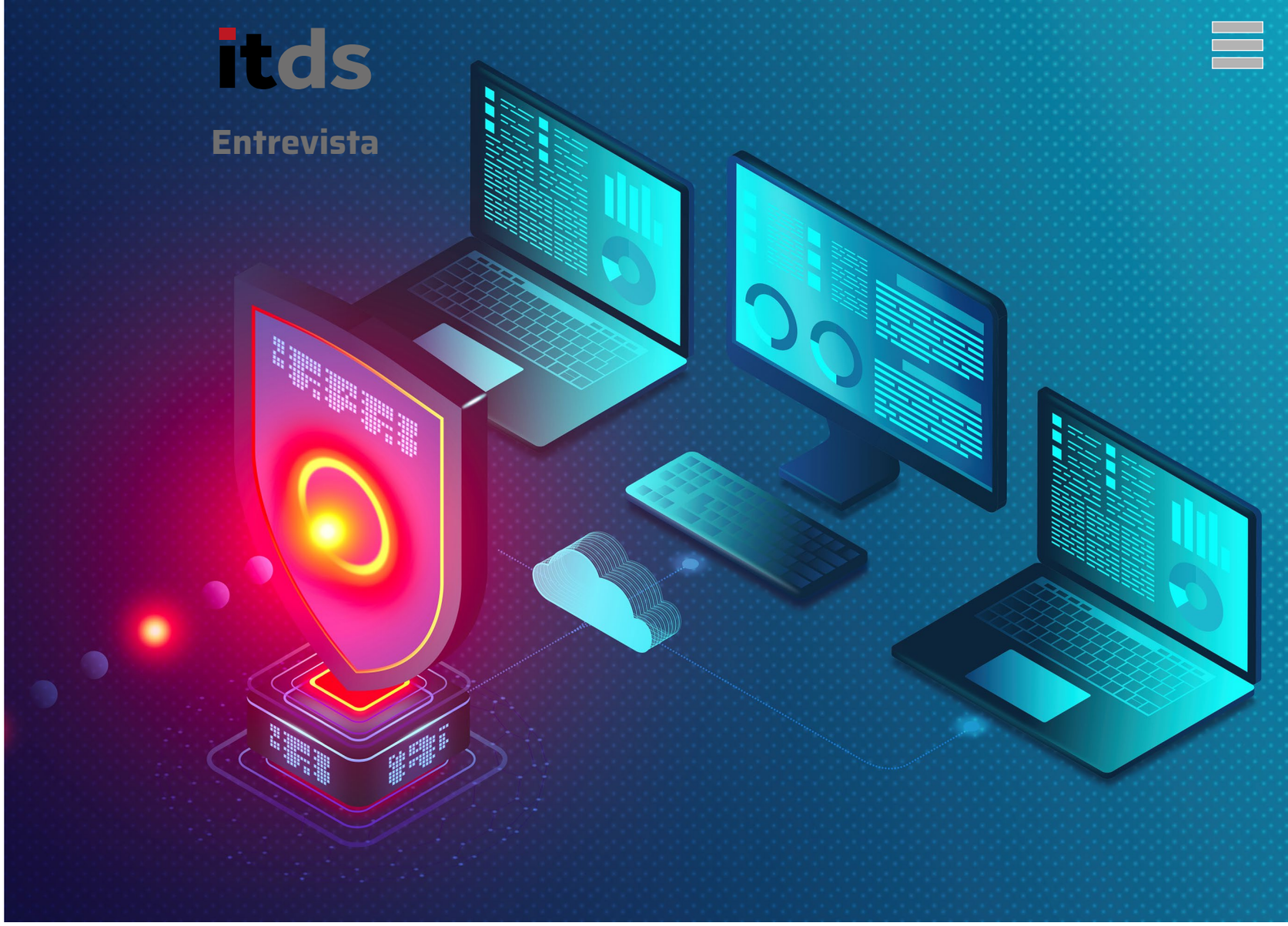
A nivel Iberia, en los dos años y medio que la compañía lleva en este territorio, se han conseguido como clientes a 16 empresas del Ibex 35, “que han apostado por nuestra tecnología para proteger tanto sus entornos de endpoint como de estaciones de trabajo, máquinas virtuales, o servidores de toda índole”, asegura Juan Luis Garijo añadiendo que Crowdstrike ha conseguido demostrar que “resolvemos problemas reales” y que, “poniendo mucho foco en la prevención, es fundamental, cuando uno recibe un ataque, ser capaz de detectar y remediar en muy poco tiempo”. Teniendo en cuenta que cuando se produce un cibertaque el tiempo es oro, el objetivo de la compañía es: detectar un ataque en menos de un minuto, analizarlo en menos de diez y remediarlo en menos de 60 minutos”.

"Cada vez tenemos más partners que quieren ser afines a nuestra tecnología, porque resolvemos problemas reales de seguridad y muchos integradores que tiene con los mejores"

Diferencial de Crowdstrike

Para el responsable de la compañía para la región de iberia, entre los diferenciales de la compañía destacan tanto la visibilidad como la inteligencia; “nadie en este mercado tiene concatenado y

Teniendo en cuenta que cuando se produce un cibertaque el tiempo es oro, el objetivo de la compañía es: detectar un ataque en menos de un minuto analizarlo en menos de diez y remediarlo en menos de 60 minutos



cualificados a los cibercriminales como los tenemos nosotros". Asegura el directivo que la compañía tiene detectados más de 150 grupos de cibercrimen organizado y que son capaces de identificar en muy poco tiempo quién está atacando y qué objetivo tiene.

La información de ciberinteligencia, que es algo que está cada vez más de moda y donde triunfan empresas como ZeroFox o KELA, es un servicio propio de Crowdstrike. El sistema de ciberinteligencia de la compañía se llama Falcon X donde hay un módulo concreto que se llama Recon que permite adentrarse en la Deep y Dark Web, donde se categoriza en tiempo real cualquier exfiltración de tarjetas de crédito, robo de propiedad intelectual en un laboratorio farmacéutico, robo de contraseñas en una compañía de seguros… "y podemos avisar en cuestión de segundos a las empresas afectadas".

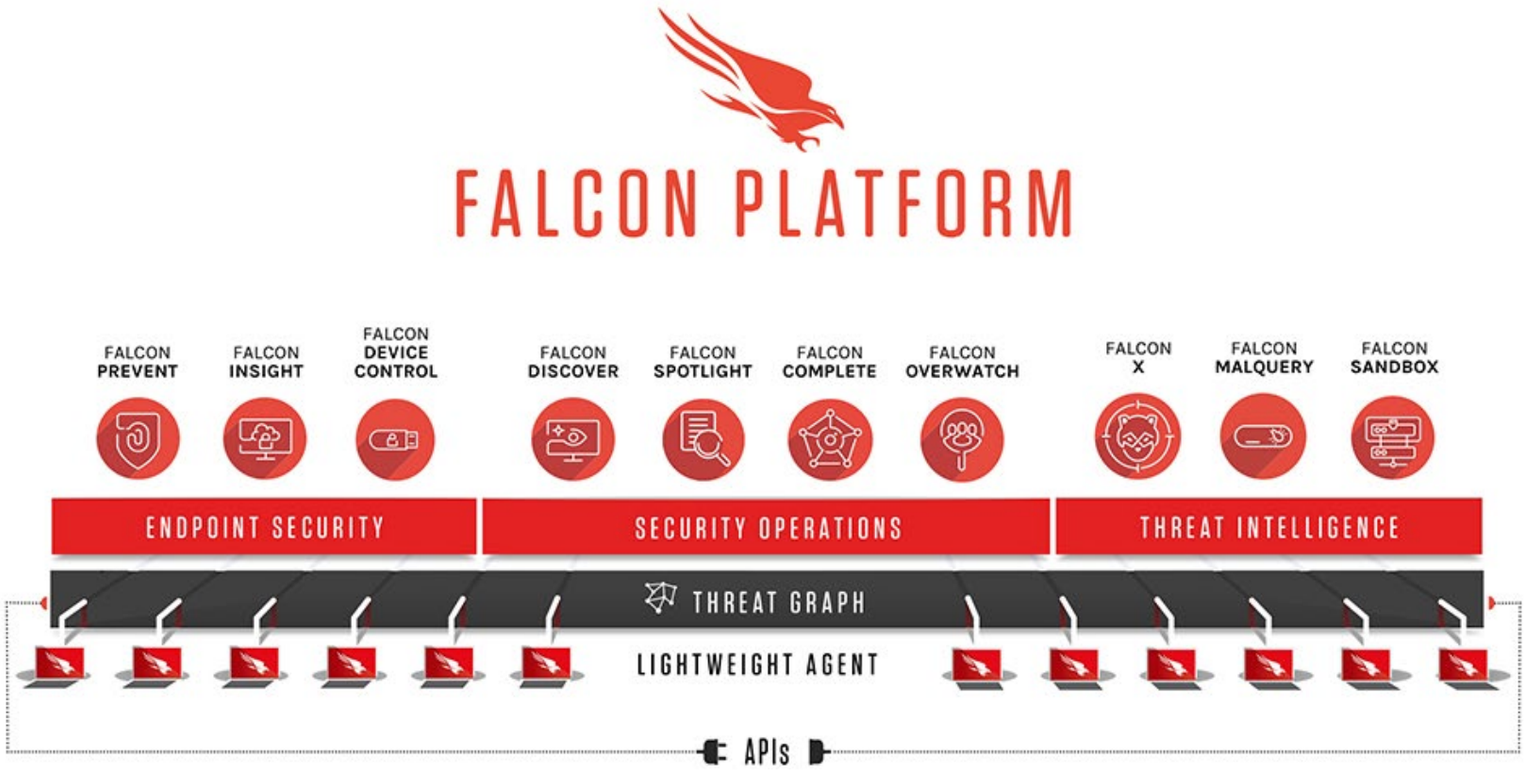
Volviendo a Falcon, la plataforma de la compañía en la que no dejan añadirse nuevos módulos, nos cuenta Juan Luis Garijo que lo que habitualmente demanda el cliente como parte de un acuerdo "es tener acceso a la parte de telemetría, a la parte de servicio de Threat Hunting, que es OverWatch. Otro módulo que se usa mucho es el de Discover", que permite detectar a tiempo real qué ordenadores están bien plataformados, bien actualizados, etcétera; "imagínate tener ese conocimiento con una base instalada en 200 países distintos, con husos horarios distintos".

La plataforma Falcon permite satisfacer cualquier caso de uso, "pero principalmente destacaría la

Falcon, el secreto del éxito

Falcon es, sin duda, el valor diferencial de Crowdstrike. La compañía aprovecha los datos empresariales y de seguridad de los clientes conectados a su plataforma de ciberseguridad, y utiliza su agente ligero habilitado y la base de datos Threat Graph para generar correlaciones con los eventos de ciberseguridad. Cuantos más datos de seguridad del cliente se introduzcan en Falcon, más inteligente se vuelve la nube de seguridad para brindar detección, prevención y/o respuesta rápidas contra ciberataques y amenazas.

La plataforma Falcon actualmente ofrece 22 módulos en la nube, que cubren una amplia gama de soluciones de ciberseguridad, desde seguridad en la nube y protección de identificación, hasta inteligencia de amenazas y detección y respuesta extendidas. El enfoque basado en la nube de CrowdStrike permite la expansión oportuna de las ofertas de módulos en respuesta a los riesgos empresariales. La capacidad de la empresa para implementar de forma rápida módulos adicionales para los clientes sin necesidad de configuración ni consultoría adicional ha sido una característica atractiva para las empresas globales que intentan reforzar sus ciberdefensas a medida que migran más cargas de trabajo a la nube



visibilidad, la ciberinteligencia y la parte de Threat Hunting", que es Falcon Overwatch un servicio gestionado de Threat Hunting que permite, en tiempo real, ser capaces, a cualquier hora del día, "detectar una alarma en un cliente, llamarle y decirle: te están intentando atacar, pongámonos manos a la obra".

Acuerdos con terceros

La volumetría masiva de datos que ya vaticinó George Kurtz está en pleno auge. Es el tiempo de la ingesta de información de toda índole para poder hacer frente a una situación que se hace cada vez más complicada. La estrategia de Crowdstrike es entenderse e integrarse con otras muchas empresas, desde Netscope o Zscaler, a Okta o Proofpoint… "Tenemos obsesión por entendernos con terceros e ingestar información de terceros en toda su índole", que ha llevado a la compañía más allá del endpoint, ingestando no sólo los datos que generan los puntos finales, sino los que se generan en la nube o en las redes.

Con esta estrategia abierta la compañía y un mensaje de integración con terceros, "porque no queremos ser un mercado propietario", la compañía no sólo participa en el mercado ERD sino en las sucesivas tecnologías que se han acoplado a la detección y respuesta, como es el NDR (Networks Detection and Response) o XDT (eXtended Detection and Response). "La compartición, la colaboración con terceros es fundamental en el mundo de la ciberseguridad", asegura Juan Luis Garijo.

El espíritu de alianzas es la que permite a Crowdstrike proteger cualquier punto final. Si hablamos de manera específica de IoT, resalta Garijo la integración con empresas como Clarity o Armis.

Dentro de este espíritu de colaboración, la compañía ha trabajado con el CCN para homologar su tecnología y estar incluido en la Guía de Seguridad de las TIC CCN-STIC 105.

Adquisiciones

Crowdstrike está creciendo de manera orgánica entre un 65% y un 70% año tras año, “pero se están viendo nuevas necesidades de seguridad en los ciberataques”, por lo que en los últimos 16 meses se han realizado tres adquisiciones estratégicas, nos cuenta Garijo.

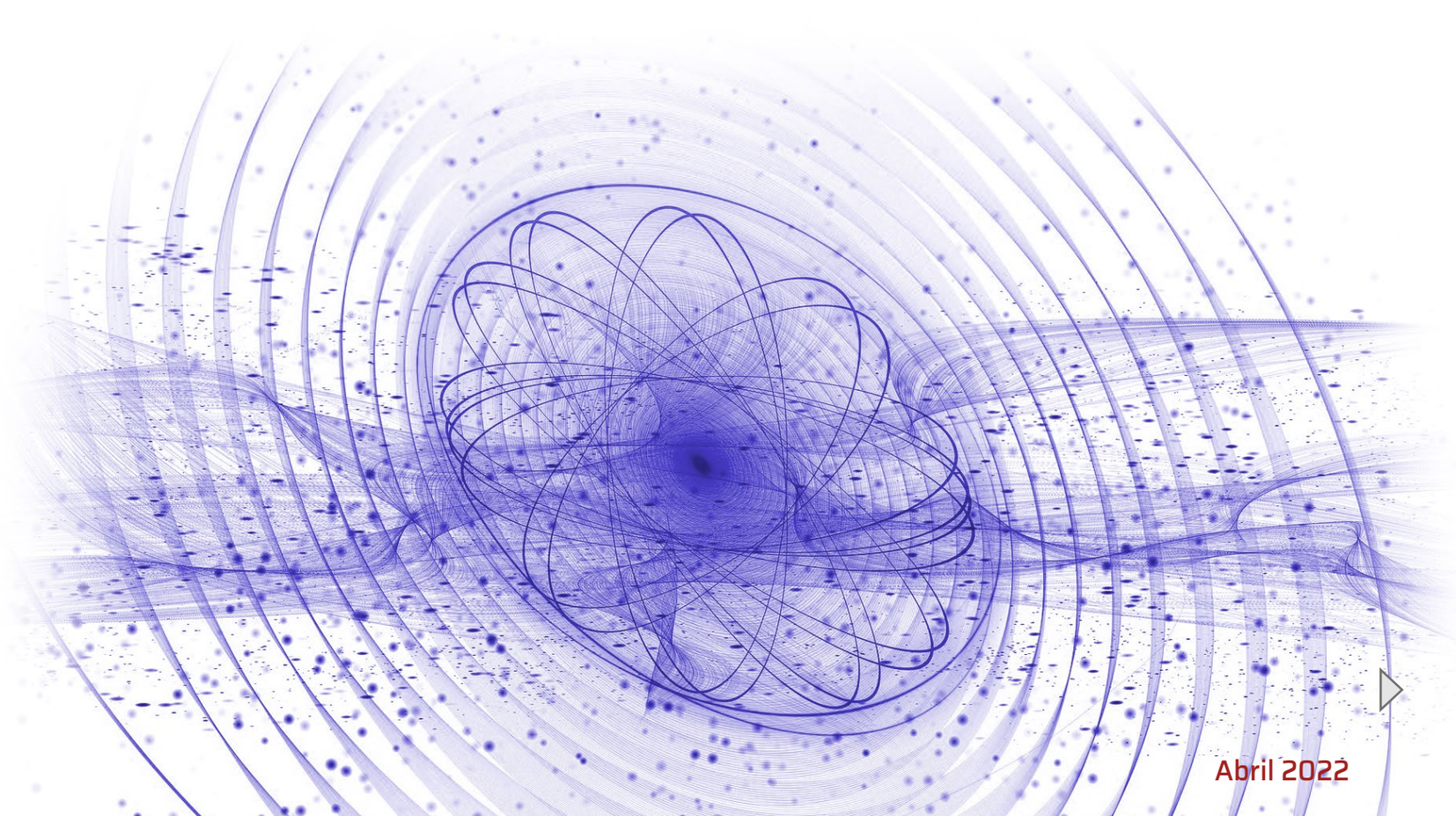
En septiembre de 2020 se compró, por 96 millones de dólares, Preempt Security, una compañía con una tecnología de protección de identidades que permite, entre otros, proteger el directorio activo, algo que para el directivo de Crowdstrike es “fundamental”. En junio de 2021 se pagaron 400 millones de dólares por Humio, que ayuda a correlar toda la volumetría masiva de datos que se genera y saber, en cuestión de milisegundos, si son ciberataques o no. Se trata de una tecnología que según Garijo “es diez veces más rápida que muchos SIEMs y con un coste muy eficiente”; además, la compañía acaba de anunciar que se amplía el periodo de retención de logs de siete o 90 días a 365, algo que “es una petición del mercado ya no solo por casuística y operación real, sino por temas legislativos”.

Asegurando que uno de los mayores problemas de las empresas es la exfiltración de datos interna, habla Juan Luis Garijo de la última compra de la compañía: Secure Circle, sobre la que asegura que es un Next Generation DLP que ya se ha añadido a la plataforma Falcon de la compañía. Una plataforma que destaca por tener un único agente, “el agente más ligero de todo el mercado”.

Cliente

Dice Juan Luis Garijo que, aunque históricamente se ha pensado en la solución de Crowdstrike sólo para grandísimas corporaciones, “el agente es tan ligero, tan fácil de utilizar y de instalar -que no hay

"La plataforma Falcon permite satisfacer cualquier caso de uso, pero principalmente destacaría la visibilidad, la ciberinteligencia y la parte de Threat Hunting"



ni que reiniciar el equipo, que hemos lanzado servicios gestionados, de MSSP, con ciertos partners para que cualquier usuario de cualquier parte del mundo pueda utilizar Crowdstrike en su dispositivo personal".

De hecho, la compañía trabaja también en un proyecto de Kit Digital asociado a los fondos europeos por el que muchos integradores van a incluir a tecnología de la compañía "para dar servicio a pymes desde 1 a 10 empleados, desde 10 a 49, que es como ha empezado ahora la fase uno del proyecto que digital de la Unión Europea. Y vamos a dar servicio gestionado a compañías de cualquier índole y de cualquier entorno", tanto del sector privado como del sector público, incluidos el educativo o el sanitario.

"No podemos dejar de dotar de seguridad a cualquier tipo de perfil de cliente", asegura Juan Luis Garijo.

Crowdstrike está creciendo de manera orgánica entre un 65% y un 70% año tras año, pero también se crece de manera inorgánica y en los últimos tres meses se han comprado tres empresas: Preempt Security, Humio y SecureCircle

Canal

Hace tiempo que el canal es de valor. Hace tiempo que dejaron de vender cajas para vender licencias y

Enlaces de interés...

- CrowdStrike amplía sus capacidades de detección y respuesta de su plataforma Falcon
- Crean una coalición para impulsar la detección y respuesta ante incidentes
- ¿Por qué es necesario innovar en prevención y remediación?

> Lo que habitualmente demanda el cliente como parte de un acuerdo "es tener acceso a la parte de telemetría, a la parte de servicio de Threat Hunting, que es OverWatch"

adentrarse en el mundo de los servicios. La llegada de los EDR al mundo de la seguridad enpoint ha añadido un reto: qué hacer con toda la información que generan este tipo de soluciones. Un reto que los clientes han trasladado a los partners, y los partners a los fabricantes, algunos de los cuales han desarrollado propuestas de MDR (Managed, Detection and Response).

En Crowdstrike es Julia Barruso la directora de canal y alianzas para el Sur de Europa, incluyendo Francia, Italia, España, Portugal, Israel, Grecia, Chipre y Malta. Además, no hace mucho que la compañía ha fichado a Lucas Rey como responsable de canal para España y Portugal, “y cada vez tenemos más partners que quieren ser afines a nuestra tecnología, porque resolvemos problemas reales de seguridad y muchos integradores que tiene con los mejores”.

Se ha trabajado en un modelo de canal Tier 1, hasta que hace un año se firmó un acuerdo de mayorista con Westcon “para poder tener más capilaridad y dar servicio a través de partners”, dice Juan Luis Garijo para añadir: “Queremos tener partners reales, partners de alianza, de confianza, especializados. Partners que realmente sean un wi-win”.

Compartir en RRSS

aruba
a Hewlett Packard
Enterprise company

LLEVE LA SEGURIDAD AL EDGE

Proteja su entorno de trabajo híbrido

La Seguridad en la nueva era de SD-WAN

Organiza: it Digital Security

Patrocina: aruba, a Hewlett Packard Enterprise company

Abril 2022

La Seguridad en la nueva era de SD-WAN

La desaparición del perímetro tradicional, la adopción de entornos híbridos y multi-cloud, el acceso a los recursos empresariales desde cualquier lugar y sin importar el momento o el dispositivo, está generando una convergencia creciente de la red y de la ciberseguridad. Además, el progresivo volumen de datos generados en el Edge, el extremo de la red, está abriendo nuevas oportunidades de negocio, pero también planteando importantes retos para los equipos de TI. Considerado como un elemento clave en cualquier proceso de transformación digital, SD-WAN mejora el rendimiento de las aplicaciones empresariales, optimizando la experiencia de usuario y simplificando las operaciones; todo ello de la mano de nuevos modelos de consumo como SaaS o NaaS.

Con el objetivo de analizar la situación a la que se enfrentan en este sentido los responsables de ciberseguridad de las empresas, entender en qué punto se encuentran de su transformación digital, y determinar los retos que afrontan y cómo pueden hacerles frente hemos reunido, con el patrocinio de Aruba, a un grupo de CISOs formado por: Fernando Cocaro, Senior Security Architect de Clariant Iberica; Carlos Asún, CISO de Food

ENCUENTROS ITDS
NUEVOS ENFOQUES PARA LA SEGURIDAD DE HOY

CLICAR PARA VER EL VÍDEO

Los cambios significativos en los patrones de tráfico y aplicaciones, incluido el incremento en el uso de servicios en la nube, impulsan la necesidad de SD-WAN

Delivery Brands; Ángel Uruñuela, CISO de Fluidra; Elena García Díez, CISO de Indra; e Iker del Fresno, Country Manager de Aruba, a Hewlett Packard Enterprise company.

El debate arranca con la bienvenida de Iker del Fresno, Country Manager de Aruba, una empresa especializada en redes y seguridad y cuyo enfoque se basa en utilizar la tecnología para mejorar la productividad de cada uno de sus clientes.

Durante el mismo, los participantes hablaron sobre los procesos de transformación digital que están acometiendo, así como de los principales retos que enfrentan en este sentido; la importancia -o no- que modelos como Zero Trust o SASE tienen para su organización; y sobre el proceso de implantación de SD-WAN en sus respectivas empresas, y la responsabilidad que sobre esto comparten los departamentos de redes y seguridad.

it whitepapers

EL ESTADO DE LAS ARQUITECTURAS ZERO TRUST, SD-WAN Y SASE

Esta infografía resume un informe de Ponemon sobre la adopción de SD-WAN asegurando que las mejores capacidades de SD-WAN combinadas con los mejores proveedores de seguridad en la nube son una forma sencilla y eficaz de incorporar servicios de seguridad basados en la nube a la infraestructura de red y seguridad existente.

LA VISIÓN DE LAS EMPRESAS

"Zero Trust y SASE son nombres nuevos para controles no tan nuevos, que siguen siendo los mismos, pero aplicados de una forma particular en algunos casos"

Fernando Cócaro, Clariant Iberica

Fernando Cócaro, Senior Security Architect, CLARIANT IBERICA

"La migración a la nube es nuestra máxima prioridad y, por ende, nuestro reto tecnológico principal en estos momentos", reconoce, Fernando Cocaro, Senior Security Architect, Clariant Iberica. "Si no somos la primera empresa química, estamos cerca de serlo, en integrar todo el sistema de TI en global, en la nube". A este respecto explica, están trabajando para que las operaciones de la empresa pasen de Data Center a Cloud del modo más transparente posible, tanto desde el punto de vista de continuidad de negocio como del de la seguridad efectiva. "También estamos analizando los conceptos de Zero Trust, pero nuestro foco principal es asegurar la continuidad de negocio y de las operaciones en esta migración a Cloud".

Sobre la importancia que realidades como Zero Trust o SASE juegan para su empresa, Fernando Cocaro coincide con la idea ya planteada de que se trata de nombres nuevos para controles no tan nuevos, "que siguen siendo los mismos, pero aplicados de una forma particular en algún caso". No obstante, reconoce que afrontan un proyecto de adecuación a Zero Trust que busca entender cuál es la realidad del negocio y ajustarla, desde el punto de vista de la seguridad, para mejorar la postura de la empresa. "Tratamos de responder a esta pregunta: ¿vamos a estar bien defendidos más allá de Zero Trust cuando nos ataquen? Tenemos que aceptar que el ataque va a suceder, y que cuando ocurra, el tiempo necesario para responder a ese ataque va a ser el mínimo necesario. Y a eso es a lo que estamos apuntando para generar nuestro modelo. Más allá de integrar una herramienta que asegure que ya somos Zero Trust Compliance, nuestro enfoque es más estructurado, desde el punto de vista de la gestión del riesgo, la implementación de controles y la mejora de la visibilidad".

Con SD-WAN implementada desde hace tiempo, no hay muchos retos específicos más allá de los derivados por un tema de distancia, latencias o similar, reconoce Fernando Cocaro. No ocurre lo mismo a nivel general, donde el mayor reto supone afrontar el día a día, una responsabilidad, no obstante, compartida entre el departamento de seguridad y el de redes. "Seguimos una estrategia corporativa de segregación de funciones, por lo que cualquier cambio a efectuar por redes pasa por seguridad, y los acometidos por seguridad los implementa redes". También es cierto que, más allá de SD-WAN, "toda la red de la empresa se maneja desde el punto de vista de la seguridad operacional".

Ángel Uruñuela, CISO,
FLUIDRA

Empresa especializada en el sector piscinas y con presencia mundial, Fluidra ha emprendido un proceso de transformación digital que abarca tanto el componente tecnológico como la seguridad y las comunicaciones. “Un reto muy importante para nosotros es lo relacionado con Identity-First Security, donde estamos embarcados ahora mismo e invirtiendo muchos recursos”.

Bajo su punto de vista, el concepto de SD-WAN donde se integraban todas las sedes hiper conectadas y bajo una WAN se está difuminando con la adopción progresiva de servicios en la nube y el teletrabajo. En muchos casos, lo que se busca es romper la red, no unirla, por un tema de seguridad, de impacto y de contención en caso de incidente. “SD-WAN, como lo entendíamos hace una década, está herido. Hay que empezar a hablar de SASE SD-WAN, y ver cómo evoluciona en los próximos años”.

En lo que respecta a SASE y pese a ser un concepto muy completo, Uruñuela reconoce que es complicada su implementación, no tanto para una pequeña empresa, pero si para una gran organización, con miles y miles de empleados y activos, ya que requiere de una gran inversión, en tiempo y dinero, y de una importante gestión del cambio. “SASE, como enfoque, como concepto, es algo bonito, alineado con la nueva noción de Cybersecurity Mesh, pero a los vendors les falta mucho para llegar ahí. Vemos muchas integraciones, todo es SASE, pero realmente cuando rascas detrás del logotipo, las integraciones son débiles, no te dan ese Mesh y no te facilitan ir a un modelo Zero Trust o SASE”.

Fluidra está afrontando un proceso de transformación de su red liderado por el área de Ciberseguridad, pero ejecutado desde IT. En este caso, y aunque son dos equipos diferentes, están trabajando conjuntamente para conseguir el objetivo común.

En este proceso de transformación, y en cualquier otro, Ángel Uruñuela pediría a los fabricantes, algo que los profesionales de la ciberseguridad llevan años reclamando, una integración real. “Tenemos muchísima tecnología, diversos productos, pero entre ellos no se hablan”. Por eso, y aunque “podemos hacer integraciones con APIs, necesitamos productos y tecnologías que se integren, y que lo hagan en un ecosistema como el actual, de rápida evolución”.

Para concluir, este responsable se muestra convencido de que poner diferentes nombres a cosas que ya existen -como decía Elena García de Indra- no es la solución. La seguridad comienza a ser entendida, los riesgos son más visibles, pero, en general, queda por avanzar. “Aunque contamos con mucha más tecnología de seguridad, tenemos más incidentes que nunca y no parece que estemos ganando la batalla”.

Carlos Asún, CISO,
FOOD DELIVERY BRANDS

"SD-WAN nos da facilidad, rapidez, centralización y una capa de seguridad (aunque no tengamos SASE) de la que no disponíamos antes"

Carlos Asún, Food Delivery Brands

Food Delivery Brands, grupo multimarca especializado en pizza delivery, afronta una profunda transformación digital en la que la seguridad es, según Carlos Asún, una parte crucial a todos los niveles, tanto de los sistemas críticos (e-commerce) como no críticos. Además, el hecho de que bajo la denominación comercial se integren oficinas, tiendas y fábricas traslada la seguridad hasta una doble dimensión: IT y OT. "También estamos en proceso de migrar todo al cloud, algo complicado pues contamos con múltiples sistemas, proveedores y elementos legacy que es necesario actualizar". Otros retos a los que hacer frente tienen que ver con los terceros con quienes interactúan en estos procesos de transformación digital: "los fabricantres y sus partners deben entender nuestras necesidades y ser capaces de cooperar con otros proveedores", y con la tecnología escogida para conformar su capa de seguridad, y que deben cumplir "tanto nuestras políticas internas como los niveles de riesgos aceptables en los análisis de riesgos que realizamos".

Zero Trust y SASE están muy ligados a SD-WAN, pero mientras que Zero Trust puede considerarse el Santo Grial, SASE: un "marco muy importante si realmente queremos contar con una SD-WAN robusta y eficiente", es más complicado de implantar por todo lo que abarca. Por eso, "los fabricantes tienen que trabajarlo y desarrollarlo aún más, para hacerlo más modular y que las empresas puedan escoger las opciones que realmente necesitan. Esto nos permitirá ser más eficientes y que la continuidad de negocio y operaciones vaya acorde".

Con SD-WAN implementado en cada vez más sedes, entre oficinas, fábricas y tiendas repartidas principalmente por Europa y Latam, Carlos Asún reconoce que es una tecnología que funciona. "Estamos haciendo una implementación a nivel global de SD-WAN porque nos da facilidad, rapidez, centralización y una capa de seguridad (aunque no tengamos SASE) de la que antes no disponíamos. También, el poder desplegarlo en cualquier tipo de entorno, utilizando la misma tecnología, métricas y políticas ha sido esencial. Las empresas que no tengan SD-WAN deberían analizarlo".

En lo que respecta a los departamentos que lo gestionan, Carlos Asún explica que es una responsabilidad compartida entre seguridad, redes, negocio y operaciones, además de IT y OT. "Es importante estar muy bien alineados, porque, al menos en nuestro caso, es un proyecto que impacta en casi todas las áreas de la empresa, especialmente en las ligadas al negocio". También les ha ayudado con los franquiciados, quienes demandan un ahorro de costes y una transparencia importantes. Por todo ello, "SD-WAN (no SASE) es fundamental para nosotros. Está siendo muy bonita esta transformación de la parte de MPLS a SD-WAN".

Elena García Díez, CISO,
INDRA

Como gran tecnológica y proveedor de servicios y soluciones tanto para TI como para el mundo del transporte y de la defensa, Indra afronta un proceso de transformación digital continuo. “Vivimos transformando; a nuestros clientes y a nosotros mismos”, afirma Elena García Díez. Por eso, y desde una perspectiva conservadora y cortoplacista, la WAN de Indra está llamada a evolucionar y a flexibilizarse, sobre todo por la alta dispersión de su fuerza laboral.

Coincidiendo con lo apuntado por Iker del Fresno esta responsable explica que, para una gestión efectiva de la WAN, es necesario mantener cierta visión, seguridad y determinados instrumentos comunes. “Estamos en transformación continua”, recuerda. Por eso, “todo el ecosistema SASE y la arquitectura SD-WAN que pueda venir, orquestada en un click, es la tecnología que necesitamos; preparada para la nube, pero también para conservar cierta inteligencia en el CPD. SD-WAN nos va a aportar esa infraestructura flexible donde mantener los niveles de riesgo y aprovechar cualquier oportunidad de este entorno, también más deslocalizado”.

Sobre el grado de integración en su empresa de tecnologías como Zero Trust o SASE, explica que estos términos junto con Zero Touch o SD-WAN no dejan de ser nombres –acuñados por las consultoras- para definir planteamientos en los que, en seguridad, se lleva tiempo trabajando. Por tanto, las empresas no tienen por qué lanzarse a integrar estas disciplinas porque se hable de ellas, sino que cualquier proyecto de transformación o evolución en la gestión de la seguridad debe atender a las propias necesidades, a las prioridades del negocio y al nivel de madurez del mismo. “Hay que dejar evolucionar la WAN y mantener los servicios de seguridad existentes para que, según vayan cambiando los controles técnicos, decidir si es mejor estrategia llevarlos arriba (nube), dejarlos o utilizar un híbrido”.

Y en esta evolución tecnológica de la arquitectura de las empresas, “la SD-WAN podrá subsistir, siempre que aporte lo que no ofrecía la WAN, esa orquestación en un click y esa WAN flexible, polivalente y cambiante que no es necesario modificar para poder ir añadiendo las piezas y los hilos que necesitamos en cada momento”.

Al respecto de los retos que la adopción de SD-WAN pueda estar generando a su empresa, Elena García destaca que no hay retos específicos en su implantación: cambia el perímetro de exposición, la relación con un determinado proveedor… “El reto es abordarlo con naturalidad y hacerlo manteniendo el nivel de riesgo y la manera de gestionar la seguridad que subsiste en cualquier organización”.

"SD-WAN podrá subsistir siempre que aporte lo que no ofrecía la WAN, orquestación en un click y esa WAN flexible, polivalente y cambiante que no es necesario modificar"

Elena García Díez, Indra

LA VISIÓN DE LA INDUSTRIA IT

Iker del Fresno, Country Manager de Aruba,
UNA COMPAÑÍA DE HPE

"Concebimos la seguridad de nuestros clientes como una heterogeneidad y SD-WAN es la base para poder aportar valor"

Iker del Fresno, Aruba

Iker del Fresno, Country Manager de Aruba, define SD-WAN como "el nuevo backbone inteligente de interconexión", al que es necesario proteger desde el extremo hasta la nube, con una oferta integrada (Zero Trust, SD-WAN y de Cloud Delivered Security Services) y una orquestación de todo en uno a través de lo que recientemente ha bautizado Gartner como Security Service Edge (SSE). Con esta oferta tecnológica integrada, Aruba pretende optimizar la experiencia del usuario, desde el punto de vista del ahorro de costes y de tiempo, ofreciéndole además la flexibilidad y la agilidad necesarias para adaptarse a la transición a la nube. Y, por supuesto, tener la visibilidad, el control de la WAN y una gestión centralizada, además de automatización (Zero Touch Provisioning) y escalabilidad.

A colación de lo comentado por los distintos participantes sobre el momento actual de SD-WAN, Iker del Fresno coincide con la necesidad de esa perspectiva de cambio y, sin usar la palabra transformación, expone como los modelos SD-WAN tienen que tender hacia una flexibilización del entorno y hacia una orquestación del mismo porque al final se trata de entornos absolutamente híbridos, distintos para cada empresa. Por eso es importante flexibilizar todo esto, "como hacemos en Aruba". Aunque todo tiende al cloud, con proyectos de data centers que migran a cloud (utilizando SD-WAN) hay que ser capaz también de acercar el cloud al on premise si fuese necesario. Orquestar determinados entornos o tener visibilidad también del Edge.

Sobre la dificultad para que términos como Zero Trust o SASE calen en los idearios de las empresas, Iker del Fresno resalta que, pese a todo, se ha avanzado mucho con respecto a hace 15- 20 años, cuando lo que funcionaba con un determinado usuario no tenía por qué hacerlo con otro. "Es cierto que se han renombrado determinados protocolos para llevarlos a cabo, pero también se les ha dotado de cierto halo de simplicidad, porque si no sería imposible desarrollarlos". No obstante, las empresas tienen que saber cuál es su trascendencia. No pueden embarcarse en un proyecto de Zero Trust compliance sin saber cuál será su alcance efectivo. "Y aquí es clave la labor tanto del vendor y del partner, que tienen que entender al cliente, como de éste, que debe tener claro hasta dónde puede llegar con la tecnología. Tampoco deben sentirse empujados a llevar a cabo ciertos proyectos de adecuación hacia la seguridad, de SASE o SSE, por la propia presión de vendedor, del mercado o por la situación general".

Los fabricantes tienen que adecuarse también a este proceso de transformación, trabajar para no intentar imponer el "all in one" (todo conmigo y todo a la vez) ser más flexibles y ser capaces de integrarse en todo lo que hay. "El 'all in one' no va a funcionar".

Como reflexión final, y ante la importancia que durante el debate se ha dado a elementos como “integración”, “orquestación” o “simplicidad”, Iker del Fresno ha querido dejar claro que para una empresa como Aruba estos factores son claves. “Concebimos la seguridad de nuestros clientes como una heterogeneidad y esta es la base para poder aportar valor”.

Orquestar es esencial también, y hacerlo con un solo click, aumentará el valor de las soluciones que ya tiene el cliente. En este sentido, es primordial integrar el concepto Zero Trust, la capa de SD-WAN, SASE y llevarlo a Cloud Security, orquestándolo de manera unificada. Dar este valor y esa flexibilidad va a ser fundamental ahora y en los próximos años para conseguir esa mejora continua y esa adaptación a los nuevos riesgos que lleva implícita la oficina distribuida.

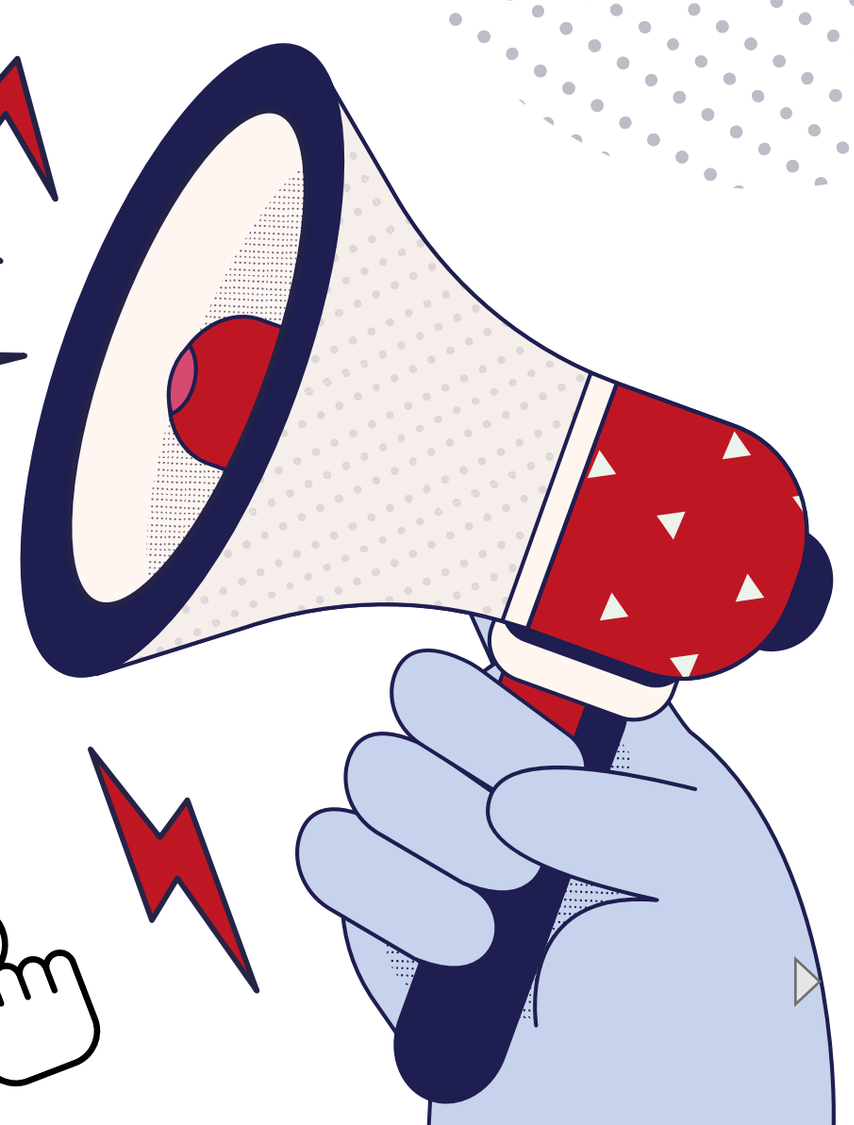
“El Edge to Cloud Security básicamente se basa en entender que los riesgos son compartidos, que existe una base instalada y que debemos adaptarnos a lo que ya tenemos para aportar un valor adicional, siempre que orquestemos y nos integramos con un one click”, concluye. it

Administración Pública Digital

NUEVA WEB

¡VISÍTANOS!

www.administracionpublicadigital.es



it Digital Security

Desayuno ITDS

Protección de aplicaciones web y APIs en el mundo cloud

Recientemente acuñado por Gartner, el termino Web Application and API Protection (WAAP) engloba una oferta de servicios basados en la nube y organizados bajo un único paraguas: mitigación de bots, WAF, protección de APIs y seguridad contra DDoS, lo hacen imprescindible. Repasemos el camino hasta llegar a él.

Desayuno ITDS

En un mercado cada vez más conectado y basado en la nube y en los servicios proteger las aplicaciones y APIs frente a amenazas y fraudes es, sin duda, prioritario, así como garantizar la disponibilidad y el cumplimiento.

Convertidas en un blanco objetivo para los ciberdelincuentes, Gartner ha acuñado el término Web Application and API Protection (WAAP) para describir los servicios diseñados para protegerlas. Para conocer si este vocablo tiene sentido, comprender cuáles son los principales retos a la hora de salvaguardar aplicaciones web y APIs, la evolución de los WAF o cómo han impactado la nube, los modelos as-a-service, el desarrollo ágil o los contenedores en su seguridad, nos acompañan en este #DesayunosITDS Daniel Howe, Senior Sales Engineer de Fastly; Nuno Silveiro, Principal Sales Specialist de Citrix Iberia; Francisco Lahoz, Ingeniero Preventa de F5 Networks; José Juan Díaz, Iberia Senior SE de Barracuda; y Eusebio Nieva, Director Técnico de Check Point. Especialistas en este terreno, estos participantes hablarán también acerca de las principales amenazas y darán a conocer las propuestas tecnológicas de sus respectivas empresas para contrarrestarlas.

Principales retos

Para Eusebio Nieva el principal reto surge por un cambio de escenario, hacia la nube, en el que todos los servicios son muy distribuidos. Hay un protocolo ubicuo, HTTP, que es el que permite hacer una entrega de esos servicios. Asimismo, se están multiplicando las APIs utilizadas para interconectar los servicios de manera interna y el número de interacciones entre los diferentes servicios o micro servicios ha crecido rápidamente. “Es necesario adoptar medidas específicamente diseñadas para atajar esta problemática”.

En la misma línea, José Juan Díaz reconoce que el paso hacia la nube ha derivado en la obligación de conocer todos los servicios existentes, proteger el tráfico este-oeste y, según el tipo de aplicaciones, definir una estrategia de microsegmentación o de zero trust, si las apps se comparten a nivel interno. “La mayoría de los ataques son automatizados y muchos van contra la cadena de suministro; hay que proteger tanto la aplicación como lo que se ejecuta en el equipo del usuario. Esto

añade una capa de complejidad que no existía hasta hoy".

Según Francisco Lahoz, desde la aparición hace unos años del desarrollo basado en micro servicios, la seguridad ya no se focaliza únicamente en la aplicación o en la API. La seguridad tiene que ser flexible, ágil y llegar a las nuevas aplicaciones dinámicas, cambiantes y muy distribuidas. "Las compañías que nos focalizamos en la seguridad, tenemos que ser capaces de seguir el ritmo que imponen los desarrolladores, aquellos que entregan las aplicaciones que corren en los negocios de las compañías".

"Las aplicaciones han cambiado, los entornos se han descentralizado por lo que su exposición a los elementos externos es mucho mayor", asegura Nuno Silveiro. Sin embargo, ese cambio no ha venido acompañado de mayores recursos para mejorar su seguridad, por lo que la tecnología debe ayudar en ese sentido. Las aplicaciones web son uno de los principales vectores de ataque. Por ello, las organizaciones se enfrentan al reto de proteger su perímetro, mientras mantienen la agilidad y la seguridad del dato en todo momento.

El mundo distribuido ha cambiado, está en un entorno cloud, en aplicativos, en diferentes regiones, en distintos sitios y con un mismo requisito: la disponibilidad de la plataforma. "Flexibilidad y agilidad son claves", explica Daniel Howe. Y con los micro servicios ocurre algo similar; están desplegados por todos los sitios. "Es necesaria una flexibilidad y una agilidad para llegar a ellos y garantizar que estos sistemas estén siempre disponibles para todos los usuarios".

#DESAYUNOSITDS. PROTEGIENDO APPS Y APIS

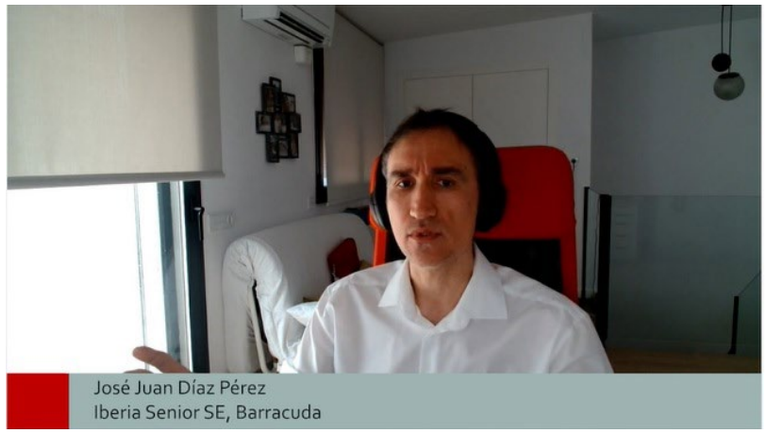
CLICAR PARA VER EL VÍDEO

Los WAF tradicionales ya no son suficientes

Aunque hace años que convivimos con los Web Application Firewall (WAF), es importante conocer cuál ha sido su evolución y en qué situación se encuentra, en estos momentos, está tecnología.

Sobre su papel actual, José Juan Díaz afirma que, tal y como especifica Gartner, los servicios WAF conocidos no son suficientes para proteger las actuales aplicaciones web. "Las propias aplicaciones de los usuarios son APIs que permiten conectarse B2B con el cliente y también directamente, son aplicaciones móviles. Por ello, los WAF deben tener servicios DDoS y capacidades de protección API y del lado cliente y, sobre todo, proteger contra bots, principal vector de ataque.

Para Francisco Lahoz esta progresión viene marcada por dos aspectos: la evolución de WAF



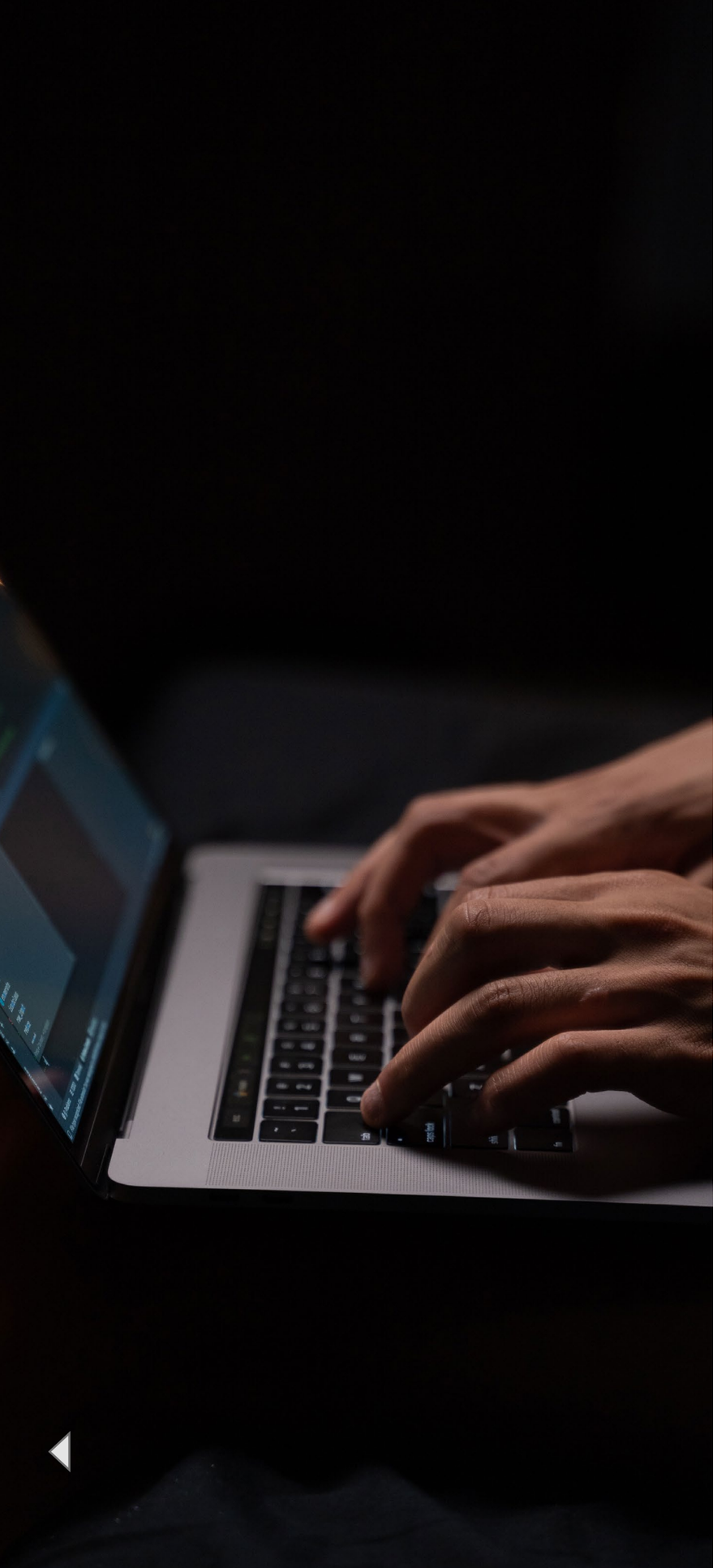
"La mayoría de los ataques son automatizados y muchos van contra la cadena de suministro; hay que proteger tanto la aplicación como lo que se ejecuta en el equipo del usuario. Esto añade una capa de complejidad que no existía hasta hoy".

José Juan Díaz, Iberia Senior SE de Barracuda

en cuanto a funcionalidades y por el despliegue. En el primero, y por la naturaleza cambiante de las aplicaciones, hablamos de una solución más ágil en cuanto a funcionalidades y un aprendizaje más inteligente, mientras que, en el segundo, y por la diversidad de sitios en los que puede residir una aplicación, se tiende a adquirir soluciones WAF o WAAP como servicios globales, para un despliegue próximo a la aplicación.

Las aplicaciones han evolucionado muchísimo en los últimos años y, en consecuencia, el WAF ha tenido que adaptarse; “ahora hablamos también de WAAP”, puntualiza Nuno Silveiro. La inteligencia artificial y el machine learning han cambiado el modo en que el WAF percibe las amenazas y protege las aplicaciones en un entorno cada vez más distribuido; como un paraguas único e independientemente del formato, arquitectura, ubicación y de donde provengan las peticiones a esas aplicaciones.

Para Daniel Howe, la evolución es adaptarse a lo que los clientes demandan: la flexibilidad para



itds

Desayuno ITDS

"La inteligencia artificial y el machine learning han cambiado el modo en que el WAF percibe las amenazas y protege las aplicaciones en un entorno cada vez más distribuido; como un paraguas único e independientemente del formato, arquitectura, ubicación y de donde provengan las peticiones a esas aplicaciones".

Nuno Silveiro, Principal Sales Specialist de Citrix Iberia

securizar APIs o aplicaciones web, en cualquier entorno o llegar a aquellos puntos donde las APIs se están implementando, incluso dentro de la empresa. "Se trata de representar esa visibilidad de correlación de uso y de aplicativo para descartar fallos en el sistema de la cadena de comunicación entre los micro servicios, y verificar que todo se está correlacionando de un modo correcto. Eso hace que obtengas una plataforma de observabilidad del negocio".

Eusebio Nieva considera que, hoy por hoy, los WAF deberían ser casi completamente autónomos, para minimizar la intervención de los CISOs. También, deberían adaptarse a los ataques actuales, y gracias a la inteligencia y al aprendizaje automático, facilitar que las decisiones de seguridad se adecuen a los cambios de la aplicación web y a los nuevos usos que se hagan de esa aplicación y esas APIs que interconectan los diferentes servicios. "El WAF, no obstante, no es la única solución. Hay que poner otras barreras".

Cerrando esta ronda, y ante la pregunta de si a la luz de todos estos cambios, podría empezarse a hablar de un Next Generation WAF, Daniel Howe reconoce que, en su empresa, trabajan con el suyo

propio, y este aporta un nuevo enfoque basado en las necesidades y en los retos actuales. “La seguridad no puede ser entendida como un elemento ajeno, hay que integrarla en un entorno DevOps para garantizar que las alertas llegan a los equipos y que las APIs están disponibles, para que las actualizaciones se realicen del modo más automatizado posible y no tener equipos destinados a analizar logs continuamente”.

"La seguridad no puede ser entendida como un elemento ajeno, hay que integrarla en un entorno DevOps para garantizar que las alertas llegan a los equipos, que las APIs están disponibles, para que las actualizaciones se realicen del modo más automatizado posible y no tener equipos destinados a analizar logs continuamente".

Daniel Howe, Senior Sales Engineer de Fastly

Elementos externos

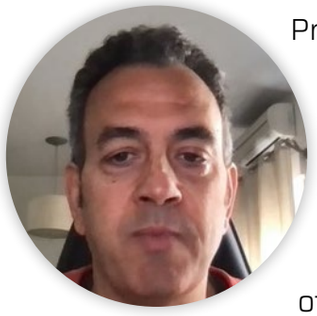
¿Cómo ha impactado el cloud, los modelos as-a-service, el desarrollo ágil, los contenedores… en la protección de aplicaciones y APIs? ¿Han sido capaces las empresas de adaptar esta evolución tecnológica para proteger adecuadamente las aplicaciones y las APIs?

Francisco Lahoz reconoce que el impacto de esta diversidad de entornos heterogéneo es distinto, según el tipo de compañía. En aquellas que consiguen operar como un modelo departamental único y ágil, el concepto de cloud DevSecOps puede ser exitoso, pero si funcionan como silos, puede haber problemas a la hora de adaptarlos. “Por eso, los fabricantes ofrecemos soluciones cada vez más ágiles e integradas, que satisfagan las distintas demandas y que protejan a una empresa cuando sus aplicaciones queden expuestas al mundo salvaje”.

Daniel Howe resalta la importancia de la flexibilidad para poder adaptarse a todos los cambios durante el proceso de vida de las APIs, y que todas las mejoras que ha ofrecido la evolución del WAAP, puedan ser aplicadas para garantizar su

Propuestas tecnológicas

¿Qué propuestas o tecnologías son las más adecuadas para proteger APIs y aplicaciones?



Presente en el mundo CDN desde hace 10 años, y con alcance mundial, la adquisición de Signal Sallent permitió a Fastly acercarse a las integraciones de DevOps, para ofrecer soluciones integrales de seguridad edge. Además de proteger APIs y aplicaciones web, Fastly ofrece soluciones de mitigación DDoS, protección contra bots y cifrado TLS. “Trabajamos para mejorar y garantizar que la plataforma y la infraestructura de nuestros clientes está dedicada al servicio que ofrecen y no al abuso de otros que la puedan estar utilizando”, afirma **Daniel Howe.**

Check Point proporciona un producto, integrado en CloudGuard, que además de las capacidades propias de seguridad de la plataforma, ofrece funcionalidades específicas para APIs y aplicaciones web basadas, sobre todo, en la simplificación y automatización de la seguridad. “Para algunos clientes era imposible implementar un WAF por su complejidad. Check Point pone un punto de control en el cual estos clientes colocan su seguridad y prácticamente se olvidan”, manifiesta **Eusebio Nieva.**

La propuesta de Barracuda es una evolución de su oferta WAF. Basándose en la sencillez y adaptabilidad, su plataforma suma capacidades de contenerización (as-a-service) y aprovecha el machine learning para la monitorización automática, la corrección de vulnerabilidades y la protección avanzada contra amenazas. “Buscamos adaptarnos -del modo más automático posible- a las necesidades de nuestros clientes y a las vulnerabilidades que puedan surgir”, asevera **José Juan Díaz.**

La evolución de F5 como protección al mundo WAAP se basa en cuatro pilares: un motor WAF con capacidades de detección de falsos positivos y mitigación; un pilar muy potente de DDoS orientado a la capa 7; un motor bot para distinguir acciones o malos comportamientos; y una capacidad de protección de APIs que permite aplicar las políticas necesarias de seguridad.

“Y todo ello, sin importar el entorno y con la capacidad de automatizar el despliegue y las configuraciones de seguridad donde se origine el mismo”, explica **Francisco Lahoz.**

Para proteger aplicaciones y APIs, Citrix intengra en una capa común, la inteligencia, trazabilidad, lógica de inteligencia artificial y machine learning de su solución WAF, con dos modos de consumo, uno cercano a la aplicación y otro a la nube. “Esta plataforma provee visibilidad holística y control, para que desde un único punto se puedan aplicar las reglas y la inteligencia y el aprendizaje, independientemente de la ubicación, el directorio de aplicación o el formato aplicado en las comunicaciones”, concluye **Nuno Silveiro.**

disponibilidad. “Con WAAP no solo se protege del tráfico malicioso, de bots o de cualquier top ten OWASP, también se puede ayudar a los equipos de desarrollo para que puedan ser conocedores de pequeños fallos o versionados que se estén quedando obsoletos y que no hayan sido integrados en las necesidades del negocio”.

Nuno Silveiro observa que el desarrollo de servicios y contenedores ha incrementado el riesgo de errores. Por eso, es importante comprender lo que está detrás, con una solución que permita identificar esos problemas, entender las vulnerabilidades y protegerlas. “Ya no hablamos de nube híbrida, hablamos de multi nubes y multi entorno. Esa monitorización y conocimiento de lo que está ocurriendo

detrás de las aplicaciones web y las API, va a ayudar a proteger las aplicaciones que están en desarrollo y las que están publicadas".

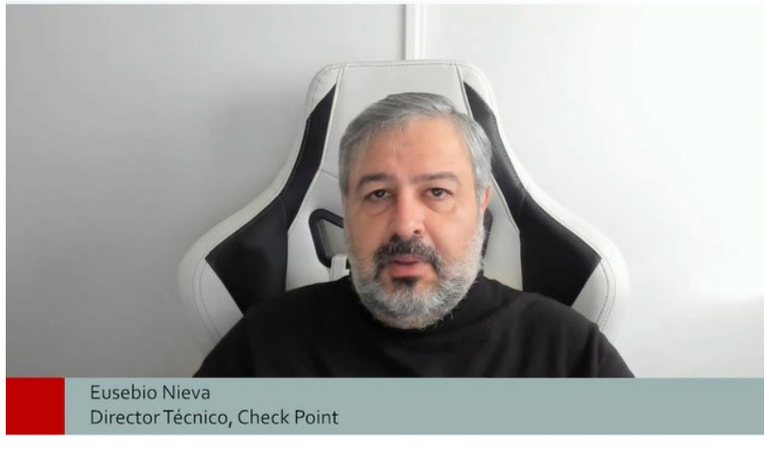
Al respecto de cómo están afrontando las empresas esa protección de aplicaciones, Eusebio Nieva comenta que existe una tendencia a integrar la seguridad directamente en DevOps, para mitigar riesgos y proteger antes de que se produzcan daños, insertando la seguridad en cada uno de los componentes. Se trata de tener una arquitectura de seguridad totalmente automatizada. "La seguridad en la nube puede ser muy compleja de gestionar, requiere muchos puntos de control. Pero también, y eso es lo fundamental, se puede automatizar, con lo cual vamos a tener esa ventaja".

En la misma línea, José Juan Díaz destaca la automatización y sugiere que los clientes migran a la nube por dos motivos, para tornar la infraestructura en código, convertir DevOps en DevSecOps y disponer de más servicios con menos infraestructura, o para transformar la seguridad en un servicio, por no disponer de la inteligencia o de las capacidades para poder administrar este tipo de soluciones. "Este cambio hacia el machine learning permite asegurar

Francisco Lahoz
Ingeniero preventa, F5

"Los fabricantes ofrecemos soluciones cada vez más ágiles e integradas, que satisfacen las distintas demandas y que protegen a una empresa cuando sus aplicaciones queden expuestas al mundo salvaje".

Francisco Lahoz,
Ingeniero Preventa de F5 Networks



"WAAP viene a evidenciar una situación nueva en la cual los servicios de la nube o web se consumen de dos modos: a través del método tradicional, HTTP puro, o como arquitectura para el diseño de servicios (API First). "Hay que proteger ambos métodos de acceso a los servicios de una compañía. Eso es lo que refleja el término de Gartner".

Eusebio Nieva, Director Técnico de Check Point

de forma automática este tipo de entornos y tener una monitorización de lo que está sucediendo".

Un concepto nuevo, pero no novedoso

WAAP, un concepto acuñado por Gartner, está de actualidad. Conozcamos ¿qué viene a solucionar y por qué se ha vuelto fundamental en la protección de estas aplicaciones?

Gartner ha tomado un término del que ya se hablaba y lo ha democratizado, convirtiéndolo en una tendencia que los fabricantes ya habíamos detectado, señala Nuno Silveiro. "Esta tecnología puede ayudar a que más empresas, también pymes, respondan mejor a los retos a los que se enfrentan las aplicaciones. Es necesario actualizar la infraestructura de seguridad en base a los retos antes comentados".

Para Daniel Howe era cuestión de tiempo que se crease y adaptase un término que completa la protección de los aplicativos webs, "ya que ahora hay

muchas APIS que proteger. Hay que incluir todos los elementos dentro de la ecuación para que el cliente tenga una buena percepción del aplicativo, pueda realizar sus transacciones con seguridad e integrar estos elementos en DevOps para no crear más infraestructura".

WAAP viene a evidenciar, según Eusebio Nieva, una situación nueva en la cual los servicios de la nube o web se consumen de dos modos: a través del método tradicional, HTTP puro, o como arquitectura para el diseño de servicios (API First). "Hay que proteger ambos métodos de acceso a los servicios de una compañía. Eso es lo que refleja el término de Gartner".

En línea con lo comentado, José Juan Díaz, añade que, tanto las aplicaciones web como las APIs se han convertido en el estándar de comunicación entre las empresas y entre estas con sus clientes y sus proveedores. "Son API First, por lo tanto, si no existen estas capacidades de detección y de control no va a ser posible proteger las aplicaciones de los propios clientes·.

Por último, Francisco Lahoz señala que WAAP es el cambio natural de lo que se ve y de lo que las organizaciones demandan. "Es la evolución natural del nombre de una tecnología destinada a proteger los frontales, la autopista que publica las aplicaciones y el uso que se hace de ellas".

Enlaces de interés...

- Nuevas reglas de seguridad para aplicaciones web y API
- La expansión descontrolada de las API supone una posible brecha de seguridad
- Dos tercios de los incidentes en cloud se generan por API configuradas incorrectamente

Compartir en RRSS

FORO it Digital Security

SASE

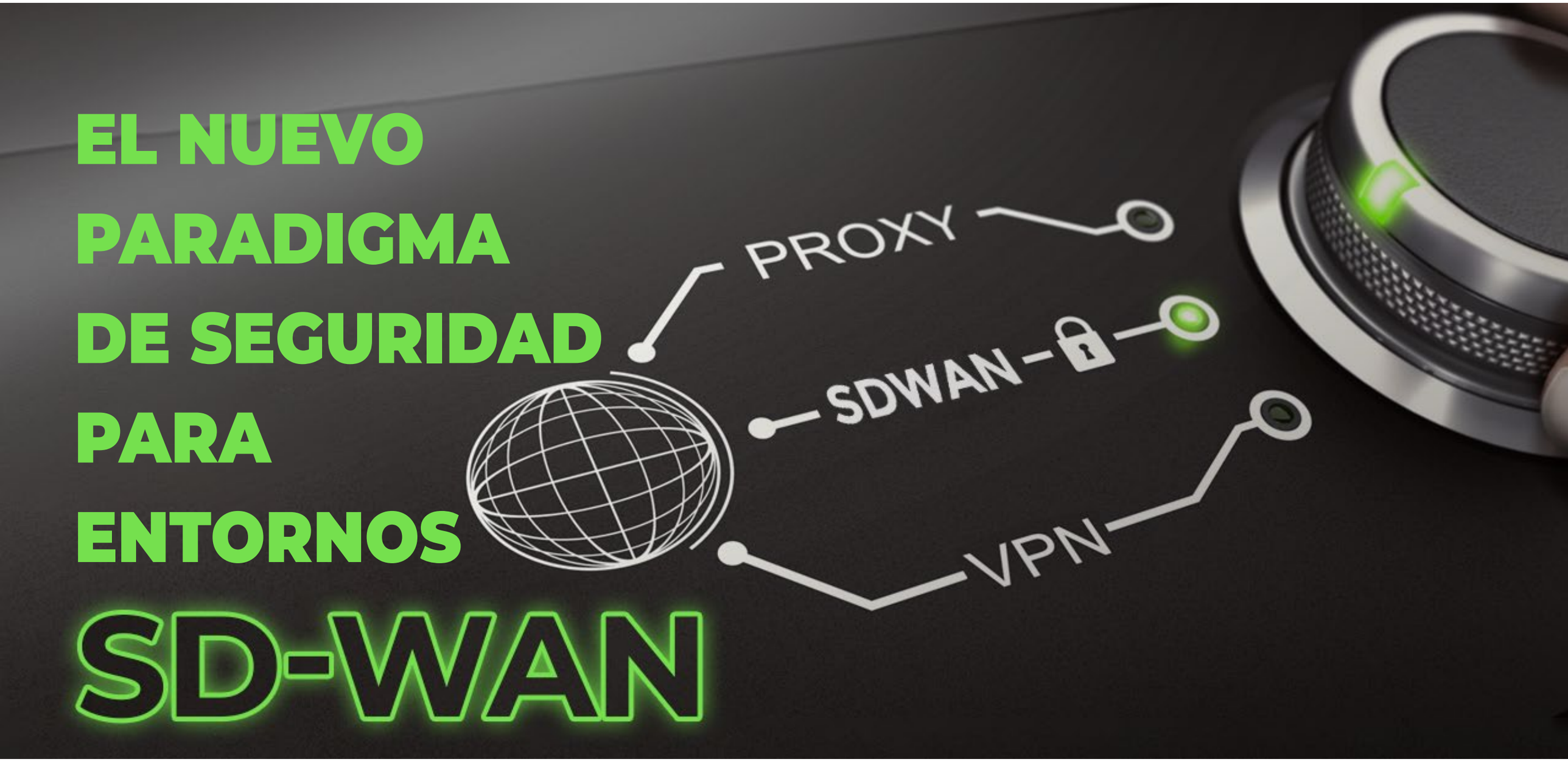
EL FUTURO DE LA SEGURIDAD DE LA RED

EVENTO ONLINE,
28 DE ABRIL DE 2022

it Digital Security

Webinar Aruba

EL NUEVO PARADIGMA DE SEGURIDAD PARA ENTORNOS SD-WAN



aruba

a Hewlett Packard Enterprise company

Abril 2022

Webinar Aruba

El nuevo paradigma de seguridad para entornos SD-WAN

La desaparición del perímetro tradicional, la adopción de entornos híbridos y multicloud, y el acceso a los recursos empresariales desde cualquier lugar, en cualquier momento y con cualquier dispositivo, está provocando una convergencia creciente entre los ámbitos de red y la seguridad.

Considerado como un elemento clave en cualquier proceso de transformación digital, SD-WAN mejora el rendimiento de las aplicaciones empresariales, optimizando la experiencia de usuario y simplificando las operaciones; todo ello de la mano de nuevos modelos de consumo como SaaS o NaaS, que permiten minimizar la inversión de capital requerida para la transformación. Pero en este nuevo paradigma, es necesaria una propuesta integrada de seguridad desde el extremo a la cloud, que combine estrategias como Zero Trust y Seguridad en la nube con SDWAN, para securizar las comunicaciones y proteger todos los dispositivos.

Teniendo en cuenta esta situación se organizó un encuentro en el que participaron portavoces de Aruba, una compañía de HPE, junto con algunos de sus clientes, y en el que se planteó por qué SD WAN, cómo tiene que ser gestionada o cómo encaja en el modelo SASE.

Iker del Fresno, Country Manager de Aruba, una compañía de HPE; Pedro Martínez, Responsable

"Con SD-WAN el cliente recupera la visibilidad y el control de lo que ocurre en esa red WAN para mejorar procesos y elegir dónde quiere que pase cada cosa"

Iker del Fresno,
Country Manager de Aruba,
una compañía de HPE

de Desarrollo de Negocio de Aruba; David Elvira, Jefe CoE Ciberseguridad de MAHOU; Javier Larrea Arias, Responsable de sistemas de Gadisa y José Antonio Campos Leal, Director de infraestructura y comunicaciones de Grupo Nueva Pescanova, fueron los participantes de un debate que arrancó con la visión de Aruba presentada por Pedro Martínez.

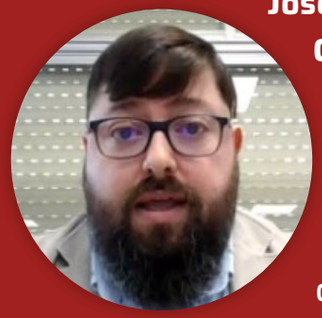
Aruba SD-WAN

Antes de adentrarnos en cómo ve Aruba el nuevo rol de SD-WAN en el nuevo entorno corporativo y qué implicaciones tiene desde el punto de vista de seguridad, Pedro Martínez Bustos quiso explicar cómo es la visión integrada extremo-nube de Aruba.

Hablaba el directivo de un extremo inteligente formado por todos aquellos lugares en los que nos encontramos con personas, dispositivos o cosas que generan datos, como pueden ser colegios, hospitales, universidades, oficinas, fábricas…. Lugares en los que esos usuarios y dispositivos intercambian información entre sí, pero también acceden a servicios que están en un entorno de nube híbrida y, cada vez más, en un modelo de consumo SaaS. En medio de estos dos elementos está SD-WAN,

Quién es quién

Antes de iniciar el debate se pidió a cada uno de los portavoces a qué se dedican sus empresas.



José Antonio Campos Leal, Director de infraestructura y comunicaciones de Grupo Nueva Pescanova explicaba que la compañía, con presencia en 19 países, centra su actividad en el sector del pescado y del congelado y que, en su proceso de transformación digital, está renovando todas las infraestructuras y las comunicaciones.

Respecto a **Mahou** es una empresa familiar con más de 130 años de historia, una implantación internacional en más de 70 países y marcas tan relevantes como Mahou, San Miguel, Solán de Cabras o Alhambra. La compañía tiene ocho centros de producción en España, dos fuera y cuatro manantiales con sus plantas de envasado.

En cuando a Gadisa, que se ha formado por la integración de distintos distribuidores de alimentación con más de 100 años de antigüedad, es una cadena de alimentación con 8.000 empleados y más de 400 puntos de venta localizados principalmente en Galicia y León. **Javier Larrea Arias, Responsable de sistemas de Gadisa,** dice que la compañía esté en un proyecto de migración de comunicaciones basado en SD-WAN.

"La solución SD-WAN permite escoger la mejor infraestructura disponible en cada ubicación geográfica sin depender ni del operador ni de la infraestructura que maneje en cada zona, ni de sus acuerdos"

Javier Larrea Arias,
Responsable de sistemas, Gadisa

"el nuevo backbone inteligente de interconexión que nos permite interconectar por un lado estos usuarios y dispositivos dentro del extremo para que se intercambien información entre sí, pero también para que puedan acceder a estos servicios en la nube".

Este nuevo paradigma, en el que prácticamente nos encontramos el Edge en cualquier localización, tiene claras implicaciones en términos de una mayor superficie de exposición, lo que implica un aumento de los riesgos, explicaba Pedro Martínez, añadiendo que la red WAN tradicional ya no es la ruta óptima a la nube y que hay que encontrar un equilibrio entre la experiencia del usuario y la seguridad, sobre todo en un entorno "en el que las cosas ya no dependen sólo de nosotros, porque estamos

Webinar Aruba

"Con Aruba conseguimos orquestar un montón de soluciones con unas integraciones bastante sencillas que nos permiten aprovechar las sinergias al máximo e intentar ir hacia el modelo de Zero Trust"

David Elvira,
Jefe CoE Ciberseguridad, MAHOU

EL NUEVO PARADIGMA DE SEGURIDAD PARA ENTORNOS SD-WAN

CLICAR PARA VER EL VÍDEO

accediendo a servicios que están fuera del entorno corporativo".

Aruba EdgeConnect y Aruba SD-Branch son las dos aproximaciones de la compañía para hacer frente a esta situación. La primera, explicaba el directivo de Aruba, es una solución pensada esencialmente para entornos donde el foco es la transformación de la WAN "y donde lo que va a primar es optimizar la experiencia del usuario, sea cual sea la red WAN que tenemos por debajo". En cuanto a Aruba SD Branch está muy dirigida a entornos donde el objetivo es la transformación de la Branch y lo que prima es dar una solución integrada no solo para la WAN, sino para la LAN y la WiFi, en una gestión integrada a través de un panel de control único que permite controlar la totalidad de tecnología de comunicaciones y seguridad de branch desde un único punto.

A partir de aquí aseguraba Pedro Martínez que el modelo de seguridad que tenemos que adoptar

"Necesitamos que nuestras comunicaciones y nuestras integraciones también evolucionen, intentando reducir costes y unificar lo más posible para que no tengamos ni silos ni cosas desplegadas 30 veces en 30 países diferentes"

José Antonio Campos Leal, Director de infraestructura y comunicaciones, Grupo Nueva Pescanova

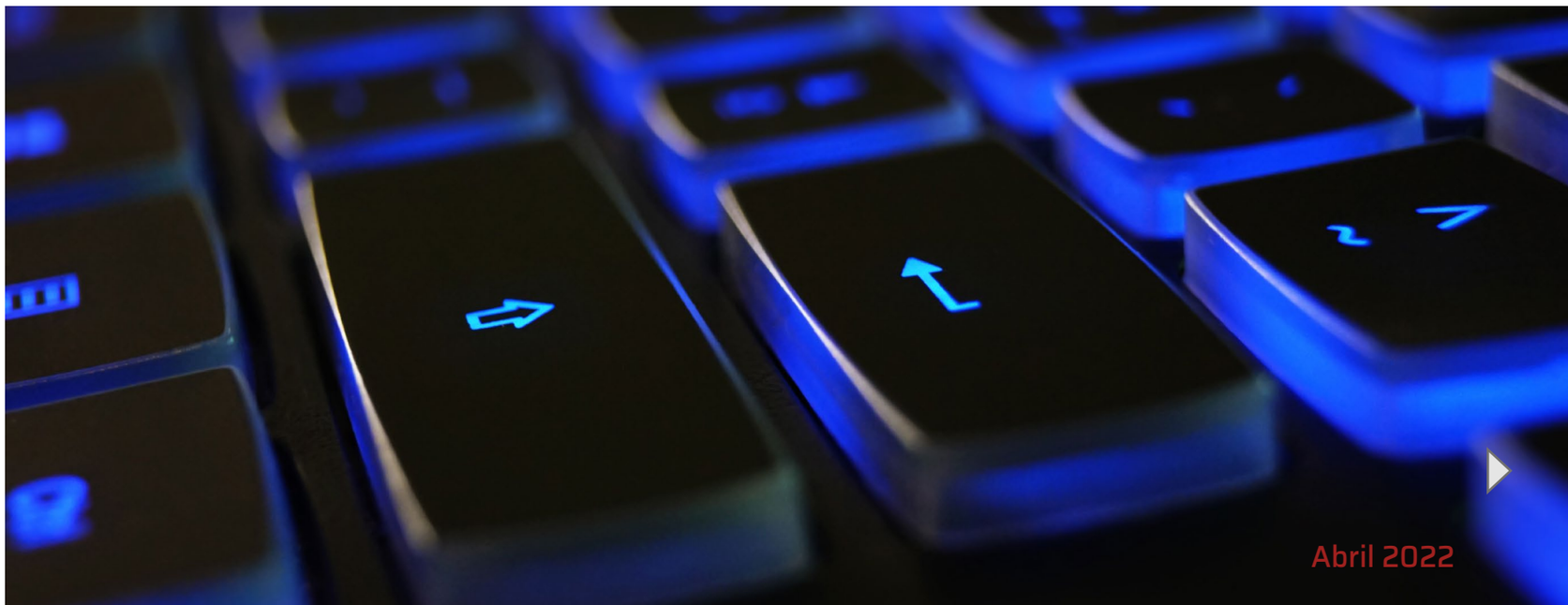
para este nuevo entorno extremo-nube es clave, y que la propuesta de Aruba se articula en tres pilares fundamentales: Zero Trust, SD-WAN y Seguridad en la nube. Tras explicar las diferentes opciones de la solución Aruba SDWAN, destacada el directivo los tres elementos de la propuesta de valor de la compañía: Seguridad, Inteligencia y Simplicidad.

SD-WAN a Debate

Iker del Fresno Country Manager de Aruba, una compañía de HPE, arrancaba el debate preguntando a los invitados qué impulsó la adopción de SD-WAN, qué esperaban conseguir y qué es lo que les ha aportado.

Dentro de una transformación mucho más amplia y a todos los niveles, en Grupo Nueva Pescanova hay un foco importante en la integración de las sedes, explicaba José Antonio Campos Leal, Director de infraestructura y comunicaciones de la compañía, añadiendo que en muchos de los países en los que la empresa tiene presencia las comunicaciones son complicadas. La solución SD-WAN de Aruba, combinado con un cambio de operador ayuda a minimizar el impacto porque "permite mezclar tecnología y hacer una adecuación de la red para que podamos integrar las sedes internacionales".

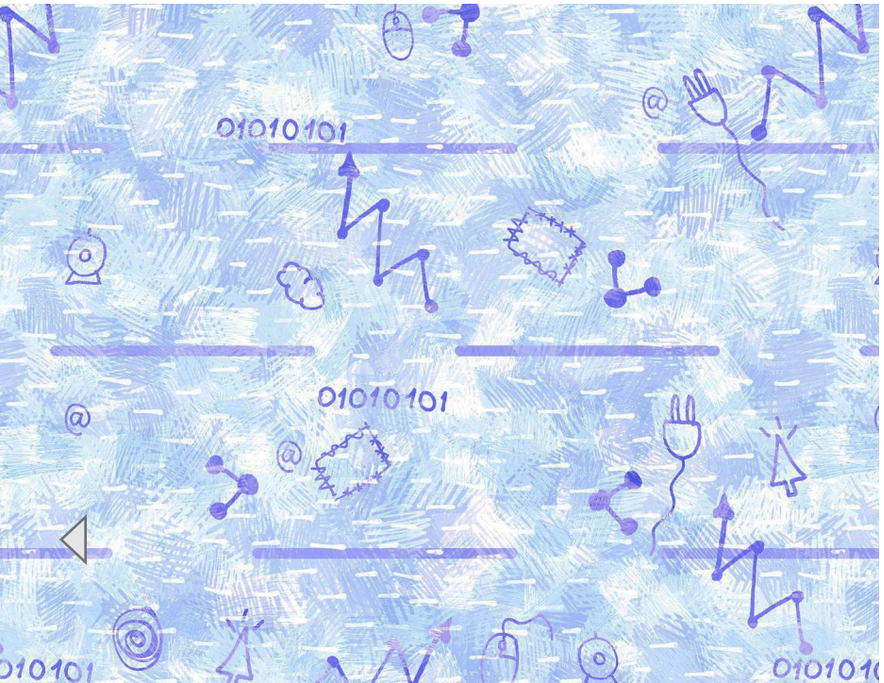
En el caso de Mahou, más enfocados en el ámbito nacional, "adoptar una solución como es SD-WAN nos viene derivada de múltiples factores, como es el aumento de trabajadores remotos que se conectan directamente a aplicaciones en la nube", decía David Elvira, responsable de Ciberseguridad de Mahou, para quien la seguridad tradicional basada en perímetro ya no es suficiente. Añadía este directivo que la transformación digital conlleva necesariamente una transformación de la WAN y de la seguridad, y que la integración de las capacidades de SD-WAN con los servicios de seguridad modernos "permiten ofrecer un servicio de calidad y una mejor experiencia de usuario"



"Este nuevo paradigma, en el que prácticamente nos encontramos el Edge en cualquier localización, tiene claras implicaciones en términos de una mayor superficie de exposición"

Pedro Martínez, Responsable de Desarrollo de Negocio de Aruba, una compañía de HPE

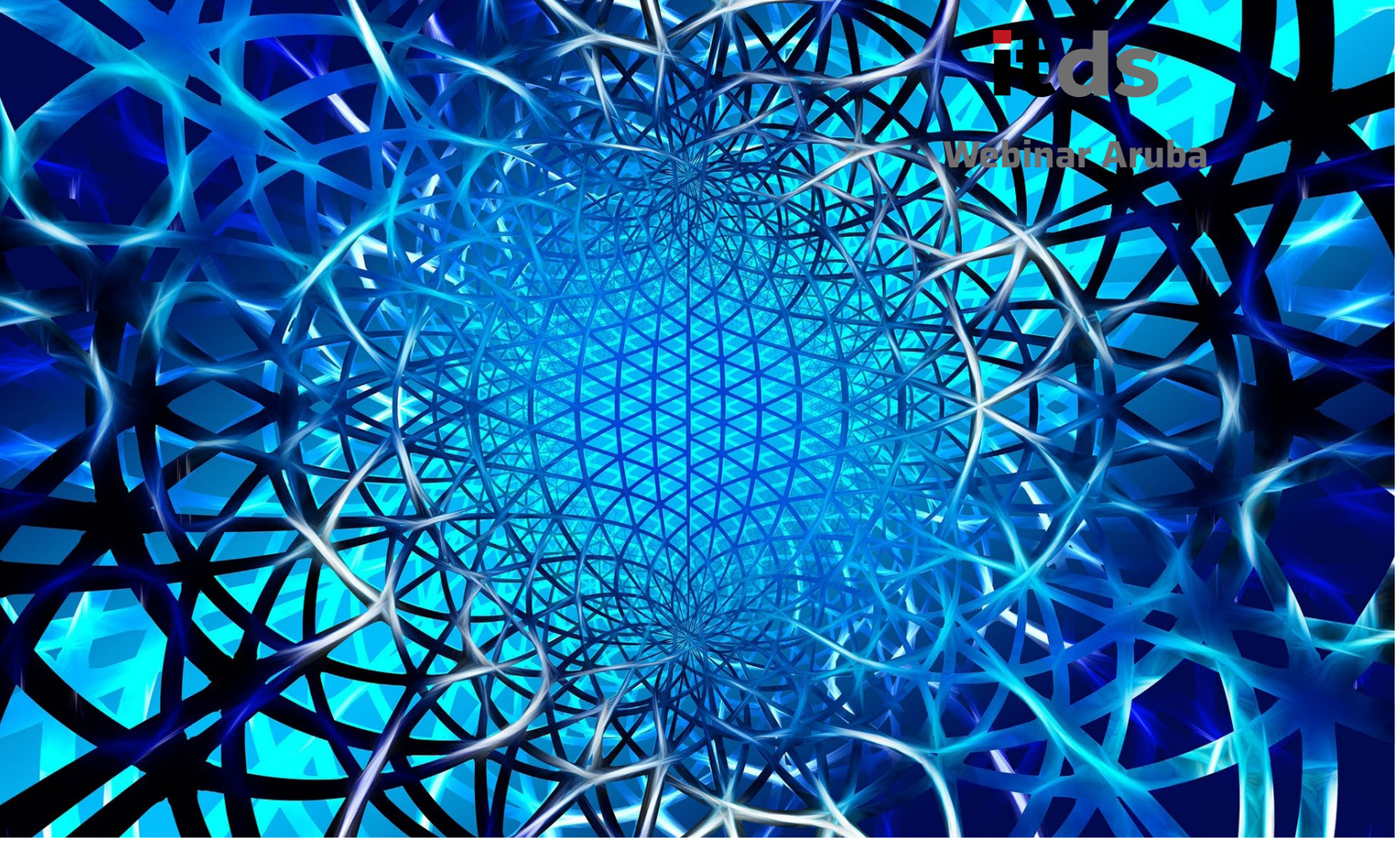
Asegurando que hay provincias en España en las que te puedes encontrar con los mismos problemas de comunicación que se encuentra Grupo Nueva Pescanova en algunos de los países que opera, explicaba Javier Larrea Arias, Responsable de sistemas de Gadisa, que "la solución SD-WAN resuelve el problema porque te permite escoger la mejor infraestructura disponible en cada ubicación geográfica sin depender ni del operador ni de la infraestructura que maneja en esas zonas, ni de sus acuerdos. Es decir, al final tú tienes el control, que es algo que nosotros valoramos mucho". Además, la tecnología SD-WAN permite a la compañía "decidir qué tráfico viene a la central y qué tráfico sale localmente por las conexiones que hay en cada centro, y aplicarles políticas unificadas de una manera sencilla porque se aplican mediante plantillas y esas plantillas son compartidas por todos los centros".



Destacaba en este punto Iker del Fresno que tradicionalmente la WAN ha sido territorio de los operadores tradicionales de comunicaciones que aportaban la solución de interconexión. Añadía que con SD-WAN el cliente recupera la visibilidad y el control de lo que ocurre en esa red WAN para mejorar procesos y elegir dónde quiere que pase cada cosa, y planteaba a los invitados al debate si el Service Provider sigue siendo imprescindible en este nuevo escenario y qué papel tiene.

En el caso de Gadisa explicaba su responsable de sistemas que cada cierto tiempo se evalúan los operadores que prestan servicio a la compañía, y que uno de los requisitos solicitados es el hacer una transición hacia SD-WAN. La historia de Gadisa, y por tanto una herencia que ha ido evolucionado a nivel de infraestructura, llevó a la empresa a optar por la solución de Aruba porque "es la que mejor cumplía los estándares para la interconexión con dispositivos de otros fabricantes. Hay otros fabricantes de soluciones SD-WAN, pero en general están muy enfocados a que toda la infraestructura sea del mismo fabricante. Aruba no. Aruba nos da la opción de elegir en cada momento".

A nivel de proveedor, explicaba David Elvira que la situación de Mahou era un poco especial "porque manejábamos líneas activo-pasivo, sobre todo para temas de contingencia". El nuevo escenario de SD-WAN facilita la situación porque proporciona un punto de gestión centralizado que permite orquestar todas las comunicaciones de la compañía hacia



la WAN, independientemente de los operadores; “nosotros estamos trabajando en varios centros con distintos operadores, y no sólo distintos operadores, sino distintas tecnologías por un tema de contingencia de negocio. Necesitamos tener líneas que no sean cableados para que nuestras fábricas, en un momento dado, no se paren”.

Añadía que ahora la tecnología permite abstraerse del operador y tener líneas activo-activo; “las orquestamos para que podamos utilizar las aplicaciones que demandan los usuarios en función de la calidad que ellos requieren. Si a esto le añadimos la posibilidad de que sea dinámicamente, pues se nos abre un abanico entero de posibilidades que estamos utilizando y creo que de alguna manera bastante eficiente para nosotros”.

Sobre la abstracción del operador, comentaba José Antonio Campos Leal que la adopción de SD-WAN ha permitido a Nueva Pescanova “contratar líneas más convencionales en cada uno de los países y luego nosotros hacer ese soporte de la red a través de SD-WAN”. Explicaba que “nosotros hemos hecho la instalación con operador, pero mañana podemos añadir un operador sin ningún problema o añadir una nueva tecnología sin ningún problema, simplemente modificando una configuración que mañana despliegas a cualquier parte del mundo de una manera relativamente sencilla”. Sobre la facilidad de Aruba para trabajar con el resto de fabricantes del ecosistema, apuntaba la facilidad de crear reglas y el control de la seguridad de SD-WAN, así como “la simplificación de tareas

CONCLUSIONES

Pedro Martínez, Responsable de Desarrollo de Negocio de Aruba, fue el encargado de ofrecer las conclusiones destacando cómo durante el debate se habló de la importancia de las soluciones SD-WAN para optimizar la experiencia del usuario en un entorno en el que la red corporativa tradicional ya no es la ruta óptima a los servicios en la nube, o la flexibilidad que proporciona a la hora de definir cómo quieres avanzar hacia esa migración de servicios a la nube.

En lo que se refiere a la seguridad “ha habido bastante unanimidad en que este nuevo modelo de conectividad extremo nube requiere una aproximación un poco distinta” que contempla combinar estrategia de Zero Trust y SASE “que nos da ese equilibrio óptimo entre garantizar esa mejor experiencia de usuario, pero al mismo tiempo proporcionar ese nivel óptimo de protección”.

Destacó también Pedro Martínez el nuevo rol de los operadores en el modelo de conectividad basado en SD-WAN, que permite la elección de los mismos, lo que impacta en el coste, una mayor posibilidad en la elección y combinación de tecnologías de conectividad y mayor visibilidad y control de la WAN por parte de las organizaciones.

Por último, destacó el directivo de Aruba la capacidad de simplificar que brinda la tecnología al permitir una gestión integrada todo lo que es el entorno de la WAN desde un panel de gestión único y “las posibilidades de automatizar, así como las capacidades de escalar, son las ventajas que nos da el tener una solución en la nube”.

que para que los equipos de operación y la administración no sufran tanto el tema de la gestión de la parte WAN y de la parte LAN”.

Asegurando que Aruba siempre ha creído en la importancia de la seguridad como algo transversal, plantea Iker del Fresno cómo se ve la confluencia de Zero Trust, SD-WAN y seguridad cloud, tres elementos que confluyen en el modelo SASE.

El primero en responder fue David Elvira, de Mahou, quien aseguró que lo que ahora Gartner llama SASE es algo en lo que se lleva trabajando desde hace tiempo y que les ha sorprendido cómo Aruba ha sido capaz de integrarse con estas soluciones; “al final lo que conseguimos es orquestar un montón de soluciones con una integraciones bastante sencillas – cuando digo sencillas hablo de minutos, que nos permiten aprovechar las sinergias al máximo e intentar ir hacia hasta este modelo de Zero

Trust que es difícil de conseguir, pero que al final, orquestando varias piezas aunque sean de varios fabricantes, nos proporciona un ecosistema de herramientas de seguridad integrados con la parte de SD-WAN que nos ayuda en el día a día bastante".

Afirmando que la seguridad es vital para Gadisa, señalaba su responsable de sistemas que hay una capacidad de Aruba muy interesante relacionada con el acceso a la propia red, que no es otra que ClearPass. Sobre esta herramienta destacaba Javier Larrea Arias la integración que tiene y que permite "perfilar los clientes, gestionar sus tráficos, analizar lo que hacen, que vayan solo a donde pueden ir", además de la gestión de las plantillas ya permite "tener un modelo de gestión unificada para que todo el mundo vaya a donde tiene que ir y por dónde tiene que ir y solo así", de forma que combinas la automatización, el control y perfilado de usuarios, las plantillas, "y tienes ya una solución muy unificada, con una visión única de todo lo que está pasando en tu red".

"Estandarizar, que todos los sitios sean más o menos iguales o con una tecnología más o menos igual, para nosotros es primordial", explicó José Antonio Campos Leal cuando se le plantea el valor que tiene, y más como director, infraestructuras y comunicaciones de Grupo Nueva Pescanova, el poder tener una visión global; "tenemos una gestión controlada en cualquier país, desplegamos los mismos SSIDs prácticamente en todos los países del mundo, lo cual facilita mucho la gestión de los PCs que es una manera de facilitar el trabajo a nuestros compañeros de IT".

Destacó también el directivo de Grupo Nueva Pescanova la solución Silver Peak de Aruba, que se utiliza en algunas de las sedes de la compañía, lo que facilita el poder priorizar el tráfico, saber que entornos podemos acelerar en un momento dado, qué tráficos tenemos que priorizar... y administrarlos

de una manera sencilla. “Para nosotros todo esto es vital”.

Más allá de SD-WAN

Los tres clientes de Aruba que participaron en este evento tienen una implantación de SD-WAN más o menos avanzada. Ya saben lo que les está aportando. ¿Qué hacer a partir de aquí?

Reconociendo que Clear Pass es una de las soluciones de Aruba que más le gustan, dice el portavoz de Gadisa que el siguiente paso es “extender ClearPass hasta el límite de la red”. Explicó que hasta este momento la compañía utiliza la solución para gestionar toda la parte de servicios centrales, la WiFi, lo tradicional… “pero no teníamos visibilidad de lo que ocurría en los centros. Ahora con la integración de ClearPass y Aruba Central podemos llegar hasta el borde”.

Se autodefine David Elvira como un “fanático de la automatización” para comentar que en Mahou existen integraciones de automatización entre Aruba y otros fabricantes “que nos están aportando muchas ventajas y reduciendo costes”. Por otra parte, y apoyandonse en la infraestructura y funcionalidades que se están utilizando y que proporciona Aruba “hay un paso que queremos dar: el perfilado de esos dispositivos de forma automática. Vosotros tenéis una aproximación que me gusta para incorporarla a todo el tema de seguridad que es la parte de Clearpass Device Insight que me parece muy interesante”.

Explica el portavoz de Nueva Pescanova que la compañía tuvo un cambio organizativo importante hace más de un año, con la incorporación de un nuevo CISO, José Manuel Carpallo, que estableció el Cloud First como estrategia en una empresa muy legacy y un montón de fábricas. En esta reconversión digital que conlleva llevar muchos entornos a la nube “necesitamos que nuestras comunicaciones y nuestras integraciones también evolucionen, intentando reducir costes y unificar lo más posible para que no tengamos ni silos ni cosas desplegadas 30 veces en 30 países diferentes. Toda esa integración requiere una comunicación estable, segura, con una alta disponibilidad, que evite los cortes. Y este es nuestro paso más importante en el próximo año desde el punto de vista de infraestructuras y comunicaciones”.

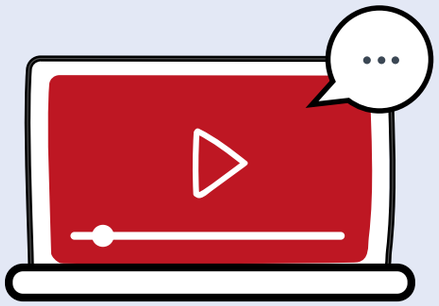
El nuevo paradigma de seguridad para entornos SD-WAN

La desaparición del perímetro tradicional, la adopción de entornos híbridos y multicloud, y el acceso a los recursos empresariales desde cualquier lugar, está acrecentando la convergencia entre la red y la seguridad. En este encuentro conocerás por qué se tiene que adoptar una estrategia SD-WAN, cómo se tiene que gestionar, qué aporta al concepto SASE o cuál es el siguiente paso.

Opera tu IT de forma inteligente y mirando al futuro: conoce OPTIC de Micro Focus

El éxito del negocio en un mundo digital depende de la habilidad de la organización de IT para transformarse al mismo tiempo que el negocio, ofreciendo servicios con agilidad y manteniendo el rendimiento. Pero no es tarea fácil, se requiere un nuevo enfoque.

¡Consulta nuestros webinars!



#ITWEBINARS

La transformación del trabajo: el empleado conectado

ON DEMAND

La naturaleza del trabajo ha cambiado rápidamente. COVID-19 ha tenido, y continuará desempeñando, un papel fundamental en esta transformación del entorno laboral. La mayor parte de las compañías, para mantener a salvo a sus empleados, está adoptando un modelo híbrido o remoto, de manera definitiva. El empleado conectado y productivo requiere, por tanto, de un nuevo entorno de trabajo que le proporcione la mejor experiencia. ¿Cómo construirlo? Únete a este Encuentros IT Trends.

Prioridades tecnológicas para los CIO en 2022

En los últimos dos años el progreso tecnológico se ha disparado. De un lado, la industria avanza en sus propuestas y del otro, la empresa se ha visto abocada a acelerar sus planes de adopción. La transformación digital es una evolución constante y pone sobre la mesa de los decisores de TI múltiples frentes. ¿Cuáles serán sus prioridades en este año?

Retos y soluciones para una
Sanidad en cambio

Patrocinadores:

Retos y soluciones para una Sanidad en cambio

La pandemia del coronavirus ha puesto en evidencia la necesidad de acelerar la transformación digital de prácticamente todos los sectores. En España, al igual que en el resto del mundo, una de las áreas que más afectada se ha visto por su propia naturaleza ha sido la de la sanidad, que se ha enfrentado a una situación sin precedentes que ha obligado a buscar nuevos modelos de atención basados en la tecnología.

Durante estos últimos años, hemos sido testigos de un momento de gran aceleración en la adopción de nuevas tecnologías en todos los sectores. Uno de los más importantes ha sido el sanitario, donde la pandemia ocasionada por la COVID-19 ha puesto de manifiesto la necesidad acuciante de implantar soluciones tecnológicas que dieran respuesta a los grandes retos del presente y del futuro. En una crisis de salud pública como la que vivimos se ha evidenciado que las organizaciones sanitarias no estaban preparadas para atender de forma personalizada a pacientes que no llegaran a través de las vías habituales.

RETOS Y SOLUCIONES PARA UNA SANIDAD EN CAMBIO

Desde la aparición de los primeros casos en febrero de 2020, son ya 11,3 millones de personas las que se han infectado con la Covid-19, y se contabilizan 101.703 fallecidos, a fecha de marzo de 2022. Con estas cifras, España ocupa la décima posición a nivel mundial en cuanto a número de casos confirmados de coronavirus.

Estas cifras han puesto de manifiesto una serie de nuevos retos que ha tenido que afrontar el sector de manera acuciante. Accenture señala en su informe Rapid Response seis retos principales: incremento de pacientes, sobrecarga de llamadas al servicio, monitorización y reporting, coordinación en la respuesta, peligros en la continuidad de la actividad y eficacia del personal.

Como indican las cifras de infectados, el primer reto al que tuvo que hacer frente el sector sanitario ha sido el del incremento de pacientes, que ha llegado casi a colapsar el sistema en momentos determinados. Es por ello que se necesitaron tomar medidas de urgencia, como la utilización de pabellones multiusos para las campañas de vacunación, plantas enteras de hospitales dedicadas a pacientes con Covid e incluso la construcción de nuevos centros hospitalarios para poder dar servicio a la población infectada. Esta sobrecarga de pacientes también se vio reflejada en las líneas telefónicas, con las centralitas de los centros sanitarios completamente colapsadas por las llamadas de los pacientes en busca de información.

Además, la necesidad de mantener una monitorización constante sobre toda la situación se convirtió en una prioridad, de manera que esa recogida de datos de lo que estaba sucediendo permitiera a las autoridades sanitarias tomar las mejores decisiones en función de cómo iban evolucionando las cifras de la pandemia. Otro de los retos más importantes que está encarando el sector es el de la coordinación en la respuesta, para ofrecer al ciudadano información precisa en cuanto a la situación y a las medidas necesarias que debiera tomar en función de su situación.

En España, al igual que en el resto del mundo, una de las áreas que más afectada se ha visto por su propia naturaleza ha sido la de la sanidad, que se ha enfrentado a una situación sin precedentes que ha obligado a buscar nuevos modelos de atención basados en la tecnología

Esta situación afectó directamente al colectivo de los profesionales de la salud, que al estar en primera línea, sufrieron directamente las consecuencias de la pandemia, llegando a contraer el virus hasta el 20% del colectivo en algunos casos, lo que suponía un problema a la hora de poder dar un servicio ya de por sí colapsado por el gran número de contagios que se estaban dando. Además, en muchas ocasiones este personal no contaba con los recursos necesarios para poder dar un servicio de calidad, ni a nivel de protección, ni a nivel tecnológico, en un sector que en la mayoría de los casos no había dado muchos pasos para afrontar su transformación digital.

LA HORA DE LA TELEMEDICINA

Para afrontar esta situación, en una pandemia cuya base ha sido la distancia social y el confinamiento de las personas infectadas, uno de los primeros campos que tuvo que revolucionar el sector sanitario fue el de la asistencia, apostando por un modelo remoto a través de la telemedicina, algo que hasta la fecha no era nada común. Un estudio de Capterra señala que un 62% de los españoles ha consultado al médico por medio de esta tecnología a raíz de la pandemia, e incluso para el 92% de las personas había sido su primera vez.

La implantación de este nuevo modelo ha sido todo un éxito, como demuestran datos como los de mediQuo, que señalan que las consultas de telemedicina habían aumentado un 153% en España a los pocos meses desde que se decretara el estado de alarma. Claramente se trata de un modelo que ha llegado para quedarse. Incluso la Organización para la Cooperación y el Desarrollo Económicos (OCDE) señalaba en un informe la necesidad de fortalecer los servicios de salud prestados de forma electrónica a través de internet.

El informe "Telemedicine: Emerging Technologies, Regional Readiness & Market Forecasts 2021-2025" de Juniper Research indica que gracias a la telemedicina el sector sanitario podrá ahorrar 21.000 millones de dólares en costes para el año 2025 y señala que para ese año ya se habrán realizado más de 765 millones de teleconsultas a nivel global.

Pero la velocidad a la que se ha impuesto este nuevo modelo hace que tanto profesionales sanitarios como pacientes se enfrenten a una serie de retos que tendrán que ir afrontando poco a poco. Uno de los más importantes es el de la reducción de la brecha digital, algo a lo que ayudaron mucho otros sectores como las compras online o las videollamadas con la familia durante el confinamiento, que pusieron sobre la mesa estas tecnologías para toda la población. Además, los profesionales sanitarios requieren de formación específica en el uso de esta nueva modalidad, de manera que sean capaces de ofrecer la mejor experiencia al paciente, ofreciéndole la mayor cercanía posible. Otro reto es el puramente tecnológico, con la necesidad de equipos

y conexiones de calidad que no entorpezcan la videoconsulta.

LOS DATOS Y SU CONFIDENCIALIDAD

Como en la mayoría de las industrias, la importancia del dato es primordial para ofrecer un servicio de calidad al paciente. En el caso del sector sanitario más si cabe, puesto que se trata de datos inherentes a las personas, con lo que la necesidad de mantener la confidencialidad médico-paciente se vuelve mucho más acuciante si cabe.

Por un lado, el sector utiliza todo el aglomerado de datos abiertos que puede obtener con el fin de optimizar su gestión y la organización de recursos, como indica el estudio "The Open Data Impact Map" de Open Data for Development Network (OD4D). Esto es muy importante en casos como el de la medicina preventiva, ya que permite el desarrollo de modelos predictivos capaces de diseñar patrones de comportamiento, que a través del análisis de los datos facilita una mejor atención del paciente, predecir su evolución e incluso adelantarse a sus necesidades.

El Big Data es un sector que está creciendo exponencialmente en todos los ámbitos, como demuestra el estudio de Technavio "Big Data Market by Type, Deployment, and Geography - Forecast and Analysis 2021-2025" que señala que para 2025 este mercado crecerá hasta los 247.300 millones de dólares con un CAGR del 18%. En concreto aplicado a la salud, el informe Big Data Analytics In Healthcare Market de Allied Market Research indica que su valor alcanzará los 67.820 millones de dólares para 2025.

En los proyectos estratégicos para la recuperación y transformación económica (PERTE), el Gobierno de España ha tenido muy en cuenta al sector sanitario, estableciendo un PERTE para la salud de vanguardia

En el sector sanitario se recaban una gran cantidad de datos que pueden provenir de diferentes fuentes: desde la información proporcionada por la maquinaria médica (pruebas de imagen y de laboratorio), hasta la información aportada por el propio paciente. La recogida, almacenamiento, tratamiento y posterior análisis de esos datos debe seguir un cuidadoso protocolo que permita facilitar la labor de los profesionales de la salud, para que puedan disponer de ellos siempre que los necesiten de una forma rápida y sencilla, pero teniendo en cuenta la importancia máxima de su seguridad, de manera que no haya brechas ni a la hora de almacenarlos ni en el momento de ser transferidos, sea por el medio que sea.

Para ello, la tecnología se pone al servicio del sector, por lo que es tarea de las organizaciones de salud implementar las soluciones adecuadas a la hora de velar por la privacidad de los datos, de contar con los dispositivos adecuados para su recogida y almacenamiento, y de preparar a los profesionales que están en contacto con ese dato, de manera que realicen un tratamiento y mantenimiento correcto.

EL GRAN RETO DE LA SEGURIDAD

Por si era poco la situación de pandemia que se desató a principios de 2020 con la aparición del coronavirus, el sector sanitario ha tenido que enfrentarse en este tiempo a un nuevo reto, el gran aumento de ciberataques que se ha producido con el punto de mira puesto en la industria de la salud. El pasado año, el Instituto Nacional de Ciberseguridad de España (INCIBE) señalaba que más de 500 instituciones sanitarias españolas habían notificado incidentes o reportes de vulnerabilidad, lo que suponía un 48% más con respecto al año anterior.

Uno de los principales riesgos a los que se enfrenta el sector sanitario es el de los ataques de ransomware, a través de los cuales el ciberdelincuente es capaz de cifrar toda la información del sistema para pedir un rescate a cambio de su liberación. Este tipo de ataques se han multiplicado en los últimos años. Según el informe "El estado del ransomware en la sanidad 2021" de Sophos, algo más de un tercio de las organizaciones sanitarias españolas (34%) recibieron algún tipo de ataque de ransomware el año pa-

sado. Para poder recuperar sus datos, el 34% decidió pagar el rescate, ya que no consiguieron hacerlo de otra forma, como demuestra que solo el 44% de las instituciones sanitarias consiguieron restaurar sus datos a través de copias de seguridad. Estos datos ponen de manifiesto el éxito que tiene este tipo de ataques para los ciberdelincuentes, lo que explica este aumento en los últimos años.

Pero el ransomware no es el único peligro que amenaza al sector sanitario. Las fugas de datos también están a la orden del día, como demuestran los datos de Bitglass, que indican que tan solo en Estados Unidos se produjeron 599 fugas de información en esta industria que afectaron en conjunto a más de 26 millones de personas. Sistemas desactualizados, tráfico de correo electrónico no cifrado, el Internet de las Cosas cada vez con mayor penetración en el sector sanitario, son muchos los riesgos que se presentan para un sector que ha tenido que afrontar una transformación digital de la noche a la mañana, para la que en muchas ocasiones se primó la necesidad de activar determinados servicios sin pararse a pensar en las capas de protección que serían necesarias para mantenerlos seguros.

Para ayudar a securizar los nuevos entornos digitales creados tras la pandemia, el Instituto Nacional de Ciberseguridad (INCIBE) ha publicado una serie de pliegos por sectores denominados Sectoriza2 con una serie de consejos y herramientas que ayudarán a las organizaciones a protegerse, incluyendo como no podía ser de otra manera también al sector sanitario.

PERTE PARA LA SALUD DE VANGUARDIA

Entre los proyectos estratégicos para la recuperación y transformación económica (PERTE), el Gobierno de España ha tenido muy en cuenta al sector sanitario, estableciendo un PERTE para la salud de vanguardia a finales del pasado año 2021. Su finalidad es la de apoyar la transformación digital de la industria sanitaria y prevé una inversión entre el sector público y el privado de 1.469 millones de euros en el periodo 2021 y 2023.

Los cuatro grandes objetivos que persigue este plan son posicionar a España como país líder en la innovación y desarrollo de terapias avanzadas, impulsar la puesta en marcha de medicina personalizada de precisión de forma equitativa, desarrollar un Sistema Nacional de

Salud digital y potenciar la atención sanitaria primaria a través de la transformación digital.

Como demuestras estos objetivos, el impulso de la transformación digital del sector es un hecho. Por un lado, el Componente 11 (Modernización de las administraciones públicas) está orientado al establecimiento de diferentes medidas para la modernización de los servicios digitales ofrecidos por el Ministerio de Sanidad en tres áreas principales de actuación: el desarrollo de servicios digitales e inteligentes, la interoperabilidad de la información sanitaria y el impulso a la analítica de datos.

Por otro lado, el Componente 18 hace mención de un Data Lake sanitario, que supone la creación de un repositorio de datos alimentado por los diferentes sistemas de información relevantes en Salud y que permitirá un análisis masivo e inteligente de los mismos, con capacidad de respuesta en tiempo real, orientado a la protección de la salud, la predicción sanitaria, así como para el incremento en la eficiencia del diagnóstico, tratamiento y rehabilitación de enfermedades, en las condiciones adecuadas de ciberseguridad.

Además, el Componente 19 hace mención a la necesidad de que los profesionales sanitarios también adquieran competencias digitales avanzadas dentro de los programas de formación, con menciones específicas a tecnologías disruptivas como la Inteligencia Artificial o la robótica, sin dejar de lado la ciberseguridad. ■

MÁS INFORMACIÓN

- Número acumulado de casos confirmados y muertes del coronavirus en España entre el 15 de febrero de 2020 y el 18 de marzo de 2022 de Statista
- Número de casos confirmados de coronavirus en el mundo a fecha de 18 de marzo de 2022, por país de Statista
- Informe Rapid Response de Accenture
- Diario Médico: profesionales sanitarios infectados por el coronavirus en España
- Capterra: Telemedicina en España: la irrupción tecnológica en la relación paciente-médico
- mediQuo: La razón por la que los médicos se deben adaptar a la nueva normalidad
- OECD Economic Surveys Spain
- Informe "Telemedicine: Emerging Technologies, Regional Readiness & Market Forecasts 2021-2025" De Juniper Research
- Estudio "The Open Data Impact Map" de Open Data for Development Network (OD4D)
- Estudio Technavio "Big Data Market by Type, Deployment, and Geography - Forecast and Analysis 2021-2025"
- Informe Allied Market Research Big Data Analytics In Healthcare Market
- Datos sobre aumento de ciberataques al sector sanitario del Instituto Nacional de Ciberseguridad de España (INCIBE)
- Informe "El estado del ransomware en la sanidad 2021" de Sophos
- Informe Bitglass sobre fugas de datos en el sector sanitario de Estados Unidos
- Sectoriza2 Salud, Instituto Nacional de Ciberseguridad de España (INCIBE)
- PERTE para la salud de vanguardia

SOLUCIONES LOGITECH PARA **ENTORNOS SANITARIOS**

Conéctese a través de vídeo de alta calidad cuando y donde sea más necesario.

Retos y Soluciones para una Sanidad en cambio

En el sector sanitario, la pandemia provocada por la Covid-19 ha puesto de manifiesto la necesidad acuciante de implantar nuevas soluciones tecnológicas que dieran respuesta a los grandes retos a los que se enfrenta el sector. Necesitamos una nueva forma de atención digital, una telemedicina que consiga conectar con los pacientes de forma preventiva y que los datos médicos sensibles y su análisis estén siempre disponibles y se pueda acceder a ellos de manera segura.

La llegada de la pandemia del coronavirus supuso una aceleración para la transformación digital de prácticamente todos los sectores, pero impactó a uno de ellos directamente: la sanidad. El sector sanitario se vio en la necesidad de realizar un cambio en sus procesos y aceleró su digitalización a pasos agigantados, tanto a la hora de hablar de teleasistencia como de los datos que manejan las organizaciones sanitarias, en muchos casos de una sensibilidad extrema. Esta rapidez a la hora de adoptar estos nuevos modelos no siempre se vio acompañada de un cuidado por la seguridad, lo que ha implicado grandes riesgos tanto para las propias instituciones sanitarias, como para el ciudadano. Por ello, el sector se enfrenta a una serie de importantes retos a los que debe dar solución de manera rápida y eficaz. Para hablar sobre cómo ha sido la transformación digital de la sanidad y cuáles son

MESA REDONDA IT: Retos y Soluciones para una Sanidad en cambio

“La visibilidad y el inventario de lo que tengas es la base para empezar a hacer políticas, segmentaciones de las redes, para intentar estar lo más seguro posible”

VESKU TURTIA

los principales retos a los que se enfrenta, hemos contado en esta Mesa Redonda IT con la participación de Vesku Turtia, Regional Director España y Portugal de Armis; David Marco, CEO de Iberlayer; Javier Rodríguez, Senior Key Account Manager de Logitech; Fernando Gutiérrez, Account Executive de MicroStrategy; Álvaro Fernández, Enterprise Account Executive de Sophos y Borja Pérez, Country Manager de Stormshield.

ESTADO ACTUAL DEL SECTOR SANITARIO

La mesa redonda comenzó agradeciendo a los profesionales sanitarios los esfuerzos que han realizado durante la pandemia, y que siguen realizando aún a día de hoy. En cuanto al estado actual del sector, para David Marco ha habido una evolución gigantesca. “Vemos una clara progresión hacia adelante, en cuanto a la integración de tecnologías dentro de la sanidad, ha mejorado en todos los sentidos, en lo personal, en lo tecnológico...”. El portavoz señala que muchos aspectos han mejorado muchísimo, como por ejemplo la teleatención. A pesar de ello, cree que hay un pequeño desfase en cuanto a la responsabilidad que tienen estos profesionales y las capacidades que se les dan.

Javier Rodríguez señala que ha habido un cambio de paradigma que ha sucedido de forma muy acelerada, por lo que han surgido algunas carencias. Por ejemplo, en el área de la videocolaboración. “No se ha hecho teniendo en cuenta la tecnología adecuada de audio y video y al final hay mucho por mejorar en ese ámbito”. Puede haber muchas vías de mejora para reducir colas en la atención primaria, para realizar algunas consultas que no requieran exploración de manera remota o para dar mejor calidad a los pacientes, que tengan que evitar desplazamientos y descongestionar un poco los centros de salud.

Por su parte, Fernando Gutiérrez cree que el estado de la sanidad en general en España en relación al dato ha salido reforzado. “Siempre se ha tenido el dato en cuenta, pero esta situación de necesidad tan brutal ha puesto de manifiesto la necesidad de apoyarse en el dato para tomar

“Si sigo construyendo la casa cogiendo piezas de la parte de abajo para crecer en altura cada vez más, pero usando materiales de abajo, llega un momento en que lo de arriba pesa tanto y lo de abajo es tan débil que no va a aguantar”

DAVID MARCO

decisiones y para la gestión”. En esos momentos que se vivieron y que se siguen viviendo de estrés es donde se ponen a prueba todos los sistemas, las cosas que funcionan bien, las cosas que tienen área de mejora... Se ha visto que esa necesidad de analizar de manera inmediata la disponibilidad de camas, de material o de personal, ha hecho que el dato haya cobrado mayor importancia.

UNA ACELERACIÓN EN SU TRANSFORMACIÓN DIGITAL

Sin duda la pandemia creo una situación sin precedentes ante la que prácticamente nadie estaba preparado. ¿La situación vivida durante estos

“Ha habido un despliegue acelerado y masivo de las plataformas de colaboración, pero hay mucho campo de mejora en dotar de los dispositivos adecuados para que los equipos médicos puedan colaborar a distancia”

JAVIER RODRÍGUEZ

últimos años de pandemia ha supuesto una aceleración en los procesos de transformación digital de la sanidad?

Para Vesku Turtia es un rotundo sí. Durante la pandemia no solo el sector de la salud, sino que todos los sectores han acelerado su transformación digital. “Lo que veo ahora con muchísima alegría es también que en el uso de distintos aparatos médicos en los hospitales tanto del sector privado como del público, están poniendo foco para ver cómo se puede securizar el uso de los sistemas médicos, porque hoy en día los hospitales, tanto del sector público como del privado, están bastante digitalizados”. Como vivimos en un mundo que no es perfecto, los ataques de ransomware pueden afectar a los sistemas de IT de un centro hospitalario, pero también ese mismo malware puede entrar en equipos médicos e incluso poner en peligro a los pacientes. “Vamos bien, pero todavía queda mucho que hacer”.

En palabras de Fernando Gutiérrez, “la sanidad no podía estar fuera de esta transformación digital”. La necesidad ha supuesto un acelerón de la digitalización, de eso no hay duda y pasa en general en todos los sectores, pero esta transformación digital ha venido muy propiciada también porque ha habido una digitalización del usuario. “La sanidad se ha encontrado con un ciudadano también más abierto, más preparado para utilizar canales digitales”. En cuanto a las personas mayores, que conforman gran parte de los usuarios de los servicios médicos, ha sido la necesidad de otros sistemas, como las compras online o las videollamadas con la familia, lo que ha conseguido que se digitalizaran.

Según Álvaro Fernández, ha habido sectores que habían avanzado más en su transformación digital porque se había demandado por parte de los usuarios. En el sector de la sanidad, al igual que por ejemplo en el de la educación, quizá no hubo esa demanda, que surgió a raíz de la pandemia y se tuvo que hacer de forma precipitada. “Desde el punto de vista de la seguridad, las prisas son enemigas de la securización. Se han priorizado los servicios perjudicando de alguna forma el hacer esos servicios seguros”. Además, añadía que “la pandemia hizo que todas las organizaciones de salud sin excepción pisasen el acelerador y fuesen a modelos más digitales para poder seguir dando un servicio”. Estas organizaciones están trabajando ahora en terminar de securizar estos servicios y en consolidarlos.

“Siempre se ha tenido el dato en cuenta, pero esta situación de necesidad tan brutal ha puesto de manifiesto la necesidad de apoyarse en el dato para tomar decisiones y para la gestión”

FERNANDO GUTIÉRREZ

Borja Pérez es de la opinión que hay distintos ritmos de transformación digital según las organizaciones. Para explicar su afirmación, saca a colación el PERTE que se ha aprobado para sanidad, el cual está dotado con 1.500 millones de euros y en el que hay cuatro grandes áreas

“Desde el punto de vista de la seguridad, las prisas son enemigas de la securización. Se han priorizado los servicios perjudicando de alguna forma el hacer esos servicios seguros”

ÁLVARO FERNÁNDEZ

de trabajo, una de ellas para la transformación digital en la atención primaria. “Las autoridades son conscientes de que hay que avanzar en ese sentido, pero hoy por hoy la atención primaria por ejemplo todavía adolece de falta de medios”. Después hace referencia a que los envíos de datos no son siempre del todo seguros: “Hay un montón de transferencias de datos en otras áreas y en muchos casos todavía no están debidamente implementados los procesos más seguros y más adecuados”.

¿ESTÁ PREPARADA LA SANIDAD?

La transformación digital de los entornos sanitarios ha supuesto la aceleración e implantación de nuevos modelos de asistencia, la telemedicina, la gestión y análisis de los datos y la securización de todos los sistemas. ¿Realmente está la sanidad preparada para todos estos avances?

En opinión de Vesku Turtia, lo más importante es que las organizaciones sepan lo que tienen en su infraestructura. “La visibilidad y el inventario de lo que tengas es la base para empezar a hacer políticas, segmentaciones de las redes, para intentar estar lo más seguro posible”. Es importante ser consciente de todo lo que hay, para después poder hacer las estrategias e integraciones necesarias para proteger todos los sistemas. “Cuanto más avanzamos en integración tecnológica, más dependientes somos de ella”, comenta David Marco, que añade hablando de la securización de los sistemas: “Rara vez se piensa en la seguridad antes que en el servicio”. El portavoz señala hay pocos servicios sanitarios que tengan un departamento de seguridad, y subraya la importancia de proteger el correo electrónico: “9 de cada 10 ataques de ransomware empiezan por un email, sin embargo solo el 5% de los presupuestos de ciberseguridad se dedican a proteger el correo”.

Álvaro Fernández también pone el punto de mira en la seguridad, cuando habla de la transformación digital acelerada que tuvo que emprender el sector a raíz de la pandemia: “Hay mucho espacio de mejora. Hemos podido salvar el escollo sabiendo que no ha sido todo lo seguro que debiera y hay muchas cosas que hacer”. En su opinión hay diferentes escenarios en cuanto al estado de las organizaciones sanitarias se refiere: “hay algunas que están mejor, otras que están peor, pero por supuesto hay mucho que hacer”.

“Hay concienciación sobre privacidad y confidencialidad de los datos del paciente, pero yo creo que no hay todavía los recursos dedicados a proteger la integridad y a proteger la disponibilidad de los datos”

BORJA PÉREZ

A Borja Pérez no le preocupan tanto estos nuevos servicios como el tema de los datos: “me preocupa más la gestión de datos internamente dentro de las distintas organizaciones”. A la hora de hablar de Big Data, es importante que los datos vayan anonimizados para trabajar con ellos.

Por otra parte, también cree que en el sector hay luces y sombras. "Es un entorno muy heterogéneo e incluso dentro de un mismo hospital hay áreas que están a la última y áreas que están todavía muy atrasadas".

DATOS Y TELEASISTENCIA

La nueva normalidad en la sanidad conlleva una securización del acceso a datos especialmente sensibles y del análisis de los mismos, así como de un nuevo modelo como es el de la teleasistencia, la virtualización o la movilidad que implica la asistencia remota.

Según Vesku Turtia "es muy importante proteger los datos de dentro del hospital con las segmentaciones". Es de la opinión que se está mejorando muchísimo en ese aspecto, y las instituciones, tanto públicas como privadas, están esforzándose muchísimo para proteger nuestros datos aparte de nuestra salud. Sobre todo cree que hay que poner el foco en que la circulación de los datos sea segura.

Javier Rodríguez comenta que "Los centros sanitarios donde hemos hecho despliegues de soluciones de videocolaboración, en barras por ejemplo de última generación, estas barras vienen ya con computación integrada, con inteligencia artificial, y sí que veo a los responsables de los centros sanitarios concienciados con el tema de la seguridad". Señala que hay cierta concienciación, pero está seguro que aún queda mucho por hacer.

En palabras de Fernando Gutiérrez, "en la parte del dato, hay velocidades distintas, no es lo mismo la sanidad pública que la sanidad privada y dentro de cada uno de ellas, hay hospitales y organizaciones en distintos rangos". El objetivo es que también la sanidad siga el concepto de Data Driven Company. También señala que la población cada vez es más digital, pero sigue habiendo una brecha importante que hay que romper.

Para Borja Pérez "Hay concienciación sobre privacidad y confidencialidad de los datos del paciente, pero yo creo que no hay todavía los recursos dedicados a proteger la integridad y a proteger la disponibilidad de los datos". El portavoz subraya que no se trata de un problema exclusivo de España, sino que es un problema a escala mundial. "No se están tratando de forma adecuada esos datos, no se están almacenando adecuadamente".

ÁREAS DE MEJORA

Ante este panorama, ¿cuáles son las principales áreas de mejora que debe considerar la sanidad?

David Marco señala que descuidar la seguridad puede traer tres tipos de consecuencias: en el funcionamiento de la organización, consecuencias legales y para pacientes y empleados. "Si sigo construyendo la casa cogiendo piezas de la parte de abajo para crecer en altura cada vez más, pero usando materiales de abajo, llega un momento en que lo de arriba pesa tanto y lo de abajo es tan débil que no va a aguantar". Hay que avanzar, pero de forma segura.

Donde pone el acento Javier Rodríguez es en la videocolaboración: "Ha habido un despliegue acelerado y masivo de las plataformas de colaboración, pero yo creo que hay mucho campo de mejora en dotar de los dispositivos adecuados para que los equipos médicos puedan colaborar a distancia y al final puedan llegar a diagnósticos entre varios especialistas remotamente, realizar por ejemplo ciertas terapias...". A nivel de teleasistencia sí cree que se han dado pasos agigantados y los pacientes están más concienciados, pero tenemos que dar un salto en la calidad de la tecnología que se utiliza para dar esa asistencia.

Por su parte, Álvaro Fernández señala que las principales áreas de mejora en sanidad son cerrar la brecha que se ha producido entre servicios y seguridad por las prisas con las que se hizo la implementación y dotar a las organizaciones de más personal de IT. "Es uno de los ratios de los diferentes sectores donde menos personal de IT tiene más carga tecnológica para gestionar". ■

MÁS INFORMACIÓN

Retos y Soluciones para una Sanidad en cambio

MAURICIO VALBUENA, RESPONSABLE DE INNOVACIÓN,
DIRECCIÓN DE PROYECTOS Y MEJORA CONTINUA DE LOS HOSPITALES
DEL T2 PÚBLICOS BCN-VALLÉS, QUIRÓN SALUD

“Esta situación vivida ha puesto a prueba la adaptabilidad de las organizaciones”

Tras dos años en el foco de la actualidad, directamente impactado por la pandemia, el sector de la Sanidad ha visto que los proyectos de Transformación Digital han tenido que acelerarse para poder estar a la altura de las demandas de profesionales y pacientes. De la situación actual que vive el sector, así como de los retos pendientes, hemos conversado con Mauricio Valbuena, responsable de innovación, Dirección de Proyectos y Mejora Continua de los hospitales del T2 Públicos BCN-Vallés, Quirón Salud.

¿Cómo valora la situación actual de la Sanidad después de estos dos últimos años de pandemia?

Escenarios como el surgido en Wuhan hace 2 años, que carecieron de un adecuado análisis predictivo integrado por parte de los sistemas de vigilancia epidemiológica a nivel mundial, ha puesto en el punto de mira la fragilidad y las grandes carencias de los ecosistemas sanitarios del siglo XXI. Es importante reconocer que nos queda mucho camino por recorrer no solo en materia de igualdad de derechos, sino también de accesibilidad, de igualdad de oportunidades y de mejorar las coberturas; hay que resaltar que la inversión es importante y que las organizaciones sanitarias deben asumir después de esta situación de emergencia no solo un compromiso, sino el reto de transformarse.

La realidad de los pacientes crónicos y los que se encontraban en listas de espera, el frenazo a la investigación científica al concentrarse fundamentalmente en el Covid-19, el impacto de la

pandemia y sus consecuencias en la salud mental, así como la situación que viven los profesionales sanitarios, ha creado una realidad muy compleja para asumir.

Se hace muy necesario no solo el conocimiento en materia de actualidad sino la capacidad de implementar medidas de cambio agiles y con visión holística, que permitan a los lideres de las organizaciones sanitarias agilizar la adaptación a este período de transición y anticiparse a lo que sucederá en los próximos años. Ha de quedar claro que no solo hablamos de avances en el área tecnológica, sino también en lo relacionado a la adopción de nuevos modelos organizacionales innovadores, más dinámicos y eficientes, centrados en las personas pero que utilizan la tecnología como palanca de aceleración, todos nacidos dentro de la filosofía de cambio implícita en la ola de la transformación digital y que indudablemente están cambiando la manera de funcionar y de gestionar la salud por parte de las organizaciones sanitarias.

¿Considera que esta situación pandémica ha provocado un cambio de paradigma en la Sanidad y, debido a esto, se han acelerado los procesos de Transformación Digital e Innovación en el sector?

La situación vivida ha roto de forma inesperada los esquemas en los que estábamos anclados, ha sido la palanca de cambio perfecta para la irrupción en pleno de este nuevo actor que es

> "La situación vivida ha roto de forma inesperada los esquemas en los que estábamos anclados, ha sido la palanca de cambio perfecta para la Transformación Digital"

la transformación digital. Es tal vez por este motivo que la gestión organizacional de esta situación tan excepcional durante la pandemia ha supuesto una serie de desafíos para los distintos actores implicados, así como la necesidad de planificación de cambios adaptativos, a una velocidad sin precedentes dentro y fuera de los ecosistemas sanitarios. Sería difícil hablar de esta gestión sin resaltar el esfuerzo titánico que esto supuso para las áreas TIC, que han tenido que afrontar con urgencia el despliegue de infraestructuras y herramientas tecnológicas a una escala sin precedentes, para hacer frente a la situación generada por el nuevo escenario que planteo la crisis sanitaria. Cambios que han llevado a rediseñar por completo, no solo la manera de prestar servicios en salud, sino la visión de las organizaciones y sus procesos, para garantizar la continuidad de aquellos servicios que pasaron del formato clásico presencial en su gran mayoría, a ser atendidos por canales digitales de la noche a la mañana.

Esta situación de cambio, derivada del afán de la implementación de estrategias de transformación digital, buscando minimizar el impacto de la pandemia en la salud de la población, ha puesto a prueba la adaptabilidad de las organizaciones, que a su vez han puesto el foco en la introducción de cambios tecnológicos, y pueden haber ignorado en algún momento el papel relevante de las personas que conforman los ecosistemas de salud. Las personas son una pieza clave, no solo en la fase de implementación, sino en la consolidación y la evolución del cambio cultural, que pueda garantizar el éxito de este nuevo paradigma que ha traído la transformación digital.

Desde las lecciones aprendidas, ¿cómo considera que deberá evolucionar el sistema sanitario para garantizar una asistencia efectiva y de calidad al paciente? ¿Cuáles deberían ser los pasos siguientes en el camino de digitalización del sector?

Los resultados y las lecciones aprendidas de la pandemia por Sars-Cov-2, en el contexto de su comportamiento impredecible y variable en las distintas olas vividas, muestran un camino claro; lo primero y muy importante es la necesidad de inversión. Y es que ahora es el momento para apostar por la innovación disruptiva, por investigar y desarrollar nuevas tecnologías en

"Asistimos a la era del Dato de calidad como herramienta útil no solo para la medición, sino en la planificación y en la predicción de escenarios fuera de lo común"

materia de atención sanitaria, implantarlas no solo como un eje de crecimiento económico, sino con un serio compromiso social de todos los actores que participan directa o indirectamente en el sector salud.

Un reciente artículo publicado en New Medical Economics comparte cinco recomendaciones que he considerado como líneas estratégicas sobre las cuales evolucionar. Estas líneas, deberían estar muy bien alineadas con las tecnológicas; con la sencilla idea de generar dinámicas que sean favorables y que permitan avanzar en este cambio cultural. Tenerlas en cuenta, garantizará la creación de modelos efectivos que sean capaces de satisfacer las necesidades de las personas integrantes de los sistemas sanitarios y que tengan a su vez un alto impacto positivo sobre el end-user que es el paciente: Formación, visión integral, inversión a largo plazo, políticas público-privadas y comunicación y compromiso.

Por otra parte, es muy necesario que se establezca un foro abierto público-privado, que permita la creación de políticas con líneas estratégicas comunes, bien definidas y que dibujen procesos con métricas claras, que nos permitan trazar dentro de las organizaciones sanitarias la situación real, su evolución y puntos de mejora. Un modelo uniforme y homogéneo que dibuje un engranaje dinámico, que permita la evolución exponencial de los todos los actores involucrados, la creación de alianzas estratégicas con actores tecnológicos que fortalezcan la sostenibilidad y adaptabilidad del modelo al entorno, y que faciliten el camino hacia la verdadera transformación digital que requieren los sistemas de salud hoy.

Es por este motivo que urge trabajar en la búsqueda de modelos innovadores de alto rendimiento, que sean capaces de conectar a todos los actores, que lideren una transformación del sistema con un "scope" holístico, donde se innove en procesos asistenciales, donde se integren nuevas tecnologías y se promueva la salud digital, que faciliten la incorporación de infraestructuras tecnológicas; no solo basados su capacidad de vigilancia y prevención en salud, sino con una alta capacidad para adaptarse y evolucionar según el entorno, que permitan la toma decisiones de alto impacto, en tiempo real, con datos fiables, recopilados de los mismos sistemas sanitarios; pero con una interoperabilidad e interconectividad de alcance global. Modelos que ofrezcan una atención sanitaria adecuada, personalizada, predecible, ágil, segura, y con un alto nivel de calidad tanto para el personal asistencial, como para el paciente.

¿Quieres saber más?

Este texto es un resumen de la entrevista con Mauricio Valbuena. Puedes leer la entrevista completa en este enlace

Desde su punto de vista, ¿cómo puede ayudar la tecnología en la evolución y medición de la calidad de la asistencia sanitaria? ¿Qué herramientas considera que son necesarias para ello?

La importancia que ha adquirido la tecnología en el mundo de la asistencia sanitaria es un hecho indudable; vemos con diferencia cómo este campo se está viendo beneficiado en gran medida por un alto nivel de inversión y por los nuevos avances tecnológicos-científicos. Podríamos decir, sin temor a equivocarnos, que asistimos a la era del Dato de calidad como herramienta útil no solo para la medición, sino en la planificación y en la predicción de escenarios fuera de lo común; sino como una nueva herramienta que juega un papel importantísimo para la

supervivencia y evolución de las organizaciones sanitarias.

Hasta hace muy poco la explotación de los datos se hacía de una forma meramente descriptiva buscando asociar factores de riesgo para plantear acciones preventivas, sobre bases observacionales aplicando estadísticas y probabilidades. Gracias a la irrupción de estas nuevas tecnologías y a su gran capacidad de análisis de grandes volúmenes de datos y prácticamente en tiempo real, es posible construir modelos con un perfil mucho más objetivo y dinámico, con un enfoque predictivo y personalizado, que nos permita abordajes más personalizados y de calidad en materia de diagnóstico, tratamiento y seguimiento de diferentes enfermedades. Los nuevos modelos de análisis predictivo permitirán una anticipación de un modo más real a situaciones como la que se vivió durante esta pandemia.

En este sentido, la aparición de la nueva cultura centrada en los datos, Data Driven, y con herramientas poderosas de análisis, Data Analytics, muestran una alta capacidad para recopilar, clasificar y analizar enormes cantidades de datos generados por dispositivos de todo tipo que son parte del día a día de las personas. El dato de calidad es el actual protagonista del nuevo modelo de atención y gestión de la salud. Gracias a herramientas tecnológicas como la inteligencia artificial y el Big Data, la interpretación y el análisis predictivo de datos está transformando la

> "La inversión es importante y las organizaciones sanitarias deben asumir después de esta situación de emergencia no solo un compromiso, sino el reto de transformarse"

forma de entender y prestar servicios dentro de los ecosistemas sanitarios.

Estamos viviendo un nuevo modelo de asistencia sanitaria... telemedicina, gestión y analítica de datos sensible, securización de infraestructura y accesos ... ¿está la sanidad preparada para soportar estos nuevos modelos? ¿Qué tipo de escenarios de atención al paciente podremos ver que se van a crear en los próximos meses/años?

Digitalmente hablando, la hiperconectividad se ha convertido en un aspecto clave de la transformación de los modelos de negocio y de las organizaciones sanitarias. La innovación y la irrupción en los entornos sanitarios de nuevas tecnologías, los grandes volúmenes de datos generados relativos a las personas plantean muchos interrogantes en materia de seguridad y desde la perspectiva de derechos y libertades. En concreto, en materia de derechos fundamentales como el de la intimidad y la protección de datos personales.

De ahí, que para que este proceso de transformación digital sea confiable y seguro, tiene que ir acompañado del cumplimiento de la normativa aplicable en protección de datos personales, el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (no hay que olvidar que no estamos protegiendo datos sino derechos y libertades de las personas físicas) y por la implementación de políticas de seguridad realmente eficientes y que comprometan al conjunto de las organizaciones sanitarias de modo efectivo. En definitiva, cumplir con esta normativa en materia de privacidad y protección de datos, supondrá una mejora en los resultados y la competitividad de las organizaciones sanitarias; que, además, permitirá aportar seguridad y confianza, favoreciendo la transparencia de las organizaciones y fortaleciendo la relación con los usuarios.

Por otra parte, una de las grandes ventajas que aporta la transformación digital a las organizaciones, es precisamente el buen aprovechamiento de la información obtenida de los datos masivos generados gracias a la incorporación de las nuevas tecnologías a los ecosistemas sanitarios. Es así, como en los últimos años se ha visto un crecimiento en la tendencia de invertir en herramientas de inteligencia empresarial, y

analítica de datos; con la consiguiente mejora de resultados comerciales y el incremento directo de beneficios para las organizaciones.

Por último, y como conclusión, ¿cuáles son, desde el punto de vista de la tecnología y su transformación digital asociada, las principales áreas de mejora que debe abordar la Sanidad? ¿Qué tecnologías emergentes o ya consolidadas van a tener un mayor protagonismo en Sanidad en los próximos años?

En líneas generales, esta pandemia podríamos decir que se ha transformado en un catalizador de grandes avances en materia de salud; el cre-cimiento abrumador de tecnologías digitales; el acceso a datos y a su creciente capacidad de análisis, la cultura de empoderamiento del paciente, su autocuidado y su experiencia son factores que juegan un papel importante en los próximos años y aceleraran aún más la transformación de los ecosistemas sanitarios.

Son ya muchas las herramientas tecnológicas nacidas en los entornos digitales forzados por la pandemia, todo ello ha despertado una respuesta de creciente interés por parte actores externos, que buscan activamente incursionar en el mundo sanitario y establecer un nicho de mercado. Muchas de estas tecnologías en los próximos años, se harán cada vez más presentes, consolidando un nuevo modelo de relación médico-paciente. Modelos basados en servicios no presenciales como punta de lanza; veremos una notable mejora no solo en cuanto al alcance de oportunidades y de cobertura de la atención médica, sino también en la gestión de la salud de las personas. Hecho que por otra parte permitirá a los actores del sistema sanitario un cambio de visión, ya que serán más ágiles y/o eficientes en la prevención y detección de ciertas enfermedades o en el seguimiento mismo del enfermo crónico; todos ellos, aspectos que fueron relegados a un segundo plano debido a la situación de colapso de los servicios sanitarios generado durante la reciente pandemia.

Creo que todas las organizaciones sanitarias deberían tomar conciencia a nivel general, que deben seguir apostando por la transformación digital. Que no es cuestión de digitalizar los procesos para generar dinámicas de cambio. Que el mindset digital se logra con un profundo conocimiento de los procesos y de los circuitos a nivel funcional de la organización. Que también resulta imprescindible adoptar un marco adecuado para el proceso de la transformación digital que vincule a las personas. Marco que implica la adquisición de capacidades digitales adecuadas, sistemas de información interconectados e interoperables, la vinculación de tecnología disruptiva e integrable, además de una financiación que habrá de ser sostenida en el tiempo. Solo entonces se podrá desarrollar una planificación clara de cuáles son las posibilidades de la transformación digital y una visión acertada de cómo y dónde verdaderamente puede ayudar la tecnología.

La Transformación Digital supone así, un paso fundamental para alcanzar una atención alineada con la ola de cambio tecnológico y científico que avanza vertiginosamente y que trae implícito un nuevo modelo de atención en salud. Con una mayor cobertura, atención de predominio virtual, el enfoque predictivo, alta capacidad diagnóstica ligada a un abordaje terapéutico en el marco de la medicina 5P, que serán, en definitiva, aspectos a tener en cuenta para que se contribuya de un modo realista y activo a mejorar la salud de las personas. ■

MAURICIO VALBUENA

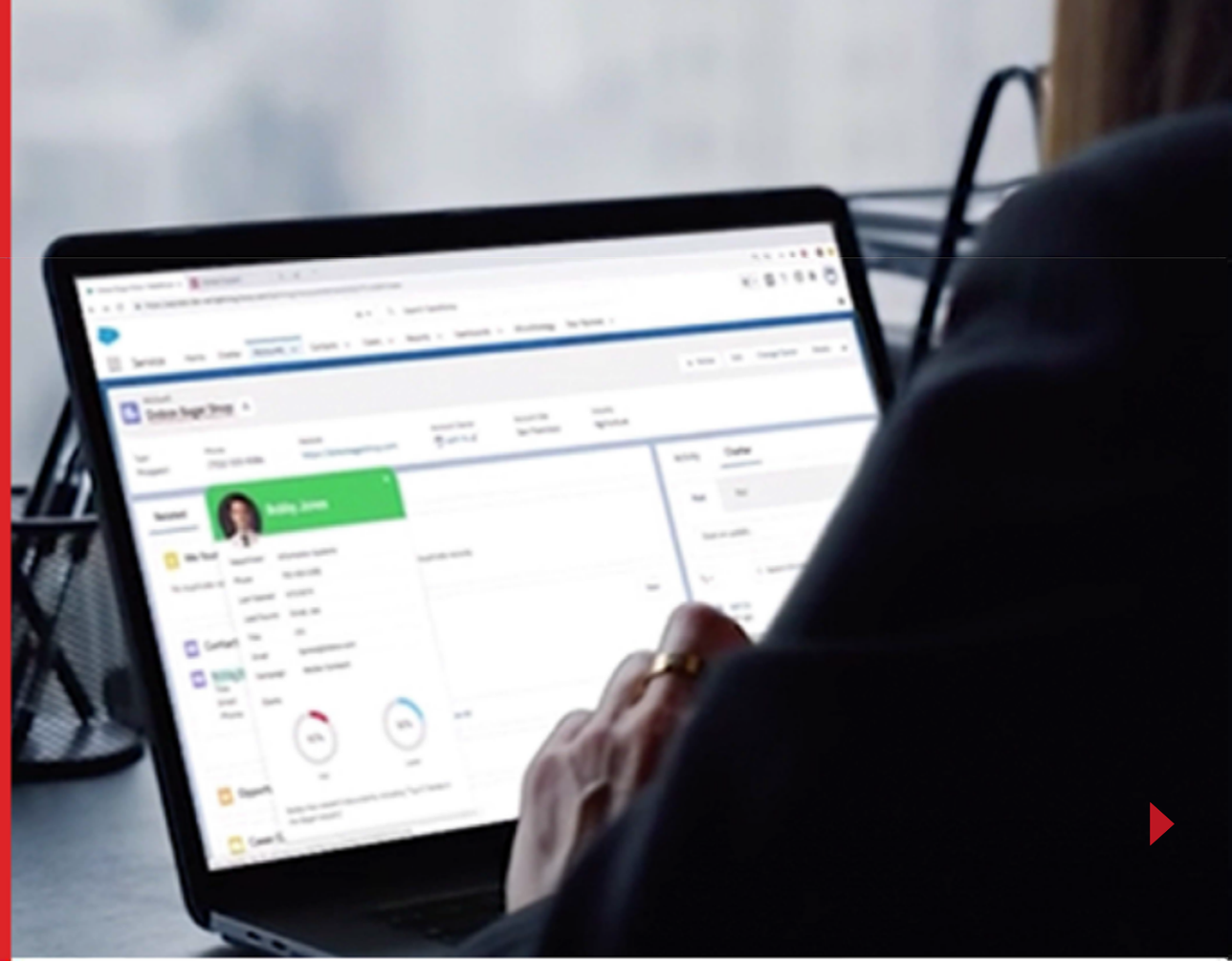
Mauricio Valbuena es médico con Postgrado Ejecutivo en Transformación Digital por IEBS y en Inteligencia Artificial en Salud por la Universidad de Standford.
Actualmente, es responsable de innovación dentro de la Dirección de Proyectos y Mejora Continua de los hospitales del T2 Públicos BCN-Vallés Quiron Salud.

HYPERINTELLIGENCE®

Las respuestas le encontrarán

MicroStrategy®

Intelligence Everywhere



eSalud, clave para la transformación del sector sanitario

JAVIER RODRÍGUEZ,
Senior Key Account Manager de Logitech

La situación de emergencia sanitaria que hemos vivido ha provocado un estado de metamorfosis continua y global, con una urgente necesidad de incluir nuevos modelos de trabajo, de comunicación, de relación o de acceso a servicios primarios, en cualquier momento y lugar.

Bajo estas premisas, la transformación digital se ha convertido en un objetivo inaplazable para cualquier organización y los centros de salud, hospitales y profesionales sanitarios no son ajenos a estos cambios. Y es que, durante la pandemia se han habilitado toda una serie de recursos y herramientas tecnológicas, así como servicios digitales para abordar la transformación digital del sector sanitario de forma acelerada, habilitando las reuniones entre equipos y centros, la discusión de diagnósticos, formaciones o convenciones. Todo ello, no solo internamente entre comunidad médica sino también con pacientes, incorporando la telemedicina para seguimientos, terapias o atención primaria, entre otros usos.

Actualmente estamos en la línea de salida del cambio en el ecosistema de salud que sitúe más cerca de la prevención de enfermedades, que sea más proactivo y que, al final, mejore la calidad de vida de los pacientes, facilitando su acceso y contacto con el sistema sanitario, y asegurando una intervención inmediata, en caso necesario, así como la desaturación de los centros de salud convencionales.

Las tecnologías para el sector salud suponen, además, la aportación de un valor añadido respecto a la cualificación de los sanitarios en el ámbito digital, una inversión a futuro que posiciona España como país referente. Según confirmamos en septiembre del año pasado en un análisis global realizado junto a Scalent sobre la opinión que merecía la atención sanitaria mediante vídeo, la mayoría de sanitarios exponían su preocupación por esta tendencia digital, pues solicitaban tecnologías intuitivas, conexión estable, aparatos de uso sencillo y con calidad de imagen y sonido comparable a lo que podría ser esa misma consulta si se realizara de forma presencial.

Entre 2020 y 2021, equipamos más de 700 centros sanitarios de la capital con sistemas de video colaboración de última generación y liderамos el proceso de digitalización de hasta 100 salas del Hospital Clínic de Barcelona con el fin de facilitar el trabajo colaborativo y el creciente servicio de telesalud al que ya se adscriben más del 57% de los pacientes en todo el mundo. En esta línea, también hemos llevado a cabo un proyecto de eConsulta para dermatología que permite captar imagen y vídeo de las lesiones de los pacientes en alta resolución desde los servicios de atención primaria para, posteriormente, compartir esos recursos gráficos con un especialista. Agilizando, de este modo, la derivación al especialista si éste lo considera oportuno.

Cada avance y cada proyecto que iniciamos comparten siempre un objetivo inamovible, que es el de proveer la mayor cantidad posible de facilidades a las personas para minimizar cualquier

obstáculo existente. Por eso, la digitalización en el sector sanitario debería dividir sus esfuerzos en cuatro ámbitos de igual relevancia: mejorar la calidad de vida de la sociedad, cuidar la experiencia del paciente, motivar la formación de los profesionales sanitarios en cuanto a lo digital y aumentar la eficiencia de los sistemas a través de su modernización.

En este sentido, la tecnología se ha posicionado como aliada indiscutible en el proceso. Propiciar la autonomía de los pacientes al implicarse en la gestión activa de su estado de salud, facilitar el acceso a historiales y datos médicos desde cualquier dispositivo, aumentar la rapidez y disponibilidad para las citas, agilizar los trámites administrativos, medir datos o celebrar formaciones y debates online son solo algunos de los servicios que ofrece la video colaboración.

Para ello es prioritaria la transformación del sistema sanitario, de forma progresiva, segura y efectiva, para habilitar experiencias personalizadas que contribuyan a la mejora de la salud de toda la población, con las innovadoras tecnologías de telemedicina que tenemos a nuestra disposición tanto para modernizar la relación médico-paciente como los métodos de comunicación entre centros o profesionales sanitarios. Es decir, una transformación a través de la tecnología que permita derribar fronteras y abrir puentes en la relación médico-paciente. ■

JAVIER RODRÍGUEZ, SENIOR KEY ACCOUNT MANAGER DE LOGITECH

Nuevos modelos de asistencia sanitaria

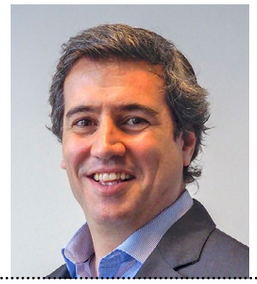
La pandemia ha transformado todos los sectores, incluido el sanitario, implicando la irrupción de nuevos modelos de asistencia sanitaria, entre los que destacan los entornos colaborativos y la telemedicina como tecnología emergente.

Según McKinsey, la utilización de la telesalud a diciembre de 2021 era 38 veces mayor que justo antes de la pandemia. Javier Rodríguez, Senior Key Account Manager de Logitech, cree que ha supuesto una aceleración de todos los procesos y ha provocado la creación de nuevos modelos de asistencia sanitaria remota, debido a los confinamientos y a la necesidad de evitar contagios. A pesar de ello, aún hay margen de mejora en cuanto a la calidad y la experiencia que se le ofrece al paciente. Estas soluciones deben contar con tres requisitos básicos: seguridad, integración y facilidad de uso.

Las soluciones Logitech se utilizan en todo tipo de áreas en el sector sanitario, desde la comunicación interna de los equipos de trabajo a la atención a distancia del paciente para tener nuevas vías de interacción. La compañía ofrece soluciones de audio, video y control que funcionan en cualquier plataforma de videocolaboración en la nube y ofrecen una buena experiencia tanto en el puesto de trabajo del personal médico como en las salas de reunión.

La sanidad y el mundo del dato

FERNANDO GUTIÉRREZ,
Account Executive de MicroStrategy



Hoy en día, la información es un activo fundamental de las empresas y la sanidad no es una excepción.

La sanidad maneja uno de los "productos" más preciados por todos, la salud.

El objetivo principal del sistema sanitario es mejorar la salud y por tanto la calidad de vida de la población. Existen también otros objetivos como facilitar el acceso a los servicios de salud, mejorar la calidad y satisfacción del ciudadano, incrementar la eficiencia y efectividad de la infraestructura hospitalaria/centros y un incremento eficiente de los presupuestos.

Como sucede en otras industrias, ese deseo de incremento en diferentes aspectos necesita de nuevas vías más allá de las vías tradicionales. El uso del dato junto con nuevas tecnologías puede permitir al sistema sanitario alcanzar los objetivos anteriormente mencionados.

Una mejora en la gestión del dato del paciente, de los centros de atención y de los procesos tiene una repercusión y un beneficio directo en la salud del ciudadano.

Por tanto, el dato se convierte en un activo fundamental que debe ser utilizado para la obtención de información y aportar ese valor diferencial al ciudadano.

No se trata exclusivamente de ver la información histórica del paciente en el momento de acudir a la consulta y ser reactivo, se trata de ser proactivo para obtener una sanidad preventiva. Las capacidades de inteligencia artificial y machine learning en la sanidad nos permiten poder ofertar una sanidad preventiva que evite problemas mayores en la salud de los pacientes, que permitan una mejor planificación y utilización de los recursos.

Otro de los aspectos que hacen que el dato sea crítico en el sistema sanitario, es el aspecto económico. Un análisis de la actividad operacional del sistema sanitario permitirá un incremento de la eficacia y de la eficiencia de los procesos, lo cual repercutirá directamente en un uso eficiente del presupuesto e indirectamente en la satisfacción del ciudadano al percibir una mejora en la calidad de los procesos, disponer de los medios necesarios y una organización más eficiente.

En los periodos de estrés se pone a prueba todo; los sistemas, los protocolos... se ve de manera clara que cosas son realmente necesarias, que cosas funcionan y que áreas son susceptibles de mejora.

Es por eso que el sistema sanitario se encuentra como muchas empresas y sectores en un proceso de transformación digital, muy encaminado a la calidad del dato y al gobierno del dato, pero también en la analítica y explotación del dato para la obtención de información.

Se podrían mencionar 3 áreas de mejora en lo que al mundo del dato respecta:

1. Uno de los objetivos que se busca con el gobierno y la calidad del dato es tener una visión del paciente 360º, necesidad incrementada con la incorporación de nuevos canales como la teleasistencia.

2. Incorporación de inteligencia artificial y machine learning para una sanidad preventiva y mejora de la operativa de los sistemas sanitarios.

3. Un área donde hay claro margen de mejora es en como facilitar el acceso a la informa-

ción para todo el personal involucrado en la operativa de un hospital o centro; ya personal sanitario, como personal de mantenimiento encargado de la gestión de las maquinas... para ayudarles en la toma de decisiones.

Hoy en día la gran mayoría de decisiones que se toman no van sustentadas en el dato. Existen 3 motivos principales, el dato se encuentra demasiado disperso y no hay tiempo, el segundo motivo es la falta de conocimiento en como acceder a todos esos sistemas y el tercer motivo es utilizar la experiencia

Es por tanto que el acceso a la información debe ser sencillo, rápido, intuitivo y multicanal. De esta manera se asegura que todo el personal dispone esté donde esté de la información relevante para la toma de decisiones. Como sucede en el resto de sectores, la sanidad no podría ser diferente, la tendencia actual es la de convertirse en un sector Data Driven con el menor coste y tiempo posible, es por ello que muchas compañías líderes han recurrido a HyperIntelligence como solución. ■

FERNANDO GUTIÉRREZ, ACCOUNT EXECUTIVE DE MICROSTRATEGY

El dato, fundamental en el sector sanitario

La situación pandémica ha implicado un nuevo modelo de la gestión del dato, tanto en su análisis como en su tratamiento, fundamentalmente dada la sensibilidad de muchos de ellos en un entorno tan específico como el sanitario.

El concepto data driven es completamente aplicable al sector sanitario. Para Fernando Gutiérrez, Account Executive de MicroStrategy, el poder disponer de datos para poder tomar decisiones y mejorar los tiempos de respuesta tiene un impacto en la sociedad brutal. El dato es fundamental para la salud del paciente, tanto en aspectos directamente relacionados con él, como en la gestión y la operación de los centros, que al final también recae en su bienestar. Además, la correcta gestión del dato ayuda a la medicina preventiva.

El objetivo de MicroStrategy es llevar de manera rápida y sencilla esa información recopilada a cualquier persona que en su trabajo requiera tomar una decisión y que pueda resultarle útil, pero de forma completamente segura. También trabaja en proyectos 360 y apuesta por una hiperpersonalización de la teleasistencia, ofreciendo una visión global de cada caso a través del dato. Además, tecnologías como la inteligencia artificial o el machine learning sirven para intentar detectar y ser proactivo ante posibles enfermedades.

El sector sanitario, protección crítica de sus datos

PEDRO DAVID MARCO,
CEO y Fundador de Iberlayer

El sector sanitario ha estado sometido a grandes tensiones durante los últimos dos años. Por las consecuencias de la pandemia de COVID 19, clínicas, centros de atención primaria, hospitales, farmacias y laboratorios farmacéuticos están jugando un papel crítico, y a esta presión se suma el hecho de que este sector, se ha convertido en un objetivo prioritario para los ciberdelincuentes.

La criticidad de los datos que manejan: hospitales y clínicas, con los registros médicos de cada paciente, y laboratorios farmacéuticos, con la documentación confidencial sobre vacunas o medicamentos; o la importancia de asegurar -en todo momento- la disponibilidad de los sistemas de información y la conexión ininterrumpida de los diferentes dispositivos y máquinas de salud, han actuado en su contra.

EL CORREO ELECTRÓNICO EN EL PUNTO DE MIRA

A esta situación se ha unido también el hecho de que el correo electrónico, uno de los servicios más antiguos de Internet y, en el caso del sector sanitario, herramienta crítica de los sistemas de información, se ha convertido en un arma de ataque para los ciberdelincuentes.

Cada vez más, entre todos los correos legítimos que circulan por Internet, se da un mayor número de mensajes SPAM, de correos con virus, troyanos, ransomware o de tipo phishing, en un intento por conseguir información sensible de carácter personal para realizar suplantación de identidad. Esta forma de comunicación no solicitada e ilícita está provocando serios problemas a las organizaciones y usuarios en cuanto a su seguridad y al consumo de recursos informáticos y ancho de banda de comunicaciones.

Las estadísticas de los tres últimos meses en el sector sanitario, al que Iberlayer proporciona su servicio de seguridad y anti-fraude para el correo electrónico en algunas compañías, muestran que en torno al 60% de los correos recibidos son SPAM. Aún más peligroso y preocupante es el hecho de que un 10% son campañas de phishing (en todas sus variantes, incluyendo intentos de fraude) mientras que otro 10% son correos con adjuntos con virus (que descargan ransomware en su mayoría).

El ransomware es un tipo de malware por el que un ciberdelincuente se lucra económicamente extorsionando a compañías a las que amenaza básicamente de dos modos posibles:

1. Cifrando todos sus datos y pidiendo un dinero de “rescate” a cambio de la clave de descifrado

2. Sacando fuera de la compañía enormes cantidades de datos internos y amenazando con hacerlos públicos si no se paga un “rescate”. A menudo, esta modalidad va acompañada de avisos a los propietarios de esos datos: pacientes, clientes, proveedores a los que se advierte que, de no efectuarse el pago, sus datos se harán públicos.

A este respecto aclarar que, en contra de lo que pueda parecer, no existe ninguna ga-

rantía de que, una vez ejecutado el pago, los datos perdidos sean recuperados o sigan permaneciendo secretos.

El sector sanitario es, por desgracia, uno de los objetivos del ransomware, y el correo electrónico es, sin lugar a dudas, el principal vector de entrada al ser los usuarios el eslabón de más débil de la cadena y el más fácil de engañar.

Otra de las amenazas más graves para el sector sanitario es el llamado Fraude del CEO, el cual es un tipo de engaño (y un posible delito a nivel legal) donde los cibercriminales crean cuentas de correo o dominios fraudulentos para hacerse pasar por ejecutivos de la organización, normalmente directores generales, o consejeros delegados, entre otros altos ejecutivos.

El fin último es intentar engañar a un empleado -con poderes para transferir dinero- para que lleve a cabo transferencias bancarias urgentes. Estos correos electrónicos no contienen malware malicioso, ni URL sospechosas; están completamente limpios desde el punto de vista de la seguridad. Por ello, es necesario utilizar una tecnología y un conocimiento especial de las técnicas empleadas por los ciberdelincuentes, para detectarlos y bloquearlos. Asimismo, es preciso poner una capa por encima de esta tecnología con un servicio de aviso personalizado, utilizando canales (para alertar a las posibles víctimas) distintos al del propio correo electrónico. ■

PEDRO DAVID MARCO, CEO DE IBERLAYER

Seguridad para el correo electrónico como servicio

La pandemia del coronavirus ha supuesto un verdadero reto para el sistema sanitario español, pero no solo a pie de campo, sino que sus sistemas informáticos también han visto cómo se han multiplicado los ciberataques amenazando la seguridad de datos muy sensibles, sobre todo a través del correo electrónico.

La forma más fácil de llegar al corazón de las empresas son los usuarios. Dado que la manera más directa de impactar al usuario es mediante el correo electrónico, se ha convertido en uno de los principales vectores de ataque. Pedro David Marco, CEO de Iberlayer, señala que no muchos directivos son conscientes del daño que le puede ocasionar a su compañía un ciberataque, sobre todo en sectores como el sanitario que no cuentan con departamentos específicos dedicados a ello.

Por esta razón Iberlayer ofrece la seguridad del correo como un servicio, lo que permite al cliente abstraerse de esa capa y tener la mayor protección que existe en el mercado sin necesidad de contar con especialistas in house. Además, sus soluciones de seguridad para el correo electrónico realizan un cifrado por defecto, de tal manera que todo el tráfico del cliente pasa a estar protegido.

El sector sanitario tiene graves problemas para detener el ransomware.

El 65% de los ciberataques consiguieron cifrar datos

Sophos Managed Threat Response

Tome medidas contra las ciberamenazas
Un servicio totalmente gestionado con funciones de búsqueda, detección y respuesta ante amenazas las 24 horas.

www.sophos.com/es-es/

SOPHOS
Cybersecurity delivered.

Los atacantes tienen una mayor tasa de éxito en el cifrado de datos sanitarios

JAVIER DONOSO,
Sales Engineer, Sophos

Según El estado del ransomware en la sanidad 2021 de Sophos, entre las organizaciones sanitarias afectadas por el ransomware, el 65% afirmó que sus datos estaban cifrados, en comparación con la media intersectorial del 54%. A nivel mundial, el 39% de las organizaciones fueron capaces de detener el ataque antes de que se cifraran los datos, pero sólo el 28% en el sector sanitario. Esta menor capacidad para detener un ataque puede ser un reflejo de los retos financieros y de recursos a los que se enfrenta el sector sanitario, en parte debido a la reticencia a desviar fondos a la ciberseguridad que podrían utilizarse para la atención de primera línea a los pacientes.

Para que los organismos sanitarios ganen terreno a las nuevas y evolucionadas ciberamenazas, deben seguir ciertas estrategias clave de seguridad para protegerse:

1. Adoptar el modelo de seguridad de confianza cero o Zero Trust. Un informe, muestra que en el sector sanitario hay más infracciones causadas por amenazas internas que externas. Esto puede atribuirse a un error humano, a la falta de supervisión en ciberseguridad o al abuso intencionado del privilegio de acceso a datos y sistemas confidenciales.

Al implementar un enfoque de confianza cero, las organizaciones de salud pueden introducir controles granulares en el tráfico de la red. Esto elimina la oportunidad de que los atacantes y los usuarios deshonestos realicen acciones malintencionadas y obtengan acceso a información personal confidencial de salud mientras permanecen fuera de todas sospecha.

2. Mejorar la ciberseguridad contra los ataques de ransomware. Más de un tercio de las organizaciones sanitarias (34%) fueron atacadas por ransomware el año pasado. Podemos afirmar, que el ransomware es un arma devastadora en manos de los ciberdelincuentes que tienen como objetivo el sector sanitario.

Estos ataques han detenido operaciones sanitarias, han paralizado los dispositivos y sistemas médicos conectados y han cifrado los registros para que el personal sanitario no pueda acceder a ellos. Sophos ofrece una seguridad líder en ransomware con Intercept X Advanced with XDR, la única solución XDR del sector que sincroniza la protección nativa de endpoints, servidores, firewalls, correo electrónico, infraestructura en la nube y M365.

3. Superar la escasez de mano de obra cualificada. La falta de personal con los conocimientos y la experiencia adecuados en materia de ciberseguridad es uno de los principales desafíos para los proveedores de servicios de salud.

Para las organizaciones sanitarias que carecen de recursos en ciberseguridad, Sophos ofrece el servicio de Managed Threat Response (MTR). Este servicio brinda una supervisión eficaz y una evaluación continua de los riesgos gracias al equipo de expertos dedicado las 24 horas del día, los 7 días de la semana. Nuestra solución va más allá de las simples alertas, ya que proporciona una respuesta contra las amenazas, asegurando que el riesgo se identifica, se contiene.

4. Cubrir los puntos ciegos en sus esfuerzos de transformación digital. Las transacciones de información entre los pacientes, los cuidadores, las agencias de seguros y otras partes interesadas deben ser fluidas y seguras. Las redes SD-WAN, con su arquitectura flexible, ha surgido como una muy buena alternativa entre las organizaciones de salud para cumplir con estos requisitos.

Es crucial proporcionar un acceso fiable y seguro a los datos clasificados de la asistencia sanitaria en un momento en que muchos hospitales están adoptando nuevas tecnologías como los dispositivos médicos conectados a la red, la telesalud y aplicaciones médicas como los sistemas de comunicación y archivo de imágenes (PACS).

Sophos, con Sophos Firewall y SD-RED, hace posible conseguir una conectividad SD-WAN en línea con sus objetivos de seguridad y continuidad.

5. Promover la concienciación en ciberseguridad. Otra preocupación importante para el sector sanitario es la falta de formación sobre ciberseguridad y la escasa conciencia sobre la privacidad de los datos entre los empleados.

Es importante tener una cultura de ciberseguridad adecuada para ayudar a reducir la alta susceptibilidad de la sanidad a una amplia gama de sofisticados ciberataques.

Con Sophos Phish Threat, los equipos de seguridad informática pueden simular ataques de phishing con sólo unos pocos clics, y proporcionar formación automatizada e in situ a los empleados de atención sanitaria según sus necesidades. ■

ÁLVARO FERNÁNDEZ, ENTERPRISE ACCOUNT EXECUTIVE DE SOPHOS

Prevención, detección y respuesta

En los últimos dos años los ciberataques hacia el entorno sanitario se han visto multiplicados como consecuencia de la pandemia, con infraestructuras, accesos y datos como principales objetivos. El ransomware es el más notorio, pero detrás de esos ataques hay mucho más.

Muchas veces se entiende el ransomware como un ataque aislado, pero realmente se trata de la última fase de un ataque, antes de aflorar han pasado muchas otras cosas. Como explica Álvaro Fernández, Enterprise Account Executive de Sophos, una vez dentro el atacante va a intentar pasar inadvertido y filtrar información, lo que supone un gran riesgo para un sector como el sanitario, y será después cuando preparará el entorno eliminando las copias de seguridad existentes para poder liberar el ransomware sin problemas y salir a la luz.

Para hacer frente a estos problemas es necesario contar con un plan de respuesta ante este tipo de incidentes. Sophos Rapid response es un servicio específicamente diseñado para este tipo de eventos que cuenta con una fase de neutralización del atacante y otra de monitorización para solucionar cualquier tipo de incidente. La seguridad del entorno sanitario se debe basar en 3 claves: prevención, detección y respuesta.

El impacto de TLStorm

en la seguridad de las organizaciones médicas y sanitarias

OSCAR MIRANDA,
CTO for Healthcare, Armis

TLStorm son un grupo de tres vulnerabilidades críticas, descubiertas por Armis, que afectan a los Smart-UPS de APC. Dos de ellas son vulnerabilidades de ejecución remota de código (RCE) en el código que maneja la conexión a la nube, lo que hace que estas vulnerabilidades sean explotables a través de Internet. La tercera vulnerabilidad es un fallo de diseño, en el que las actualizaciones de firmware de la mayoría de los dispositivos Smart-UPS no están correctamente firmadas o validadas, lo que permite a un atacante cargar firmware malicioso de forma remota y sin validación. Un ataque a estos dispositivos podría llegar a traer consecuencias catastróficas, ya que los Smart-UPS de APC se encuentran en infraestructuras críticas como hospitales, centros de datos e instalaciones industriales.

Estas tres vulnerabilidades de día cero, acuñadas como TLStorm, exponen a más de 20 millones de dispositivos en todo el mundo y podrían permitir a atacantes eludir las funciones de seguridad y controlar o dañar remotamente dispositivos médicos, industriales y enterprise críticos para el funcionamiento de cualquier organización. Datos obtenidos por el equipo de investigadores de Armis, muestran que 8 de cada 10 organizaciones podrían ser vulnerables a TLStorm.

En el sector de la sanidad, esta amenaza pone de manifiesto los riesgos que entrañan los dispositivos médicos conectados y la importancia de la seguridad de los mismos. Con activos como los dispositivos SAI convirtiéndose en un objetivo para los actores maliciosos, es más importante que nunca tener una visibilidad completa de todos los dispositivos conectados a la red, junto con la capacidad de supervisar su comportamiento e identificar los intentos de explotación de cualquier fallo de seguridad, como TLStorm.

Alrededor del 91% de los clientes de Armis del sector sanitario y médico de todo el mundo utilizan algún tipo de SAI, y de ellos el 76% tienen modelos de SAI identificados como vulnerables a TLStorm. Los clientes de la compañía pueden ver inmediatamente los dispositivos vulnerables y parchearlos, pero el alto número de posibles afectados destaca los riesgos potenciales para aquellos que no pueden hacerlo.

El ecosistema de dispositivos en empresas sanitarias va más allá de los dispositivos médicos. Los SAI se utilizan no sólo en los centros de datos sino dentro de los hospitales y clínicas, por lo que un ataque podría afectar significativamente los cuidados y el trato con los pacientes. En resumen, cualquier evento de seguridad que afecte a los dispositivos médicos conectados puede causar una interrupción considerable en la prestación de servicios sanitarios y afectar a la seguridad de los pacientes.

Los hospitales deben identificar qué dispositivos ayudan al flujo de trabajo clínico, aparte de los dispositivos médicos clásicos, y cuáles están conectados a sistemas SAI vulnerables. Solo a través de la identificación y monitoreo continuo de los dispositivos un hospital puede mitigar o remediar el riesgo creado por estos sistemas SAI rápidamente.

Aunque las ventajas de las nuevas tecnologías son evidentes, cada dispositivo médico conecta-

do crea un nuevo objetivo para los malos actores y debe utilizarse en un entorno seguro, con supervisión continua de su actividad.

El descubrimiento de las vulnerabilidades TLStorm subraya la importancia de tener un inventario de dispositivos en entornos como el médico, y de controlar la actividad de todos aquellos dispositivos responsables de mantener la energía y las operaciones críticas en funcionamiento. El uso de dispositivos médicos conectados supone una gran oportunidad para mejorar la atención al paciente en centros hospitalarios y sanitarios, pero los profesionales de la salud deben entender que también crea oportunidades de entrada para actores maliciosos.

Contar con un plan de ciberseguridad para los dispositivos médicos, es fundamental para cualquier organización que utilice el Internet de las cosas médicas, o IoMT. La Agencia de Ciberseguridad de la Unión Europea (ENISA) y la FDA ofrecen directrices para ayudar a los equipos informáticos (TI) a gestionar la seguridad de los dispositivos médicos. Ambas son un buen punto de partida para garantizar la seguridad del IoMT.

La visibilidad es fundamental para que las organizaciones sanitarias se aseguren de que todos los dispositivos están supervisados y protegidos. En la realidad hiperconectada en la que vivimos, tener visibilidad completa y a tiempo real garantiza una protección holística. ■

VESKU TURTIA, REGIONAL DIRECTOR ESPAÑA Y PORTUGAL DE ARMIS

Monitorización continua sin agentes y de forma pasiva

La situación de pandemia vivida en los últimos años ha implicado un nuevo paradigma para sectores como el sanitario, así como la aceleración de nuevos modelos tecnológicos, donde el componente de la ciberseguridad de los diferentes assets juega un papel muy importante.

La aceleración de la digitalización en el sector sanitario es un hecho desde el inicio de la pandemia, lo que ha implicado ciertos retos para los players del sector. Para Vesku Turtia, Regional Director España y Portugal de Armis, el principal reto es que las empresas logren entender qué es todo lo que tienen integrado en su red, para poder hacer políticas de ciberseguridad y proteger los assets de cada centro hospitalario. Además, es muy importante hacer una monitorización continua, sin agentes y de una forma pasiva, para no interferir en posibles procesos hospitalarios importantes.

Armis ha traído al mercado una plataforma que engloba precisamente todas estas cuestiones: inventario, visibilidad, monitorización continua, sin agentes y de forma pasiva, que se integra de forma perfecta con los sistemas del cliente. Además, cuentan con una base de datos en la nube de más de 2 billones de dispositivos distintos perfilados en 20 millones de perfiles, que permite compartir información para estar a la última en protección.

El riesgo de las infraestructuras sanitarias frente a diversos vectores de ataque

BORJA PÉREZ,
Country Manager
Stormshield Iberia

Cada vez más digital e interconectado, el sector sanitario, con los hospitales al frente, lleva tiempo siendo objetivo de ciberataques. La sensibilidad que encierra, lo han convertido en un blanco codiciado para los ciberdelincuentes, quienes lanzan sus amenazas contra estas entidades. No en vano, el sanitario fue, según la Agencia de la Unión Europea para la Ciberseguridad, ENISA, el cuarto sector más atacado durante 2020, registrando 143 incidentes , lo que supone un 47% más que el año anterior. Se trata por tanto de un sector expuesto en el que, además, y a diferencia de lo que ocurría en el pasado, no se enfrenta a un factor de riesgo uniforme, sino que los peligros, cada vez más, proceden de diferentes vectores: redes, software, físicos y humanos.

EN EL CORAZÓN DEL SISTEMA

El rendimiento y la disponibilidad de las redes informáticas de los sistemas de salud son muy importantes, dado que la vida de los pacientes a menudo depende de la información que permiten intercambiar.

Por tanto, salvaguardar esa información confidencial y vital es un tema prioritario, igual que garantizar la disponibilidad de los servicios. La salud vive al ritmo de las emergencias. Por lo tanto, requiere una reacción rápida en caso de incidente, en relación con equipos biomédicos, Gestión Técnica de Edificios (BMS) o Gestión Técnica Centralizada (CTM) del hospital. Estas intervenciones se pueden facilitar proporcionando acceso remoto seguro a técnicos o proveedores externos a través de VPN nómadas, SSL o IPSec y autenticando a los usuarios a través de flujos de red. Dos medidas que también son útiles para fortalecer el mantenimiento a distancia y el desarrollo de la telemedicina.

UN ATAQUE CONTRA EL CEREBRO

Los programas informáticos prestan innumerables servicios en los hospitales, tanto para la gestión interna como externa de la organización. Sin embargo, por su propia naturaleza, también pueden presentar puntos débiles, como lagunas o una obsolescencia, que pueden ser aprovechados por los ciberdelincuentes para acceder a los equipos médicos, informáticos o, incluso a los datos de los pacientes o a las instalaciones sensibles.

Para prevenir los ciberataques de software, es esencial la concienciación de los equipos humanos, así como el cumplimiento de las mejores prácticas en este ámbito: limitar el acceso a la red de las aplicaciones al mínimo, realizar una auditoría del sistema, endurecer las configuraciones y realizar copias de seguridad sin conexión.

TRABAJANDO SOBRE EL TERRENO

Lejos del cliché del ciberdelincuente, aislado tras su pantalla a kilómetros de su víctima, algunos se acercan lo más posible a su objetivo. Su técnica consiste en atacar directamente los equipos hospitalarios, ya sean informáticos, médicos u operativos, y explotar sus vulnerabilidades. Para ello el ciberdelincuente accede físicamente al equipo en cuestión, y se conecta a él para interrumpir su funcionamiento. Tras ello, su impacto puede ser múltiple, desde el sabotaje de la máquina hasta la

alteración -o incluso el robo- de datos sanitarios.

Para protegerse de estos ataques, es necesario salvaguardar las máquinas, como las estaciones de trabajo. Por lo tanto, se recomienda el control de acceso, la gestión de los dispositivos externos e incluso el análisis del comportamiento. Esto puede lograrse con la creación de estaciones blancas que actúan como una descontaminación de llaves USB. Como último recurso, la segmentación de la red para limitar la propagación de la infección, en caso de que esta se produjera.

RIESGO HUMANO, PRINCIPAL PREOCUPACIÓN

Además de los riesgos tecnológicos es importante tener en cuenta los asociados al ser humano, sobre todo con el uso todavía muy extendido de las memorias USB en entornos TI y OT. Por ello, es importante endurecer los puestos de control y supervisión mediante el establecimiento de soluciones de listas blancas o de análisis de dispositivos de almacenamiento, para rechazar cualquier uso de un perfil no autorizado, pero también concienciar a los trabajadores sanitarios de todos los riesgos cibernéticos para evitar cualquier error o acción involuntaria que pueda poner en peligro los datos o la infraestructura.

Adicionalmente, y además de trabajar en esta concienciación, dado que los ataques son cada vez más dirigidos y sofisticados, es fundamental ofrecer soluciones que no dependan del conocimiento que el usuario pueda tener en ciberseguridad. ■

BORJA PÉREZ, COUNTRY MANAGER DE STORMSHIELD

El cifrado de datos, imprescindible

La seguridad del sector sanitario se ha cuestionado a raíz de la pandemia, dado que se ha convertido en uno de los entornos más amenazados por los ciberdelincuentes.

El intercambio de datos sensibles entre distintas áreas del sistema sanitario, como laboratorios, hospitales, clínicas, es continuo, pero no está debidamente securizado. Así lo pone de manifiesto Borja Pérez, Country Manager de Stormshield, señalando que los datos no se están almacenando adecuadamente y el intercambio muchas veces no se hace con las medidas de seguridad suficientes. A pesar de ello, en su opinión los CISOs son conscientes del problema, pero les faltan recursos.

Para Stormshield es fundamental tener todos los datos cifrados y salvaguardados de manera segura, de manera que si se produce una filtración de datos, no se pueda sacar ninguna información útil de esos documentos filtrados. La compañía basa su propuesta en tres principios: Securización de los datos mediante cifrado de documentos y correo, protección del puesto de trabajo; y segmentación de las redes y securización de cada uno de los servicios que se estén dando en el entorno sanitario.

STORMSHIELD

La opción europea en ciberseguridad

Su socio de confianza para proteger **infraestructuras hospitalarias**

www.stormshield.com

Visibilidad, clave de la seguridad en el entorno sanitario

En el sector sanitario, Armis permite a las organizaciones utilizar la visibilidad en su ecosistema de dispositivos médicos e informáticos, para identificar, evaluar y asegurarse ante riesgos cibernéticos, a la vez que realizar mejoras operativas significativas.

Esta aproximación ofrece un valor clínico y un valor operacional. En el caso del primero, destaca el manejo y seguimiento de inventario; identificar y localizar dispositivos médicos no conectados a la red; alertar sobre dispositivos médicos que abandonen el recinto hospitalario y monitorización del comportamiento de dispositivos en busca de indicadores de mal funcionamiento. Asimismo, sobresale la utilización dirigida hacia la eficacia clínica (tiempos de espera y satisfacción del paciente); mejorar la monitorización de dispositivos de alto valor para controlar tiempos de inactividad y problemas operacionales; identificar tiempos óptimos para el mantenimiento de los dispositivos y alertar de anomalías o usos incorrectos de dispositivos para el cuidado de pacientes. Por último, mejoras de seguridad y calidad, y realizar informes trimestrales con seguimiento de medidas de los órganos reguladores.

Desde el punto de vista operacional, destaca el coste de gestión; asistir a operaciones para realizar previsiones financieras; mostrar dispositivos perdidos para prevenir la compra excesiva; y ayudar a a tomar decisiones de compra informadas al adquirir inventario adicional. Igualmente, ahorro en contratos de mantenimiento, al mostrar datos de utilización y riesgo para optimizar los Acuerdos de Nivel de Servicio (SLA) y los contratos de mantenimiento relacionados con dispositivos médicos y sistema de gestión de edificios. Finalmente, integración con inversiones existentes en TI y Seguridad de la Información como ServiceNow, Biomed CMMS o CMDB, para una mayor visibilidad y precisión de los activos; realización de informes en tiempo real sobre los usos de li-

cencias; simplificación de la implementación de soluciones de Control de Acceso a Red (NAC) (Cisco ISE); aumento de las capacidades de otras soluciones y de administración de vulnerabilidades para dispositivos no gestionados y puntos ciegos de redes; mejora de la visibilidad y alerta en la Gestión de Información y Eventos de Seguridad (SIEM); e identificación de dispositivos perdidos durante proyectos de migración de tecnología – proyectos de migración de servidores y proyectos de renovación de infraestructuras inalámbricas.

CIBERSEGURIDAD Y CONTINUIDAD DE LAS OPERACIONES

Con la Auditoría y Cumplimiento de normativas se crean informes cuatrimestrales de requerimientos regulatorios; cuadros de mando dinámicos en tiempo real para identificar dispositivos que incumplen la normativa; fuentes de información absoluta para la identificación y orquestación de dispositivos; e identificación de riesgos de terceras partes relacionados con el comportamiento de los dispositivos.

Mientras, con la Protección de la Privacidad de los Clientes, se informa de transmisiones de Información de Salud Protegida (PHI) no encriptada a destinaciones internas o externas no autorizadas; se identifican cámaras IP transmitiendo en la red; se alerta de dispositivos afectados con potencial de grabar o impactar la privacidad del paciente; y se crean normativas de seguridad para prevenir la exfiltración de datos.

Por último, con las Políticas de Seguridad y control de Regulaciones (Análisis de Brechas de Seguridad), se crean informes para la identificación de dispositivos sin los controles de seguridad enterprise necesarios como: agentes de protección endpoint, parches/asset management agent (SCCM). Ayuda a fortalecer la seguridad y protección ante ciberataques; y se identifica y ayuda a la remediación de dispositivos personales (BYOD).

ARQUITECTURA DE SEGURIDAD Y OPERACIONES

Con las Operaciones de Seguridad de la Información, se mejora la detección y respuesta del SOC ante ciberataques y detección de ransomware (reduce el tiempo de inactividad del hospital); se aplican políticas de seguridad automáticas para contener y mitigar incidentes (menor tiempo de respuesta y resolución); y se alerta ante comportamientos anómalos como exfiltración de datos, comunicación con IPs internacionales, y conexiones de red no autorizadas.

Con la Gestión de vulnerabilidades y amenazas, se manejan las vulnerabilidades en dispositivos médicos; se realizan y expanden políticas de escaneo de vulnerabilidades para dispositivos nuevos y ya existentes; se asesora sobre riesgos en tiempo real y contextualiza, según tipo de dispositivos, función, comportamiento, y vulnerabilidades; se crean informes y monitorizan en tiempo real los intentos de explotación de vulnerabilidades de día cero en dispositivos médicos y Enterprise; y se crean cuadros de mando de seguimiento de los esfuerzos de remediación.

Por último, con la Capacidad de Respuesta de Incidentes Automatizada, se integra con mallas de ciberseguridad existentes para automatizar respuestas de seguridad; se identifican comportamientos malignos y ejecuta políticas estrictas de firewall para remediarlos; se integra con soluciones NAC para segmentar la red y poner en cuarentena dispositivos; y genera tickets de forma automática para alertas, investigación y seguimiento. ■

MÁS INFORMACIÓN

- Security Operational efficiency
- Securing the patient journey
- Medical device vulnerabilities

La protección de correo electrónico, clave en el sector sanitario

Iberlayer, como compañía centrada exclusivamente en la protección del correo electrónico desde la nube, ofrece una solución en la que han confiado compañías de casi toda Europa, Reino Unido, Estados Unidos y América Latina: Iberlayer Email Guardian.

El correo electrónico es la principal vía y puerta de entrada de aproximadamente 9 de cada 10 incidentes de ciberseguridad, porque el email es la forma más sencilla de llegar al interior de las compañías y a su eslabón más débil: el usuario final. Con solo un 8% del correo electrónico considerado como limpio, todo el resto es correo no deseado, incluyendo correos spam, scam, phishing, fraudes, estafas, y correos con malware, que además de consumir recursos corporativos, como ancho de banda, carga en sistemas, espacio en disco, entre otros, puede suponer un gran riesgo en la seguridad de las propias compañías hasta límites críticos.

Hoy día, las compañías se enfrentan a la necesidad de contar con cuatro elementos fundamentales para mantenerse protegidos:

- Tecnología con años de experiencia con un alto nivel de sofisticación, automatización, disponibilidad, y capacidad de detección de los algoritmos empleados en las campañas de correo no deseado.
- Personal experto en ciber-seguridad que esté constantemente actualizado y constan-

Al tratarse de un servicio y no de un producto, Email Guardian ofrece a las compañías una capa de seguridad completa con una fuerte protección frente a las amenazas que a diario se reciben por email

temente pendiente de todas las amenazas nuevas que a diario van apareciendo...

- Personal experto en el correo electrónico y en el uso y administración de las herramientas de filtrado de correo para su correcto funcionamiento, continuos ajustes y parametrizaciones...
- Personal que esté pendiente de los paneles de control, estado de los sistemas, logs, posibles alertas... y con el nivel de entrenamiento adecuado para distinguir cuando es necesario tomar medidas drásticas.

EMAIL GUARDIAN DE IBERLAYER

Al tratarse de un servicio y no de un producto, ofrece a las compañías una capa de seguridad completa con una fuerte protección frente a las amenazas que a diario se reciben por email y sin necesidad de gestionar todas las anteriores necesidades mencionadas. Como servicio completo de protección del correo electrónico desde la nube, impide que posibles amenazas a través de este vector, lleguen hasta los usuarios, protegiéndolos contra ransomware y malware de todo tipo, Spam, Scam, Phishing, Fraudes, Estafas, y un largo etcétera.

IBERLAYER DOMAIN GUARDIAN

Uno de los principales métodos utilizados para ataques de Phishing es la suplantación de identidad. Resulta sencillo y económico registrar un dominio similar al de la víctima para hacernos pasar por un alto cargo y realizar un fraude de CEO. En muchos casos se suplantan dominios de reconocidas marcas para que resulte mucho más creíble el origen del correo. De este modo, el usuario confía en el emisor y no sospecha de un posible ataque.

El sistema de vigilancia de dominios, incluido en el servicio Iberlayer Email Guardian, monitoriza la creación de nuevos dominios similares. De este modo, se puede anticipar a una posible suplantación de identidad permitiendo tomar las medidas necesarias en un tiempo mínimo.

El laboratorio de Iberlayer vigila, monitoriza, estudia y analiza constantemente la actividad mundial relativa al email, incluyendo un servicio de vigilancia de dominios, para, no solo bloquear todo tipo de amenazas, sino también tratar de adelantarse a ellas lo antes posible. Dada la inmediatez del peligro, a través de Domain Guardian, Iberlayer es capaz de monitorizar posibles abusos, avisando al cliente de manera directa, incluso vía telefónica en casos urgentes, de aquellas actividades sospechosas de posibles fraudes o ataques dirigidos. ■

MÁS INFORMACIÓN

Iberlayer

Email Guardian

Soluciones para una telesalud de calidad

Logitech está promoviendo la adopción y eficacia de la telesalud trabajando para crear una atención médica innovadora que mejore la calidad de vida y la interacción entre pacientes, proveedores y profesionales sanitarios. Logitech permite a las organizaciones de atención médica brindar atención de alta calidad independientemente de su ubicación a través de un conjunto de soluciones de videocolaboración fundamentales y fáciles de administrar.

A medida que la telesalud continúa transformándose e innovándose, Logitech busca desarrollar soluciones que se integren fácilmente en la sanidad con el objetivo de ofrecer experiencias excepcionales a todas las personas involucradas en los servicios sanitarios a través de atención vanguardista y centrada en el paciente.

Para los profesionales, sus pacientes y los equipos de TI, las soluciones de videocolaboración de Logitech proporcionan experiencias de telesalud de alta calidad para repensar las posibilidades y necesidades de todos ellos. Logitech ayuda a las organizaciones de atención médica de todo el mundo a brindar atención de alta calidad de forma remota, mejorando los resultados, reduciendo los costes y elevando la experiencia de atención sanitaria para todos los involucrados.

De cara al paciente, las soluciones de Logitech le conectan con su especialista médico al instante y le permiten evitar desplazamientos innecesarios, porque su examen y control se realizan en modo remoto, a través de vídeo y evitando cualquier riesgo de contagio potencial.

En el día a día de los profesionales sanitarios, estas soluciones modernizan las salas de reuniones, los despachos y demás ubicaciones de los diferentes equipos multidisciplinares (MDT). Asimismo, permiten equipar las salas de los centros favoreciendo la consulta entre el personal médico y potenciar la formación a distancia, habilitando a los médicos y enferme-

Para los profesionales, sus pacientes y los equipos de TI, las soluciones de videocolaboración de Logitech proporcionan experiencias de telesalud de alta calidad para repensar las posibilidades y necesidades de todos ellos

ras la observación de cirugías y procedimientos en remoto de otros hospitales o centros de investigación.

Herramientas como webcams, auriculares y otras soluciones profesionales para equipar el espacio de trabajo personal sanitario, como es el caso de Logitech Brio, una webcam que permite habilitar cualquier espacio en una sala de consulta remota para conectar al personal médico con los pacientes, y estos con sus familiares en casos de ingreso prolongado. La implementación de auriculares con micrófono como los Logitech Zone con cancelación de ruido con el objetivo de mejorar la experiencia de los pacientes y los médicos con un audio claro y de alta calidad. O, el uso de Logi dock para simplificar la organización del espacio de trabajo del especialista, reducir la acumulación de cosas en el escritorio y contribuir a su productividad.

Además de la apuesta por avanzadas soluciones de videocolaboración para consultas o salas de formación, como es el caso de Rally Bar, una barra de video todo en uno, que facilita el acercamiento de equipos que están en diferentes centros, con el fin de reducir el número de viajes para el seguimiento de los pacientes o la puesta en común de casos prácticos. Todo ello a partir de un sistema de doble cámara y tecnología de encuadre automático RightSight 2, que además permite elegir la vista para resaltar al orador activo, la vista de grupo para capturar a todos los presentes en la sala o combinar las dos vistas para una experiencia inmersiva y atractiva; y, Tap Scheduler, un panel de programación enfocado a gestionar de forma más eficiente los espacios de reunión. Esta solución se ha diseñado para facilitar su visualización y uso, con una instalación sencilla y una experiencia de usuario intuitiva que impulsan una rápida implantación y adopción.

En resumen, todo tipo de soluciones para impulsar la digitalización del sector sanitario, compatibles con todas las plataformas de vídeo en la nube del mercado, que permitan tender los puentes necesarios de cara a mantener unidos a todos los profesionales del ámbito sanitario y apostar por una nueva relación entre médico-paciente. ■

MÁS INFORMACIÓN

- El futuro de la atención virtual conectada
- Lecciones del COVID 19

ARMIS®

Fortalece la seguridad de tus pacientes obteniendo visibilidad completa de todos tus dispositivos

Armis ofrece visibilidad completa e información precisa sobre todos los dispositivos administrados y no autorizados de tu red.

Descubre nuestra solución en
www.armis.com/medical-device-security/

Soluciones para convertir a las sanitarias en compañías Data Driven

MicroStrategy es una empresa con foco en el sector analítico, siendo una arquitectura orientada a objetos su mayor diferenciador con el resto de soluciones analíticas, una arquitectura que le permite el gobierno de la información y ofrecer una visión única de la verdad a lo largo de la toda la compañía.

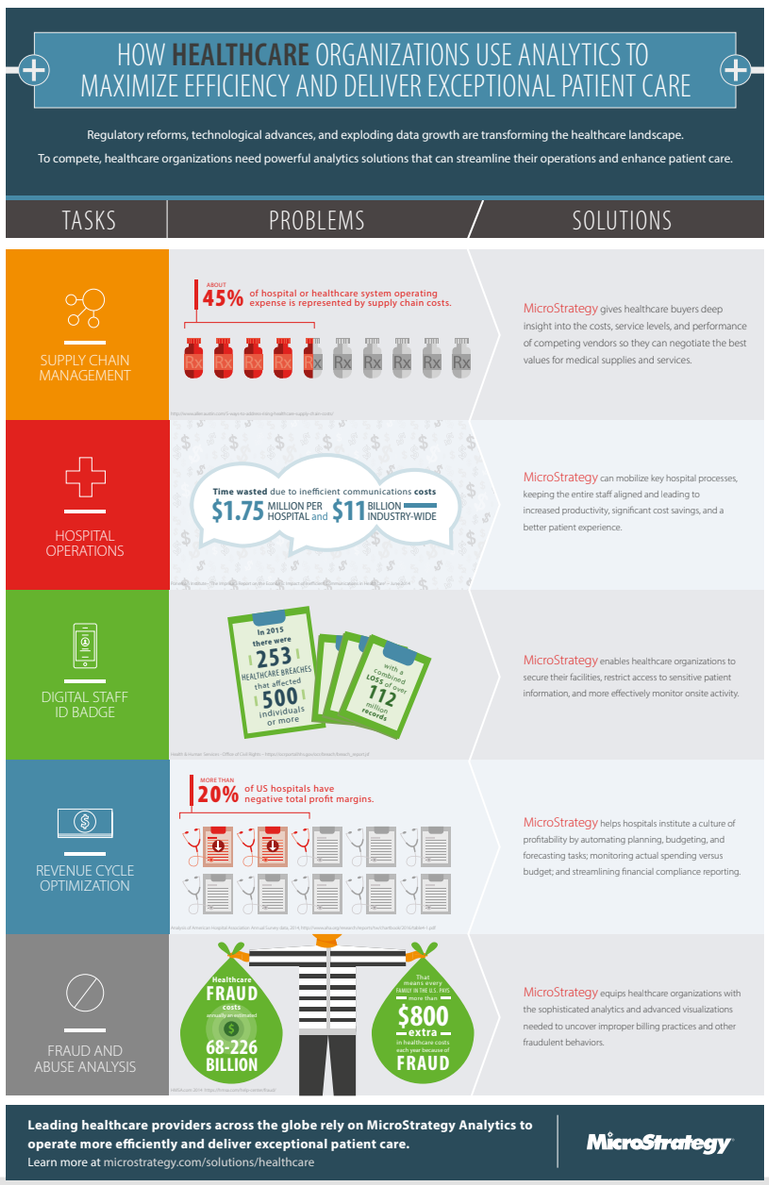
Se trata de una plataforma escalable, tanto en usuarios como en datos, que cubre cualquier caso de uso que planteen los consumidores de información sin necesidad de añadir más herramientas y por tanto pudiendo reaprovechar los desarrollos en cualquiera de los canales por los que el usuario consume la información, dando una sensación de omnicanalidad y reduciendo los costes de gestión.

Otro de los diferenciales principales de MicroStrategy es su dedicación plena a la analítica, esto hace que sea una empresa cercana con sus clientes, lo que le permite dar una atención y escucha diaria de las necesidades y tendencias. Es por eso que, desde hace unos años MicroStrategy ha trabajado en 3 áreas principalmente:

❖ **Área Corporativa.** Esto es, seguir trabajando en las capacidades para dar un servicio empresa-

rial, es decir, capacidades de gobierno del dato, de una visión única, de escalabilidad de datos y usuarios y de una seguridad centralizada.

❖ **Una arquitectura abierta.** MicroStrategy ha apificado prácticamente toda la plataforma, ha incluido un motor RestAPI para no solo poder consumir de cualquier sitio, si no para poder inyectar datos en cualquier sitio.



❖ **Modernizar la plataforma** para dar respuesta a esas necesidades de negocio modernas, como son autoservicio, pero un autoservicio gobernado, intuitivo y sin líneas de código. Dentro de la modernización, dispone de una tecnología que permite el acceso rápido, sencillo e intuitivo a la información, que se conoce con el nombre de HyperIntelligence.

Hyperintelligence es una tecnología que permite romper la brecha digital con los usuarios consumidores, y ayuda a acelerar el proceso de ser una compañía Data Driven.

El objetivo principal de Hyperintelligence es facilitar de manera rápida, sencilla e intuitiva la información a los usuarios con cero clics. Esto es, permite que los usuarios sin realizar clics con tan solo situarse sobre las palabras, conceptos de negocio que son importante para él, le abra una tarjeta que trae los datos relevantes de 1 o varias fuentes. De esta manera, la tarjeta permite consolidar los datos más importantes de múltiples sistemas, lo que acelera enormemente la productividad y permite que las decisiones estén apoyadas en los datos.

La otra gran característica de Hyperintelligence es su tiempo de despliegue, en tan solo unos días es posible tener las tarjetas disponibles, las cuales aparecerán sobre cualquier solución de mercado o aplicación desarrollada internamente que corra sobre navegador o móvil principalmente. ■

Hyperintelligence es una tecnología que permite romper la brecha digital con los usuarios consumidores, y ayuda a acelerar el proceso de ser una compañía Data Driven

MÁS INFORMACIÓN

- Healthcare Pharmaceuticals
- The Hyperintellicenge Pilot
- Health Solution Map
- Caso de éxito: Derbyshire NHS
- Caso de éxito: AllScripts
- HyperIntelligence

Seguridad Sophos para Sanidad

Sophos cuenta en su oferta tecnológica con soluciones de seguridad que aplican en el mundo de la Sanidad. Conozcamos algunas de ellas.

❖ **Sophos Intercept X EDR/XDR.** Es un sistema de protección endpoint que engloba la protección tradicional (firmas), junto con protección "next-gen" (Inteligencia Artificial, anti exploit, análisis de comportamiento, anti ransomware y anti hacking) así como protecciones complementarias (control web, control de aplicaciones, cifrado, DLP...) y, por supuesto, EDR o, a día de hoy, XDR, gracias a la integración cruzada de datos con sus firewalls, su servicio de correo, su UEM para la gestión de los dispositivos móviles y los sistemas de protección cloud. Su gestión se realiza a través de Sophos Central, lo que permite la interacción con otros productos de Sophos y gracias a su API, con cualquier fabricante.

❖ **Sophos MTR y Rapid Response**. Sophos Managed Threat Response (MTR) es un servicio gestionado de respuesta frente a amenazas, que ofrece a las empresas funciones de búsqueda, detección y respuesta ante posibles amenazas 24/7. Formado por un equipo de detección de amenazas y profesionales expertos en investigaciones avanzadas dando respuesta a los ciberataques y tomando medidas para neutralizar incluso las amenazas más sofisticadas. Sophos puede dar respuesta, apoyándose en el agente de Sophos para realizar las acciones oportunas para la detección y la mitigación de la amenaza. Cualquier empresa que sufra un ataque activo puede recurrir a Sophos Rapid Response, que es capaz de realizar un despliegue rápido del producto y su equipo de expertos en ciberseguridad son capaces de ver cuál es la situación dentro de la compañía, detener el ataque y, si es posible, detectar por dónde ha venido, a quién ha afectado y limpiar todo lo que haya sido dañado para que pueda volver a la normalidad lo antes posible.

❖ **Sophos Firewall.** La seguridad de red desde la compra de Astaro en 2008 por Sophos ha seguido evolucionando hasta llegar a los nuevos Sophos Firewall, que son gestionados de forma centralizada desde Sophos Central, se integran con el Endpoint y con el servicio MTR. Además, son capaces de hidratar el lago de datos, englobándose dentro de su estrategia XDR. La arquitectura de Xstream de Sophos Firewall protege la red de las amenazas más recientes, al tiempo que acelera el tráfico importante de SaaS, SD-WAN y aplicaciones en la nube.

❖ **Sophos Zero Trust:** Sophos ZTNA se basa en los principios de Zero Trust: no confiar en nada y verificarlo todo. Los usuarios y dispositivos se convierten en su propio perímetro microsegmentado, con lo que se validan y verifican constantemente. Con Zero Trust,

los usuarios ya no se encuentran “en la red” con la confianza y el acceso implícito que habitualmente conlleva. Sophos ZTNA es la única solución Zero Trust Network Access que se integra perfectamente con un producto para endpoints next-gen: Sophos Intercept X.

❖ **Sophos Email.** Seguridad del correo electrónico más inteligente con IA. Las actuales amenazas para el correo electrónico evolucionan rápidamente, y las empresas en expansión necesitan una seguridad predictiva para el email, es decir, que combata las amenazas de hoy día sin perder de vista el mañana.

❖ **Sophos Cloud Optix.** Conscientes de que cada vez más la infraestructura de TI está migrando a la nube, Sophos lleva tiempo hablando de CSWP y CSPM gracias al agente para servidores y a Cloud Optix, el cual audita los recursos que se tengan sobre proveedores de nube pública como AWS, Azure o Google Cloud. Además, se integra con XDR y con servicios como MTR, lo que proporciona más visibilidad e información que será recogida en el lago de datos. ■

MÁS INFORMACIÓN

- Ramsonware in Healthcare
- Adaptative Security
- Guía para la adquisición de servicios de detección

Las actuales amenazas para el correo electrónico evolucionan rápidamente, y las empresas en expansión necesitan una seguridad predictiva para el email

Seguridad de Stormshield para el sector sanitario

Stormshield cuenta con una serie de soluciones diseñadas para ayudar a las empresas del entorno sanitario a enfrentarse a los retos de ciberseguridad que tienen por delante.

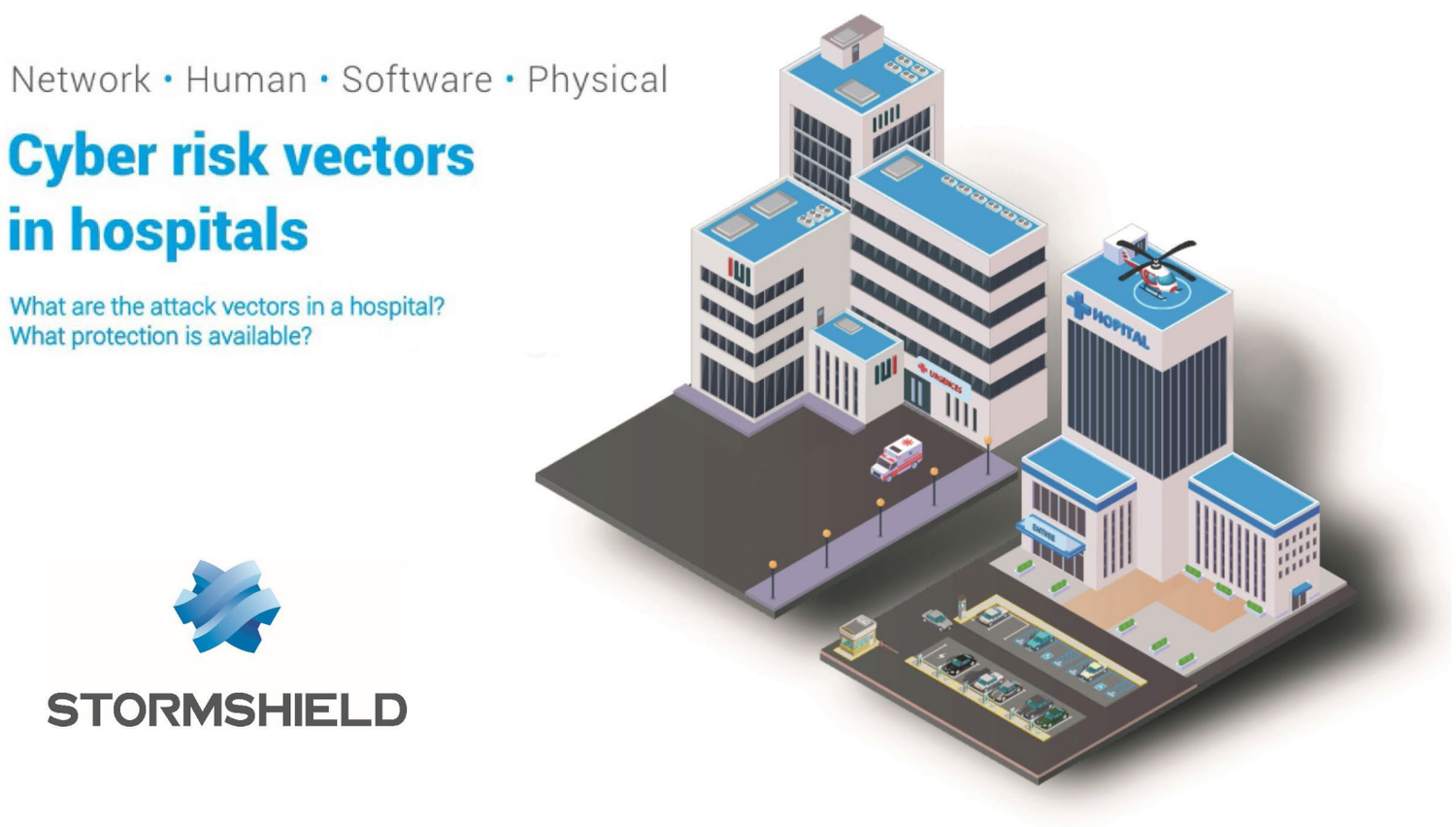
SNI20. FIREWALL A MEDIDA PARA ENTORNOS SANITARIOS

El firewall industrial SNi20 ofrece una integración de red única y completa (enrutamiento y NAT) y seguridad avanzada. Asimismo, proporciona una inspección profunda de paquetes (análisis basado en el contexto), permitiéndole proteger protocolos de comunicación de telemedicina, BMS (Building Management Systems) y CTM (Centralized Technical Management). El firewall garantiza la confiabilidad operativa de su infraestructura y una continuidad de negocio óptima en todo momento, incluso en caso de avería, gracias al sistema de alta disponibilidad y modo de seguridad de la red operativa.

El cortafuegos SNi20 ha sido diseñado para cumplir con los estándares de certificación más estrictos del mercado.

SNI40. FIREWALL PARA SISTEMAS SANITARIOS

El cortafuegos SNi40 está especialmente diseñado para proteger equipamiento médico (respiradores, imágenes médicas...) y equipamiento técnico como reguladores de presión, temperatura o gases y ofrece una amplia gama de funciones: segmentación de red, control de acceso por filtrado de direcciones IP o MAC, análisis contextual de paquetes, control de mensajes operativos y cumplimiento de protocolos (IPS) y comunicaciones seguras de mantenimiento remoto (VPN). Además, este equipo se puede integrar fácilmen-



te en su entorno, especialmente en sus armarios de control (sobre rieles DIN), gracias a un sencillo procedimiento de puesta en marcha.

El SNi40 garantiza la continuidad de la actividad gracias, en particular, a su sistema de alta disponibilidad y al modo de seguridad de la red operativa, que mantiene sus sistemas de producción funcionando sin interrupción, incluso en caso de fallo.

El SNi40 es un cortafuegos certificado al más alto nivel europeo. Ha recibido la certificación y calificación CSPN a nivel elemental, emitida por ANSSI. Por ello, si elige esta solución de Stormshield Network Security, puede estar seguro de que su infraestructura industrial estará cubierta por la mejor protección posible.

STORMSHIELD ENDPOINT SOLUTION (SES)

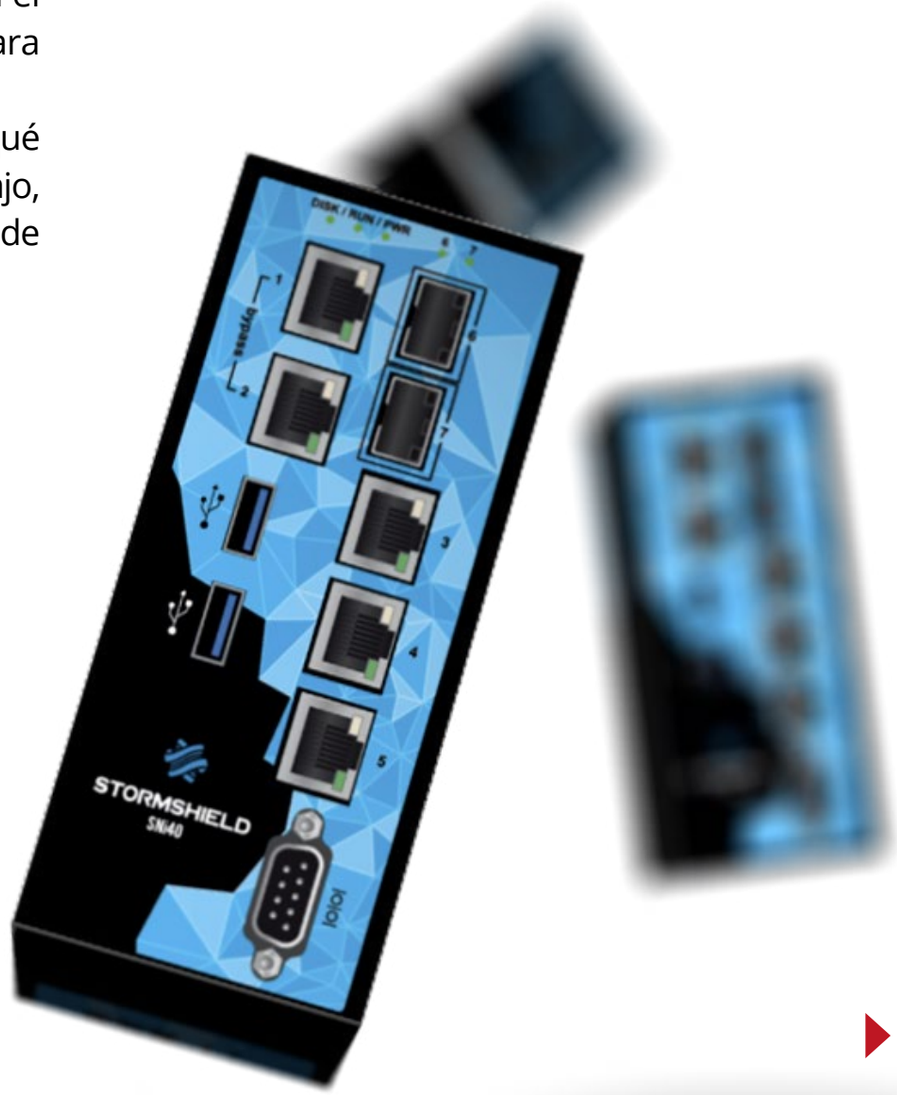
A menudo considerados como los eslabones más débiles en la seguridad de TI, los terminales incluyen todos los dispositivos que se conectan a la red central de una organización sanitaria: ordenadores de escritorio y portátiles, tabletas, teléfonos inteligentes, impresoras y todos los demás dispositivos (inteligentes o no) que se nos requiera conectar a la red interna. Sin embargo, todos estos terminales podrían ser secuestrados y utilizados por los ciberdelincuentes como un punto de entrada para penetrar en su sistema informático con el fin de instalar malware u obtener acceso a sus datos. Desde ellos, pueden saltar a la red hospitalaria provocando graves daños.

SES tiene características que lo hacen especialmente adecuado para el entorno sanitario: protege sistemas operativos obsoletos que siguen operando en redes de imágenes médicas, por ejemplo, como puede ser Windows XP. Por otra parte, SES no está basado en firmas ni necesita conexiones al exterior para su correcto funcionamiento. Por último, hay que destacar sus capacidades de creación de listas blancas, que no son manejables en el mundo IT pero sí en el sanitario, donde las aplicaciones necesarias para los puestos son mínimas y estables.

SES también controla qué dispositivos y a qué redes puede conectarse cada puesto de trabajo, bloqueando, por ejemplo, el uso no deseado de dispositivos USB. ■

MÁS INFORMACIÓN

- Telemedicina y ciber-riesgos
- Cómo prevenir ataques de ransomware
- Vulnerabilidades en la infraestructura de un hospital
- DPI Systems Network Security
- Context/Behavior-aware Endpoint Protection and response to meet digital and hybrid workforce requirement



IBERLAYER

Cloud Email Security

9 de cada 10 incidentes de
ciberseguridad empiezan por email

¿Cuánto le preocupa la seguridad del suyo?

WWW.IBERLAYER.COM

Protección total contra Spam, Phishing, Ransomware, Malware,
APTs, Scam, Fraudes de CEO, Fraudes Bancarios ...

SSE vs SASE

¿qué hay de nuevo?

SASE, o Secure Access Service Edge, es un modelo de red descrito por primera vez por Gartner en 2019. SASE realiza la transición de capacidades clave de red y seguridad a la nube, eliminando la necesidad de dispositivos basados en el perímetro y productos heredados. Brinda acceso seguro y confiable a servicios web, aplicaciones y datos, con principios de confianza cero aplicados en todo momento para lograr una confianza adaptativa continua durante cada interacción.

El modelo SASE de Gartner ha sido una respuesta a las limitaciones de las arquitecturas de red y seguridad convencionales para mantener el ritmo de las tendencias emergentes centradas en el edge, SD-WAN e Internet de las cosas (IoT).

Las arquitecturas de redes convencionales a menudo dependen demasiado de la infraestructura física y sufren la proliferación de herramientas, silos de soluciones, procesos manuales y falta de automatización. El enrutamiento de todos los puntos finales a través de un centro de datos genera problemas de rendimiento y todo ello lleva a obstaculizar la flexibilidad, la agilidad y la capacidad de una organización para ampliar su red.

SASE proporciona el marco para diseñar una arquitectura de red y seguridad convergente en un mundo donde el uso de aplicaciones en la nube es omnipresente y fundamental para los negocios. El marco SASE describe todas las tecnologías esenciales, desde la red WAN definida por software (SD-WAN), puerta de enlace web segura (SWG), firewall como servicio (FWaaS), un agente de seguridad de acceso a la nube (CASB) y acceso a la red Zero Trust (ZTNA) en una sola arquitectura unificada.

SSE se refiere al conjunto de servicios SASE utilizados para proteger el tráfico empresarial

Zero Trust

Zero Trust es compatible con SSE y SASE al garantizar que los usuarios obtengan un acceso continuo y seguro a las aplicaciones, los activos y la web de la organización.

Zero Trust puede proporcionar acceso seguro a través de cualquier topología de red (SD-WAN, VPN, Internet pública, SASE u otros) y conectar empleados remotos, terceros, proveedores de la cadena de suministro, centros de datos y más. Esto se debe a que Zero Trust traslada las defensas de los parámetros basados en la red a los parámetros basados en la identidad y valida el acceso independientemente del origen de la red. Entonces, ya sea que tenga SSE o SASE, ZTNA es el modelo más seguro para su organización.

La detección de amenazas y la prevención de ciberataques son factores clave para adoptar SSE y, en menor medida, SASE

Entre los beneficios de este modelo destaca que a SASE no le importa dónde residen las aplicaciones, que pueden estar tanto en un centro de datos corporativo, en una nube pública o privada, o ser una oferta de SaaS. La arquitectura distribuida de SASE facilita la realización de funciones de seguridad cerca del usuario final, al tiempo que simplifica la conectividad a las aplicaciones.

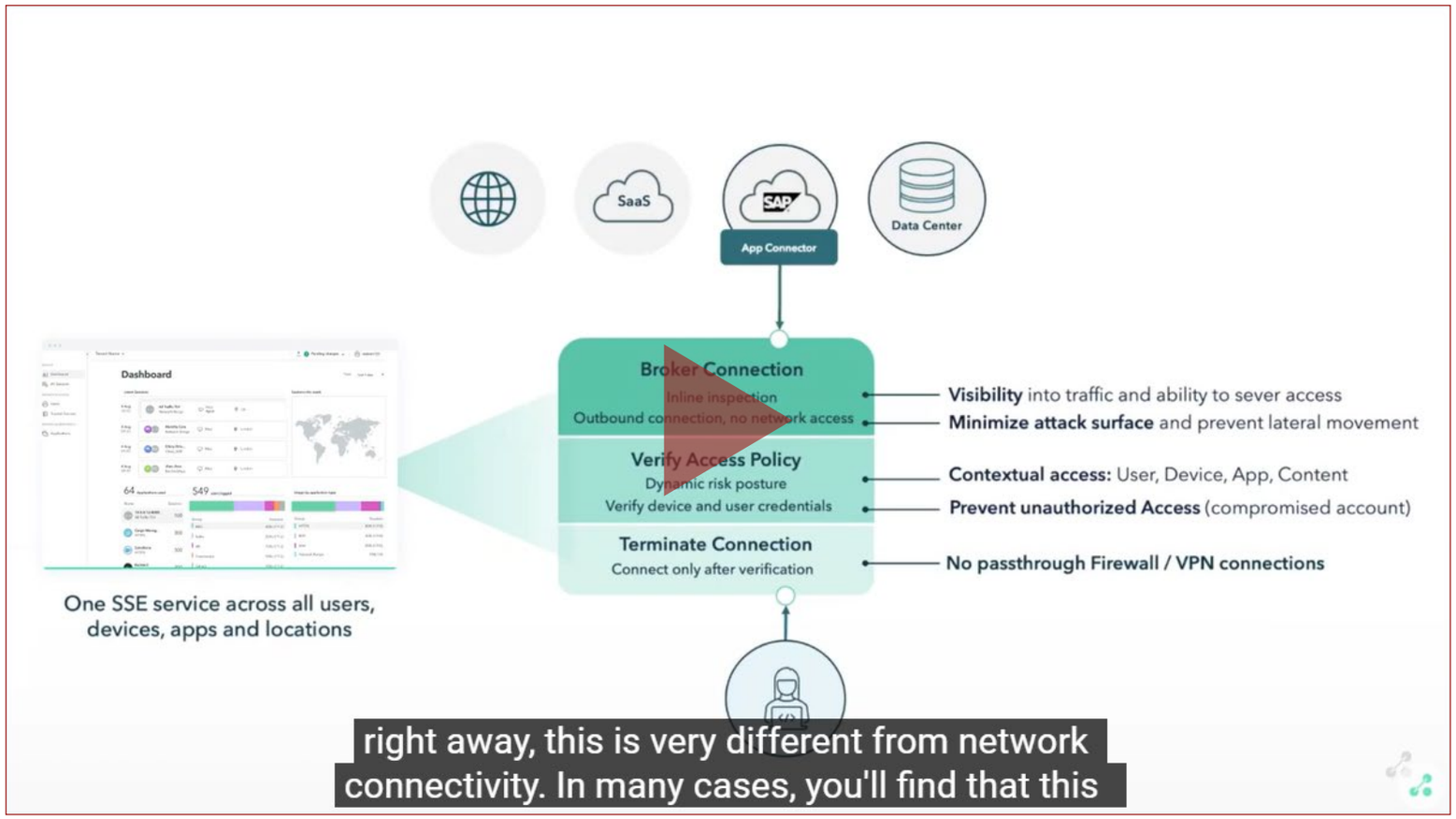
Por otra parte, la seguridad se aplica de forma dinámica, con políticas basadas en el rol de la entidad de conexión, y la gestión de la identidad se convierte en un requisito fundamental. Esta seguridad integrada y la gestión de la red de manera centralizada reducen el coste continuo de mantenimiento del sistema, así como la posibilidad de errores humanos. Se añade que, con la estructura adecuada, los mecanismos SASE pueden realizar análisis del comportamiento de la red para identificar amenazas de seguridad.

En el momento de anunciar este modelo, Gartner también predijo que para 2024 el 40% de las empresas adoptarían una estrategia SASE. Seguramente se quedaron cortos, ya que como se ha dicho en incontables ocasiones, la pandemia sanitaria aceleró la transformación digital y, por tanto, la adopción de nuevas tecnologías y arquitecturas.

SSE – Secure Service Edge

En las arquitecturas modernas, la red y la seguridad están estrechamente relacionadas. La transformación digital y la adopción de la infraestructura en la nube han convertido el acceso seguro a las aplicaciones en la nube y los centros de datos en la piedra angular de la conectividad empresarial. Sin embargo, en muchas empresas, los equipos de TI y seguridad todavía están aislados y tienen diferentes requisitos y prioridades.

Esto llevó a Gartner, a finales de 2021, a hablar de SSE, o Secure Service Edge, que “asegura el acceso a la web, las aplicaciones privadas y el uso de servicios en la nube. Las capacidades incluyen control de acceso, protección contra amenazas, seguridad de datos, monitoreo de seguridad y control de uso aceptable impuesto por la integración



WHAT IS SECURITY SERVICE EDGE (SSE)? **CLICAR PARA VER EL VÍDEO**

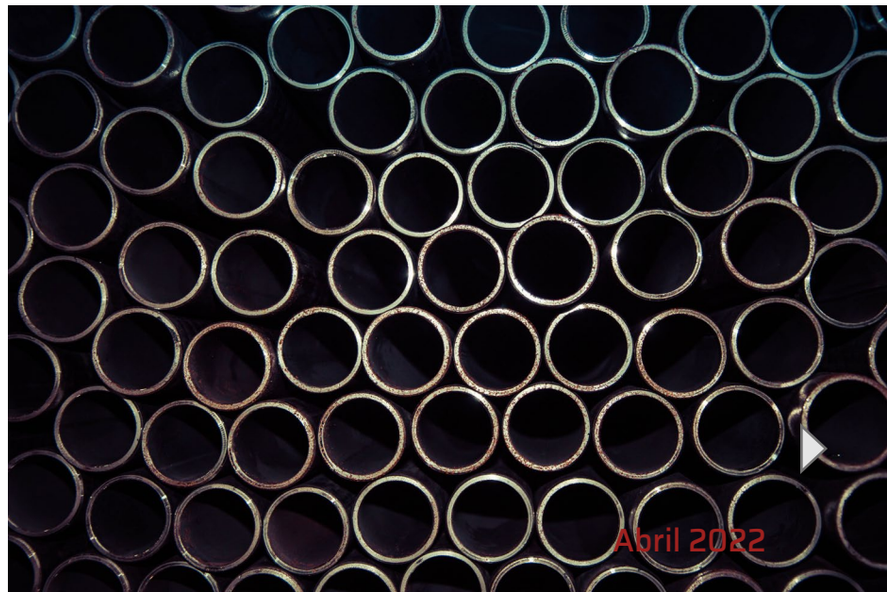
Un caso de uso imprescindible para SSE es combinarlo con SD-WAN para conseguir SASE

basada en red y API. SSE se entrega principalmente como un servicio basado en la nube y puede incluir componentes locales o basados en agentes".

Es decir, SSE permite que los equipos de seguridad modernicen su pila y servicios, independientemente de los equipos de TI e infraestructura. Este nuevo acrónimo refleja la observación de que, si bien las organizaciones buscan consolidar y simplificar la seguridad de su red para los trabajadores remotos e híbridos, algunas prefieren el mejor enfoque de proveedor dual con soluciones separadas para networking-as-a-service y security-as-a-service. Como resultado, pueden reducir la superficie de ataque sin dejar de depender de servicios de red como SD-WAN o Internet global. Cuando los equipos de TI estén listos para pasar a SASE, SSE evolucionará con ellos a SASE.

Impulsores

Los drivers de SSE son muy similares a los de SASE. Por un lado, mejora el rendimiento y la experiencia de usuario. Hay que tener en cuenta que a medida que los datos y las aplicaciones residen cada vez más fuera del perímetro de la empresa, y los usuarios cambian a modelos de trabajo remotos e híbridos, la retransmisión de todo el tráfico a una única pila de seguridad basada en on-premise tiene cada vez menos sentido ya que genera congestión, latencia y una mala experiencia de usuario. Al hacer que toda la pila de seguridad esté fácilmente disponible desde puntos de presencia en



Cuadrante Mágico de Gartner para SSE

La aparición de un mercado para soluciones SSE refleja la necesidad de que las organizaciones con fuerzas de trabajo híbridas apliquen seguridad consistente desde la nube. A finales de 2021 Gartner creó un nuevo cuadrante que identifica a los proveedores adecuados para asegurar el acceso a la web, servicios en la nube y aplicaciones privadas.

Entre los datos destacables en torno a SSE:

- **Para 2025,** el 70 % de las organizaciones que implementan el acceso a la red de confianza cero (ZTNA) basado en agentes elegirán un proveedor de servicios de seguridad (SSE) para ZTNA, en lugar de una oferta independiente, frente al 20 % en 2021.
- **Para 2025,** el 80 % de las organizaciones que buscan adquirir servicios de seguridad relacionados con SSE comprarán una solución de SSE consolidada, en lugar de un corredor de seguridad de acceso a la nube independiente, una puerta de enlace web segura y ofertas de ZTNA, frente al 15 % en 2021.
- **Para 2026,** el 50 % de las organizaciones dará prioridad a las funciones avanzadas de seguridad de datos para la inspección de datos en reposo y en movimiento como criterio de selección para SSE, frente al 15 % en 2021.

todo el mundo, los usuarios obtienen una conexión local rápida dondequiera que estén y los datos se inspeccionan más cerca de donde se accede.

Por otro lado, la naturaleza dinámica de los negocios en la actualidad requiere agilidad, no solo a la hora de apoyar a los trabajadores remotos e híbridos, sino respaldar fusiones y adquisiciones, asegurar el acceso de terceros (incluidos socios o proveedores) y aprovechar los picos estacionales. Los servicios basados en la nube son mucho más flexibles y eliminan la necesidad de instalar y mantener nuevo hardware y software a medida que cambian las necesidades comerciales.

En estos entornos híbridos, ¿cómo asegurar que se aplica la misma política de seguridad a usuarios remotos, contratistas y trabajadores de oficina? A diferencia de las soluciones de seguridad fragmentadas, un sistema unificado de administración de seguridad basado en la nube ofrece una sola consola desde la cual administrar todas las políticas, lo que mejora la postura de seguridad de toda la organización.

A la ventaja de contar con una visibilidad unificada que elimina los puntos ciegos y simplifica la auditoría, añadir que el consumir la seguridad como un servicio de la nube permite a las organizaciones subcontratar las numerosas tareas necesarias para mantener y escalar su seguridad.

Según Gartner, para 2025 el 80% de las empresas habrán adoptado una estrategia para unificar la web, los servicios en la nube y el acceso a

aplicaciones privadas desde la plataforma de servicios de seguridad (SSE) de un solo proveedor.

Casos de uso de SSE

Como hemos visto, SSE protege el perímetro de la red al combinar varias tecnologías de seguridad basadas en la nube: Firewall como servicio (FWaaS), que integra la tecnología de firewall en un servicio basado en la nube; Zero Trust Network Access (ZTNA), que aplica principios de seguridad de confianza cero al tráfico remoto; Cloud Access Security Broker (CASB), que aplica políticas y controles de seguridad empresarial al tráfico entre la nube y las redes locales.

Se han definido varios casos de uso que están impulsando a las empresas a adoptar SSE, incluida la protección del tráfico de los trabajadores remotos. Mucho antes de la pandemia, principal

El control de políticas de SSE ayuda a mitigar el riesgo a medida que los usuarios finales acceden al contenido dentro y fuera de la red

Foro ITDS. SASE, el futuro de la seguridad de la red

Gartner estima que para 2024, en al menos el 40% de las empresas se habrá adoptado una estrategia SASE, la arquitectura de seguridad que lleva a la convergencia de las tecnologías de seguridad y de conectividad de red en una plataforma proporcionada a través de la nube para proteger a los usuarios, las aplicaciones y los datos.

El próximo 28 de abril IT Digital Security celebrará un evento que reúne a numerosos expertos, incluidos portavoces de diferentes empresas de seguridad, así como CISOs hablar de SASE en torno a los cuatro componentes de seguridad clave: Secure web gateways (SWG), Cloud access security broker (CASB), Zero trust network access (ZTNA), Firewall como servicio (FWaaS).

¿Te apuntas?

impulsor del teletrabajo, muchas organizaciones reconocían las limitaciones de las VPN (redes privadas virtuales) para una fuerza laboral que podría necesitar acceso a los recursos empresariales desde cualquier parte del mundo en cualquier momento.

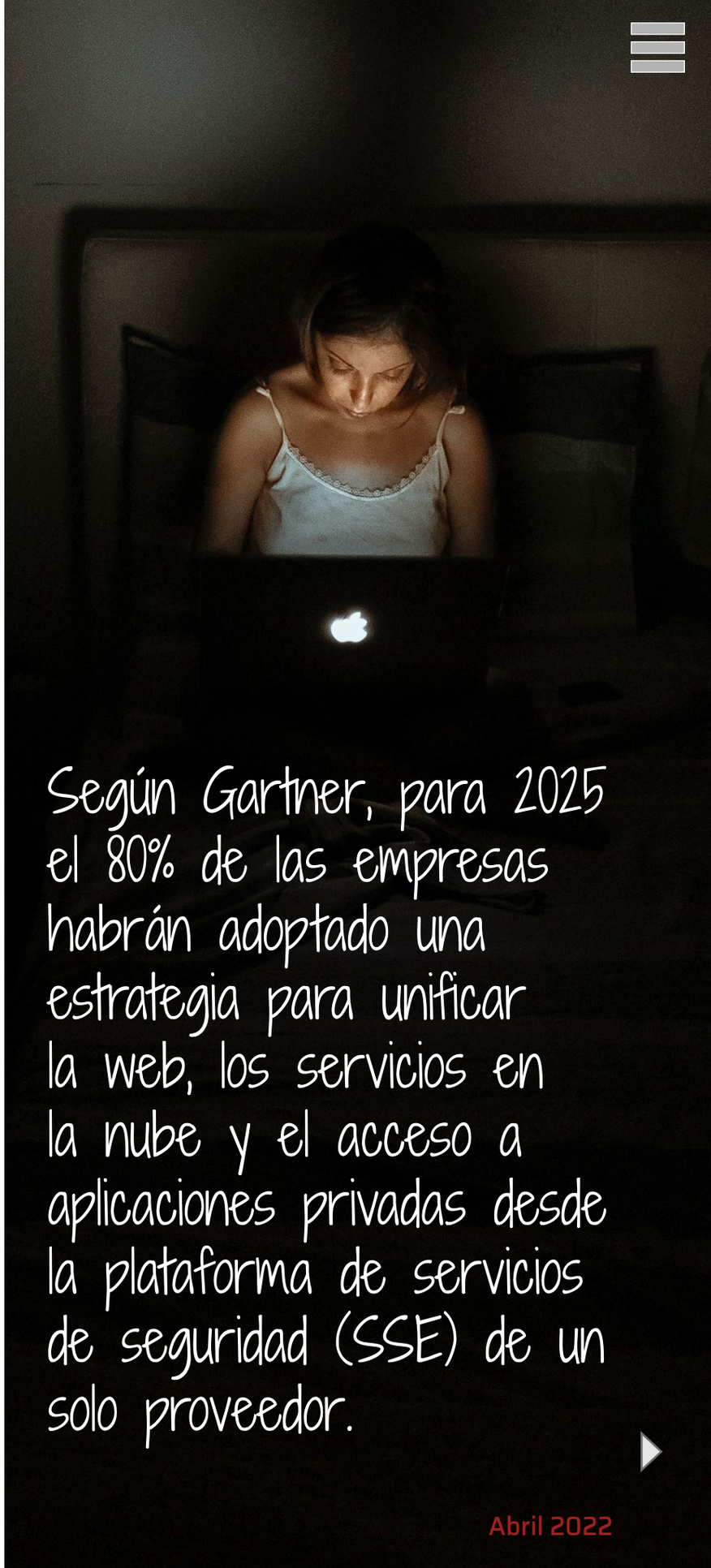
Las VPN presentan numerosos desafíos de seguridad para las empresas, como el tener que enrutar el tráfico a través de un firewall para asegurar dicho tráfico, lo que puede generar cuellos de botella. Las soluciones de VPN tradicionales no ayudan a administrar de forma centralizada sus implementaciones o monitorizar los dispositivos que se conectan de forma remota a su red. Desde el punto de vista empresarial, esto significa que se podría estar permitiendo cientos o miles de conexiones VPN remotas a una red empresarial principal, desde dispositivos que pueden o no tener controles de seguridad adecuados sin verificar la identidad o la confiabilidad de la persona que se conecta.

Además, una vez que un usuario o dispositivo se conecta a través de VPN, puede moverse libremente por la red de su empresa como si estuviera en la oficina. Esto significa que, si un ciberdelincuente compromete una cuenta privilegiada con acceso VPN, podría saltar de un sistema a otro, extrayendo datos y causando daños financieros y de reputación en el proceso.

Hacer cumplir el control de políticas sobre el acceso de los usuarios a Internet, la web y las aplicaciones en la nube (históricamente realizado por un SWG) es uno de los principales casos de uso para SSE. El control de políticas de SSE ayuda a mitigar el riesgo a medida que los usuarios finales acceden al contenido dentro y fuera de la red. Hacer cumplir las políticas corporativas de control de acceso e Internet también es un factor clave para este caso de uso en IaaS, PaaS y SaaS. Otra capacidad clave es la gestión de la postura de seguridad en la nube (CSPM), que protege a su organización de configuraciones erróneas peligrosas que pueden provocar infracciones.

La detección de amenazas y la prevención de ciberataques son factores clave para adoptar SSE y, en menor medida, SASE. Dado que los usuarios finales acceden al contenido a través de cualquier conexión o dispositivo, las organizaciones necesitan un sólido enfoque de defensa en profundidad contra el malware, el phishing y otras amenazas. Lógicamente, la plataforma SSE debe tener capacidades avanzadas de prevención de amenazas, incluido el firewall en la nube (FWaaS), el espacio aislado en la nube, la detección de malware y el aislamiento del navegador en la nube. Los CASB permiten la inspección de datos dentro de las aplicaciones SaaS y pueden identificar y poner en cuarentena el malware existente antes de que cause daños. El control de acceso adaptativo, mediante el cual se determina la postura del dispositivo del usuario final y el acceso, se ajusta en consecuencia, también es un componente clave.

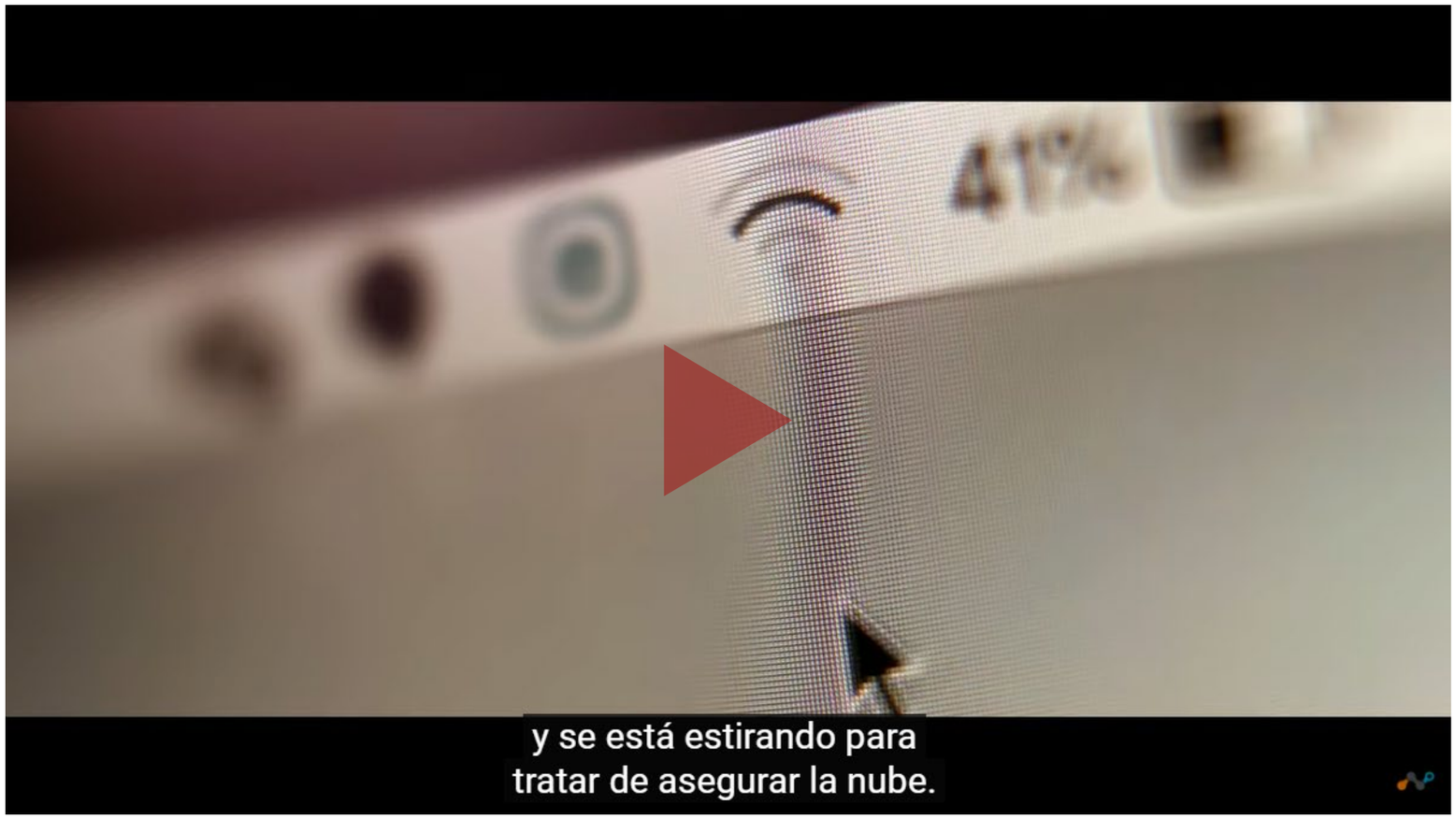
Otro caso de uso es el poder identificar y proteger los datos confidenciales. SSE permite



encontrar y controlar datos confidenciales sin importar dónde residan. Al unificar las tecnologías clave de protección de datos, una plataforma SSE proporciona una mejor visibilidad y una mayor simplicidad en todos los canales de datos. Cloud DLP permite que los datos confidenciales (por ejemplo, información de identificación personal [PII]) se encuentren, clasifiquen y aseguren fácilmente para admitir los estándares de la industria de tarjetas de pago (PCI) y otras políticas de cumplimiento. SSE también simplifica la protección de datos, ya que puede crear políticas DLP solo una vez y aplicarlas en el tráfico en línea y los datos en reposo en aplicaciones en la nube a través de CASB.

Las plataformas SSE más efectivas también brindan inspección TLS/SSL de alto rendimiento para abordar el tráfico encriptado (es decir, la mayoría de los datos en tránsito). También es clave para este caso de uso el descubrimiento de TI en la sombra, que permite a las organizaciones

SSE permite que los equipos de seguridad modernicen su pila y servicios, independientemente de los equipos de TI e infraestructura



WHAT IS SECURITY SERVICE EDGE? **CLICAR PARA VER EL VÍDEO**

bloquear aplicaciones riesgosas o sancionadas en todos los puntos finales.

Un caso de uso imprescindible es combinar SSE con SD-WAN para conseguir SASE. Como hemos comentado al comienzo, SASE es un modelo de seguridad que combina una pila de seguridad basada en la nube con tecnología de red de área amplia definida por software (SD-WAN). La pila SASE incluye las mismas tecnologías que SSE y probablemente haya notado que los nombres son muy similares. Esto se debe a que SASE es esencialmente SSE más acceso, proporcionado por una red troncal SD-WAN.

Cómo escoger la solución correcta

SSE se refiere al conjunto de servicios SASE utilizados para proteger el tráfico empresarial. SSE garantiza que el usuario (o carga de trabajo) correcto reciba acceso de forma segura y bajo el control de TI de la empresa a las aplicaciones y servicios correctos. Esos servicios pueden ser

La protección del tráfico de los trabajadores remotos es uno de los casos de uso de SSE

cargas de trabajo en una IaaS o PaaS, aplicaciones SaaS o servicios de Internet como LinkedIn o YouTube. Además, el acceso al servicio debe otorgarse siguiendo los controles Zero Trust Access (ZTA).

Teniendo esto presente, cuando se busque una plataforma SSE se necesita una que haya sido diseñada específicamente para una experiencia rápida de usuario y aplicación en la nube, y eso significa una arquitectura nativa de la nube distribuida globalmente.

También debe tenerse en cuenta que haya sido diseñada desde cero con una arquitectura de confianza cero. Ya que el control de acceso debe regirse por la identidad y nunca ubicar a los usuarios en su red, han de optarse por proveedores nativos de la nube que ofrezcan un amplio soporte para el acceso de confianza cero en todos los usuarios, dispositivos, IoT, aplicaciones en la nube y cargas de trabajo.

Capaz de inspección proxy escalable en línea. La inspección de proxy finaliza ambas conexiones, desde el dispositivo y desde la aplicación en la nube. Sentarse entre los dos significa que se puede realizar una inspección SSL completa, de forma que deberá concentrarse en las plataformas SSE que pueden ofrecer contenido e inspección TLS/SSL a escala global. Además, dado que la inspección en línea generalmente se realiza en el tráfico crítico para el negocio, las interrupciones debido a problemas de escalabilidad pueden tener un impacto grave, asegúrese de que su proveedor de SSE elegido tenga sólidos acuerdos de nivel de servicio (SLA). it

Enlaces de interés...

- Cuadrante mágico de Gartner para SSE
- Secure Service Edge Reviews, Gartner
- SASE, el futuro de la seguridad de la red

Compartir en RRSS

it User
TECH & BUSINESS

Cada mes en la revista, cada día en la web.

JOSÉ MANUEL NAVARRO

CMO MOMO GROUP

José Manuel Navarro Llena es experto en Marketing, Durante más de treinta años ha dedicado su vida profesional al sector financiero donde ha desempeñado funciones como técnico de procesos y, fundamentalmente, como directivo de las áreas de publicidad, imagen corporativa, calidad y marketing. Desde hace diez años, basándose en su formación como biólogo, ha investigado en la disciplina del neuromarketing aplicado, lo que le ha permitido dirigir, coordinar e impartir formación en diferentes masters de neuromarketing en escuelas privadas y en universidades públicas. Es Socio fundador de la agencia de viajes alternativos Otros Caminos, y de la entidad de dinero electrónico con licencia bancaria otorgada por el Banco de España SEFIDE EDE de la que en la actualidad es director de Marketing. Autor de “El Principito y la Gestión Empresarial” y “The Marketing, stupid”, además de colaborador semanal desde 2006 en el suplemento de economía Expectativas del diario Ideal (Grupo Vocento).

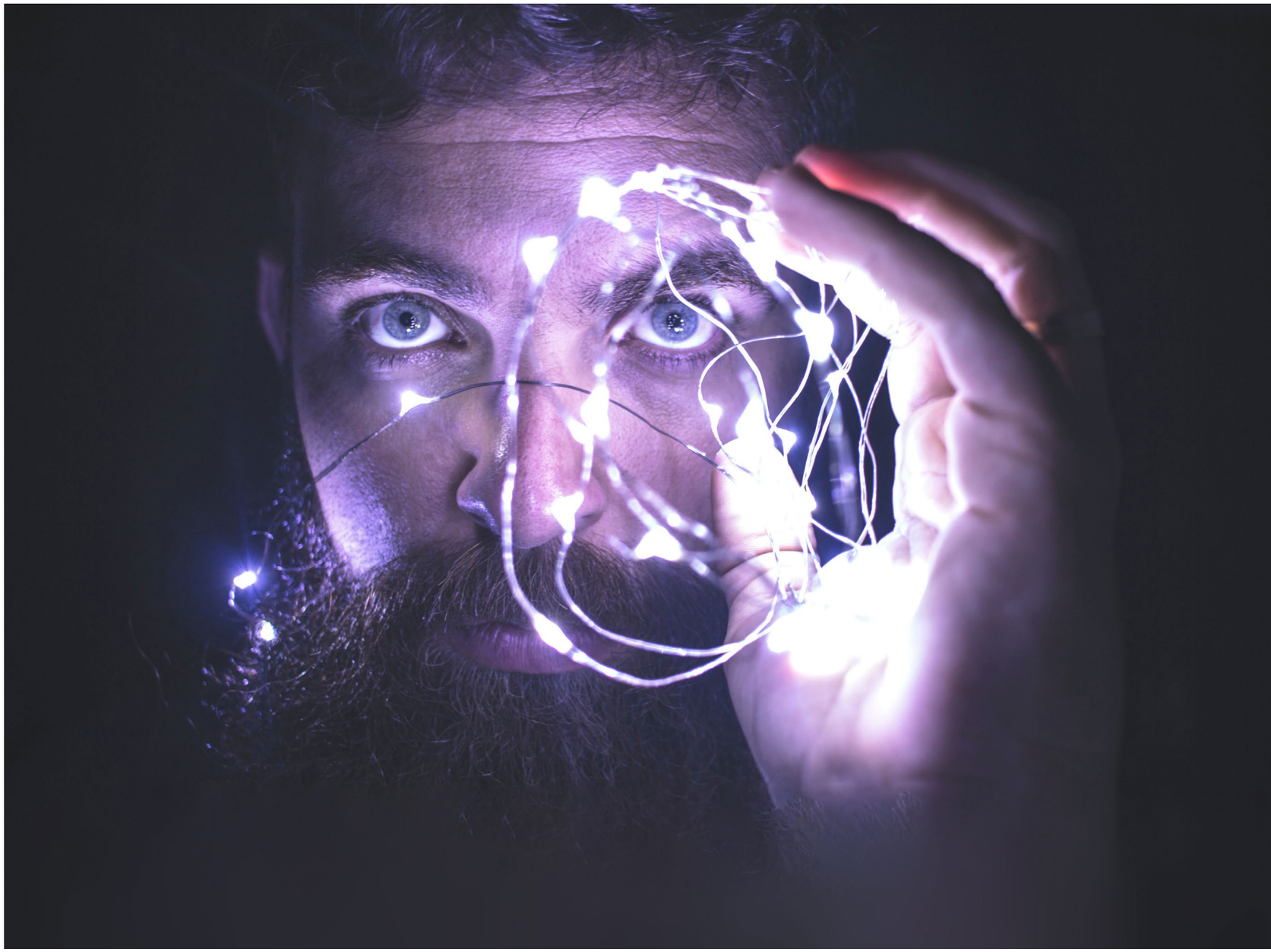
Compartir en RRSS

it Digital Security

Tribuna Marketing y Consumo

Protección de derechos personales y neurotecnología

Mientras escribo estas líneas, la revista Nature Communications publica el estudio clínico llevado a cabo por investigadores del Centro Wyss de Bioingeniería y Neuroingeniería, en colaboración con la Universidad de Tubinga (Alemania), con el que han conseguido que una persona de 30 años con parálisis completa, derivada de una esclerosis lateral amiotrófica (ELA) avanzada, se comunique gracias a la implantación de 64 microelectrodos en su corteza motora primaria y a una interfaz cerebro-ordenador (BCI). El paciente moduló las tasas de activación neuronal en función de la retroalimentación auditiva y usó esta estrategia para seleccionar letras una a una que le permitieron formar palabras y frases para comunicar sus necesidades y experiencias. Estos resultados dan esperanza a las personas que están completamente aisladas a causa de enfermedades neurodegenerativas progresivas para crear un canal de comunicación que les devuelva la facultad de expresarse.



Pero también, como manifiesta el equipo de investigadores que ha llevado a cabo el experimento clínico, éste avala las bases para avanzar en la decodificación del lenguaje directamente desde el cerebro de una persona durante el proceso de habla imaginada. Esto no solo permitiría tener una comunicación más fluida con pacientes que sufran un bloqueo total o síndrome de enclaustramiento completo (CLIS), una parálisis motora general empero con capacidades cognitivas y emocionales intactas, sino que además podría suponer el principio para poder acceder a otras funciones cerebrales más complejas como son el pensamiento, los sentimientos o la anticipación de la toma de decisiones.

Este tipo progresos tecnológicos realizados en centros científicos, públicos o privados, y bajo la premisa de ayudar a mejorar las condiciones de vida de pacientes con ciertos trastornos neurológicos que se traducen en discapacidades motoras o cognitivas, merecen todo el reconocimiento y el apoyo necesario para culminar con éxito el objetivo de integrar sistemas electrónicos en la red neuronal mediante BCI que asuman el papel de las funciones o las regiones lesionadas o deterioradas. Que una persona con ELA pueda comunicarse, un paciente con Parkinson pueda controlar los episodios de temblores y la disfunción de sus movimientos o un parapléjico pueda volver a caminar, son algunos de los ejemplos que han sido fruto del interés científico por cumplir con sus principios deontológicos de combatir la enfermedad,

procurar el bien del paciente, evitar dañar y actuar con generosidad aún a riesgo de su vida o de sus intereses personales.

Pero ¿qué puede suceder cuando esta tecnología no se desarrolla en el ámbito sanitario sino en el de empresas privadas con socios que exigen reparto de beneficios cada ejercicio? Tomemos como ejemplo Neuralink, la compañía de Elon Musk creada para desarrollar BCI que conecten nuestros cerebros a sistemas inteligentes para, en principio, ayudar a personas con discapacidad para que puedan recuperar algunas de las habilidades o funciones perdidas a través del control mental de ordenadores y dispositivos móviles. La aspiración de conectar la inteligencia biológica con la artificial, de lograrse satisfactoriamente, permitirá no solo restaurar disfunciones motrices y sensoriales, sino que será el paso para expandir nuestras capacidades cognitivas y aventurar un nuevo mundo de múltiples interacciones interpersonales (brainet) y persona-máquina, y de oportunidades para mejorar la raza humana. Estos avances, a cargo de una empresa privada que deba responder a las compañías y fondos de inversión que aportaron el capital

En el ámbito de la neurociencia no se debería esperar a evidenciar malas praxis para proteger el derecho de los ciudadanos a decidir el acceso a su "intimidad cognitiva", con independencia de que acepten el implante de "neurochips" para cuestiones médicas

No se trata de obtener datos e información de comportamiento de compra, de preferencias, de respuestas emocionales o de tendencias ideológicas, sino de acceder a la identidad personal más íntima, que es la integridad psicológica, el pensamiento y la conciencia

privado para llevarlos a cabo, ¿tendrían que ser vigilados para no caer en el riesgo de servir para otros propósitos más allá de los sanitarios?

Avances tecnológicos como por ejemplo los teléfonos inteligentes, las redes sociales o las plataformas de comercio electrónico, han pasado de ser instrumentos para comunicarse o hacer más fácil la vida de sus usuarios a ser fuente inagotable de datos para que grandes corporaciones puedan predecir y condicionar la conducta de miles de millones de personas. De manera análoga, neurocientíficos de todo el mundo ya han advertido de la posibilidad de que, en un plazo de dos décadas, los desarrollos descritos en los párrafos precedentes puedan convertirse en sistemas inteligentes para poder manipular los circuitos cerebrales, por lo que gobiernos y juristas deberían empezar a pensar en la legislación básica que proteja a los ciudadanos de esos avances enmascarados en soluciones médicas.

No se trata de obtener datos e información de comportamiento de compra, de preferencias, de respuestas emocionales o de tendencias ideológicas, sino de acceder a la identidad personal más íntima, que es la integridad psicológica, el pensamiento y la conciencia. Si contamos con una legislación sobre protección de datos personales, habrá que avanzar en los derechos de las personas para que, por un lado, no se pueda manipular su “yo” cuando se le implanten electrodos con cualquier finalidad médica ni queden registros de su actividad cerebral para monitorizar cómo se organizan las respuestas neuronales frente a estímulos externos e internos. E igualmente, no se debería aplicar esa tecnología para mejorar substancialmente las capacidades cognitivas de personas sanas para crear diferentes clases de humanos.

Aunque hay neurocientíficos, como **M. Nicolelis,** pioneros en la codificación de poblaciones neuronales , BCI y neuroprótesis, que también son defensores de la imposibilidad de poder acceder a los complejos e intrincados mecanismos que son ejecutados por grupos de cientos de millones de neuronas, de miles de millones de interconexiones entre ellas y de millones de células gliales encargadas de darles soporte y también de realizar algunas funciones conectoras, ya que los procesos que regulan no son codificados por estructuras estáticas sino enormemente variables. Esta propiedad, denominada plasticidad, eleva a un número tan extremadamente alto de posibles combinaciones de conexiones que supera a las que pueda realizar cualquier máquina

Es necesario promover también la ampliación del juramento hipocrático que realizan los médicos a los científicos especializados en neurotecnología, para asegurar la finalidad de los ensayos clínicos bajo el paraguas de unos principios deontológicos comunes

actual, y con un consumo de energía que no llega al que tiene una bombilla de 20 vatios.

No obstante existan estas cautelas, recordemos el conocido dilema de Collindridge: siempre que nos enfrentamos a la implantación de un nuevo avance tecnológico, no somos capaces de evaluar las consecuencias sociales que puede llegar a tener; y cuando detectamos posibles efectos negativos, su uso está tan arraigado que es complejo controlarlo o impedirlo. Es decir, nadie elucubró que un teléfono móvil pudiera convertirse en un dispositivo que generase tal adicción en su uso, que las redes sociales pudieran servir de fuente de datos para personalizar ofertas comerciales y argumentos ideológicos, que la biometría como método para securizar operaciones garantizando la identidad del usuario se transformara en mecanismo de control ciudadano...

Frente a este dilema, está quien contrapone el principio de precaución http://istas.net/descargas/Introducci%C3%B3n al Principio de Precauci%C3%B3n. Jorge Riechmann.pdf, ampliamente aplicado en el derecho internacional medioambiental, que (extrapolándolo) defiende que hasta que no se demuestre fehacientemente que ciertos avances tecnológicos no causan perjuicio alguno a individuos o colectivos, debe limitarse o prohibirse su aplicación. Llegar a ese extremo, seguramente limitaría la capacidad innovadora de muchos desarrolladores, por lo que los defensores del desarrollismo tecnológico pedirían un período de carencia para legislar mientras se encuentra una prueba de seguridad consistente o evidencia irrefutable de perjuicio.

Realmente es una situación compleja de afrontar, aunque la experiencia corrobora que las leyes han

Xxxxxx Andant voloresti aut faceatet peroreh enisciatia volupta aut quame est volupis ut estrum que ate eri quidel ipsum facero is ratempel iliquis porpore, nusdaep uditiae si odiorpor sinvenestio. Itatium, imusae sitibusti tem ut que imi, commollum,

ido siempre detrás de las innovaciones y tendencias sociales, culturales, tecnológicas, etc. Sin embargo, en el ámbito de la neurociencia, por ejemplo, no se debería esperar a evidenciar malas praxis para proteger el derecho de los ciudadanos a decidir el acceso a su "intimidad cognitiva", con independencia de que acepten el implante de "neurochips" para cuestiones médicas. Abordar la protección de esos derechos no es solo una cuestión jurídica, sino también ética que debe afrontarse con urgencia. En España, algo se ha avanzado en el apartado XXIV de la Carta de Derechos Digitales redactada el año pasado tomando como base las propuestas de la plataforma Neuro Right Initiative, en la que se ha recogido:

- **(I) el derecho a la privacidad mental** para garantizar que la actividad del cerebro no sea descifrada sin consentimiento expreso:
- **(II) el derecho a la identidad psicológica** para evitar que la personalidad sea manipulada;
- **(III) el derecho al libre albedrío** para no influir en los procesos de toma de decisiones;
- **(IV) derecho a la igualdad de oportunidades** para evitar le mejora cognitiva de determinadas personas en detrimento de otras;
- **(V) el derecho a ser consciente** de los efectos que puede tener la implantación de neurotecnologías y la aplicación de programas o algoritmos que pudieran llevar incorporados sesgos cognitivos.

Siendo estos principios bienvenidos para, al menos, definir el marco legal sobre el que trabajar, dado que la neurociencia lleva más de tres lustros

investigando soluciones tecnológicas para, con métodos invasivos o no invasivos, encontrar soluciones a problemas neurodegenerativos o importantes lesiones, lo que ya es apremiante es la regulación jurídica y ética con naturaleza de ley que bloquee las pretensiones de cualquier empresa de aprovechar la neurotecnología para obtener beneficios a partir de la explotación de información inherente a la actividad cerebral de los pacientes. En primera instancia, porque no olvidemos el futurible de conectar a personas con máquinas para elevar sus capacidades intelectuales, motoras o sensoriales. En segundo lugar, habrá que prever igualmente cómo prevenir el uso de tecnologías no invasivas que puedan extraer esa información de manera coercitiva o no consentida, que puedan ejercer el llamado neurohacking o la manipulación de la percepción o de la memoria.

Tranquiliza saber que, además del gobierno de España, la OCDE lanzó en 2019 una recomendación sobre innovación responsable en neurotecnología, que el Consejo de Europa ha creado el Plan de Acción Estratégica centrado en derechos humanos y nuevas tecnologías biomédicas y que la ONU pretende promover en 2023 una modificación de la Declaración de los Derechos Humanos que recoja estas inquietudes. No obstante, es necesario promover también la ampliación del juramento hipocrático que realizan los médicos a los científicos especializados en neurotecnologia, para asegurar la finalidad de los ensayos clínicos bajo el paraguas de unos principios deontológicos comunes que limiten el espacio de investigación de lo que será la cuarta revolución industrial (4.0), en la que convergirán tecnologías digitales, físicas y neurobiológicas.

Legislación, normativa ética, compromiso científico, voluntad política y conciencia social serán las claves para que los derechos de los ciudadanos, en materia de protección de la información de su actividad neuronal, no sean vulnerados, y para que los desarrollos tecnológicos no se vean abocados a cumplir el principio de Skolnikoff, es decir, que terminen siendo utilizados para otros propósitos diferentes para los que originalmente fueron creados.

Enlaces de interés...

- W Derechos de los ciudadanos
- I Estudio clínico revista Nature Communications
- W El principio de precaución
- W Carta de Derechos Digitales
- I Plataforma Neuro Right Initiative

Abril 2022